Description of document:	Department of Homeland Security (DHS) Inspector General (OIG) Special Agent Handbook, 2007-2017
Requested date:	2017
Released date:	13-June-2017
Posted date:	18-September-2017
Source of document:	FOIA Request FOIA Public Liaison DHS-OIG Counsel STOP 0305 245 Murray Lane, SW Washington, D.C. 20528-0305 Fax: 202-254-4398 E-mail: FOIA.OIG@oig.dhs.gov DHS FOIA / Privacy Act Request Submission Form

From: FOIA OIG
Sent: Tuesday, June 13, 2017 12:40 PM
Subject: 2017-IGFO-00043 FOIA Final Response

Thank you for your interest in DHS-OIG. Please find the attached final response to your FOIA request. As the document is too large to send as one attachment, I have split it into three parts that I will attach to additional emails.

Best,
Drew

1.0 ORGANIZATION OF THE DEPARTMENT OF HOMELAND SECURITY

1.1 ESTABLISHMENT OF THE DEPARTMENT OF HOMELAND SECURITY (DHS)

The Homeland Security Act of 2002 established the Department of Homeland Security as a Cabinet level department.

1.2 DEPARTMENT COMPONENTS

The Department of Homeland Security is composed of the following component agencies who report to the Secretary and Deputy Secretary. **(Exhibit 1-1)**

The **Directorate for National Protection and Programs** works to advance the Department's risk-reduction mission. Reducing risk requires an integrated approach that encompasses both physical and virtual threats and their associated human elements.

The **Directorate for Science and Technology** is the primary research and development arm of the Department. It provides federal, state and local officials with the technology and capabilities to protect the homeland.

The **Directorate for Management** is responsible for Department budgets and appropriations, expenditure of funds, accounting and finance, procurement; human resources, information technology systems, facilities and equipment, and the identification and tracking of performance measurements.

The **Office of Policy** is the primary policy formulation and coordination component for the Department of Homeland Security. It provides a centralized, coordinated focus to the development of Department-wide, long-range planning to protect the United States.

The **Office of Health Affairs** coordinates all medical activities of the Department of Homeland Security to ensure appropriate preparation for and response to incidents having medical significance.

The **Office of Intelligence and Analysis** is responsible for using information and intelligence from multiple sources to identify and assess current and future threats to the United States.

The **Office of Operations Coordination** is responsible for monitoring the security of the United States on a daily basis and coordinating activities within the Department and with governors, Homeland Security Advisors, law enforcement partners, and critical infrastructure operators in all 50 states and more than 50 major urban areas nationwide.

The **Federal Law Enforcement Training Center (FLETC)** provides career-long training to law enforcement professionals to help them fulfill their responsibilities safely and proficiently. The Special Investigations Division is the internal affairs component within FLETC.

The **Domestic Nuclear Detection Office (DNDO)** works to enhance the nuclear detection efforts of federal, state, territorial, tribal, and local governments and the private sector and to ensure a coordinated response to such threats.

The **Transportation Security Administration (TSA)** protects the nation's transportation systems to ensure freedom of movement for people and commerce. Responsibilities include hiring, training, and deploying federal screeners at 429 commercial airports, and deploying Federal Air Marshals (FAMS) on commercial flights. The Office of Inspection (TSA OI) is the internal affairs component within TSA.

United States Customs and Border Protection (CBP) is responsible for protecting our nation's borders in order to prevent terrorists and terrorist weapons from entering the United States, while facilitating the flow of legitimate trade and travel. CBP's significant sub-components include the Office of Border Patrol, Air and Marine, and CBP Officers (including Agricultural Specialists). The Office of Internal Affairs (CBP IA) is the internal affairs component within CBP.

United States Citizenship and Immigration Services (CIS) is responsible for the administration of immigration and naturalization adjudication functions and establishing immigration services policies and priorities. The Office of Security and Integrity is the internal affairs component within CIS.

United States Immigration and Customs Enforcement (ICE) is the largest investigative arm within DHS. ICE seeks to prevent acts of terrorism by targeting people, money, and materials that support terrorist and criminal activities. ICE is primarily comprised Office of Investigations, Detention and Removal Operations, and the Federal Protective Service (FPS). The Office of Professional Responsibility (OPR) is the internal affairs component within ICE.

The **United States Coast Guard (USCG)** protects the public, the environment, and U.S. economic interests in the nation's ports and waterways, along the coast, on international waters, or in any maritime region as required to support national security. Upon declaration of war or when the President so directs, the USCG would operate as an element of the Department of Defense, consistent with existing law. The Coast Guard Investigative Service (CGIS) is the internal affairs component within USCG.

The **Federal Emergency Management Agency (FEMA)** prepares the nation for hazards, manages Federal response and recovery efforts following any national incident, and administers the National Flood Insurance Program.

The **United States Secret Service (USSS)** protects the President and other high-level officials and investigates counterfeiting and other financial crimes, including financial institution fraud, identity theft, computer fraud; and computer-based attacks on our nation's financial, banking, and telecommunications infrastructure. The Office of Professional Responsibility is the internal affairs component within the USSS.

1.3 DHS Internal Affairs Organizations

DHS OIG exercises oversight authority over the Internals Affairs (IA) components within TSA, CBP, CIS, ICE, USCG and USSS to include the following organizations:

1) TSA Office of Internal Affairs

2) CBP Office of Internal Affairs

3) CIS Office of Security and Integrity

4) ICE Office of Professional Responsibility

5) USCG Coast Guard Investigative Service

6) USSS Office of Professional Responsibility

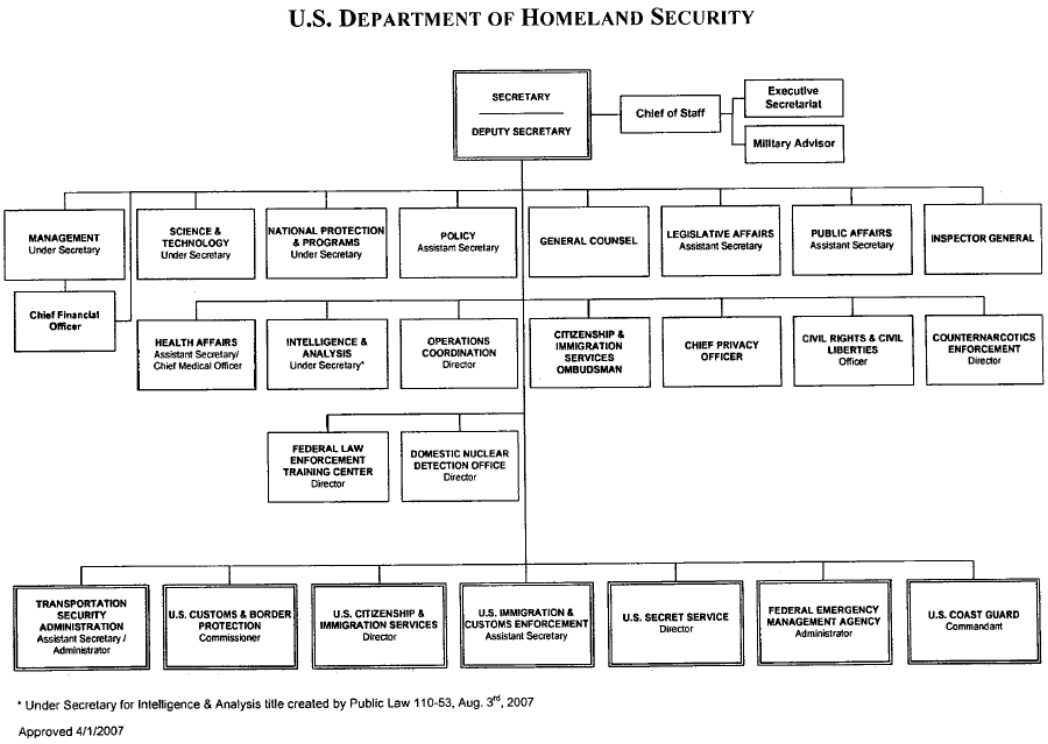
1.4 Office of Inspector General (OIG)

The OIG while organizationally a component of DHS, operates independently of the DHS and all offices within it. The Inspector General (IG) reports to the Secretary as well as to the Congress. Under circumstances specified by statute, the Secretary, upon written notification to the IG, can circumscribe the IG's access to certain types of sensitive information and exercise of audit, investigative, or other authority.

CHAPTER 1.0 - EXHIBITS

1-1 Organizational Chart of DHS

Exhibit 1-1, Organizational Chart of DHS



2.0 AUTHORITY AND ORGANIZATION

2.1 ESTABLISHMENT OF THE OFFICE OF THE INSPECTOR GENERAL

The Homeland Security Act (HSA) of 2002, PL No.107-296, as amended by PL No. 1087, established an OIG within DHS, "as provided in the Inspector General Act of 1978." 5 U.S.C.A. App. 3 (IG ACT). The IG Act created "independent and objective units to conduct and supervise audits and investigations relating to the programs and operations" of the agency" and to provide leadership and coordination ... for activities designed ... to prevent and detect fraud and abuse in such programs and operations." 5 U.S.C.A. App. 3 § 2. The Act also states that, "it shall be the duty and responsibility of each Inspector General ... to provide policy direction for and to conduct, supervise, and coordinate audits and ' investigations relating to the programs and operations in its agency." Further, each IG is authorized "to make such investigations within the agency as are, in the judgment of the Inspector General, necessary or desirable."

THE HSA ALSO PROVIDES THAT NOTWITHSTANDING ANY OTHER PROVISIONS OF LAW, IN CARRYING OUT THE DUTIES AND RESPONSIBILITIES SPECIFIED IN THIS ACT, THE INSPECTOR GENERAL OF THE DEPARTMENT OF HOMELAND SECURITY SHALL HAVE OVERSIGHT RESPONSIBILITY FOR THE INTERNAL INVESTIGATIONS PERFORMED BY ALL INTERNAL AFFAIRS COMPONENTS WITHIN THE DEPARTMENT.

2.2 ORGANIZATIONAL STRUCTURE

The OIG is headed by an Inspector General appointed by the President with the advice and consent of the United States Senate. The IG ensures a means for keeping the Secretary of DHS and the Congress fully and currently informed about problems and deficiencies relating to the administration of the programs and operations affecting DHS, and the necessity for, and progress of, corrective action. **(Exhibit 2-1)**

The OIG is organized into eight divisions:

Executive Offices (EO)
Office of Counsel (OC)
Office of Administrative Services (ADMIN)
Office of Audits (AUD)
Office of Emergency Management Oversight (EMO)
Office of Information Technology Audits (IT Audits)
Office of Inspections, Evaluations, and Special Reviews (ISP)
Office of Investigations (INV)

The IG Appoints:

- A Deputy Inspector General (DIG) who is responsible for the day-to-day operation of the OIG and acts for the IG in the IG's absence.

- A Deputy Inspector General (DIG) for Emergency Management Oversight, who is responsible for identifying fraud, waste and abuse related to disaster relief funds.

- A Counsel to the Inspector General (OC) who provides the IG with legal advice.

- Assistant Inspector General of Administrative Services (AIG ADMIN) who is responsible for all administrative functions such as personnel, budget, training, travel, and payroll.

- An Assistant Inspector General for Audits (AIGA) who is responsible for supervising the performance of auditing activities.

- An Assistant Inspector General for Information Technology Audits (AIGIT Audits) who is responsible for auditing/evaluating all issues relating to DHS information systems.

- An Assistant Inspector General for Inspections, Evaluations, and Special Reviews (AIGISP) who is responsible for the inspections of DHS activities to identify fraud, waste, abuse, or mismanagement and to develop recommendations for corrective action.

- An Assistant Inspector General for Investigations (AIGI) who is responsible for supervising the performance of all investigative activities and overseeing all DHS Internal Affairs units.

The Organizational Chart, Staffing Model, and Field Office Areas of Responsibility Map found at the end of this chapter identify the INV offices and their locations. **(Exhibits 2-2, 2-2A and 2-3)**

2.3 AUTHORITY TO ESTABLISH POLICY AND PROCEDURE

Official OIG policy and procedures relating to INV, including the instructions in this Special Agent Handbook (SAH), may be issued only under the authority of the IG, DIG, AIGI or their designee.

2.4 OFFICE OF INVESTIGATIONS (INV)

Mission Statement

Strengthen the Effectiveness and Efficiency of the Department of Homeland Security. Secure and Protect the Nation from Dangerous People and Dangerous Things. Protect the Civil Rights and Liberties of the Citizens, Immigrants, and Non-immigrants in the United States. Enforce and Enhance Departmental Priorities and Programs. Promote the OIG Law Enforcement Mission.

Investigative Strategies

Protect the Nation from Dangerous People and Dangerous Goods

- Open 100% of referrals of corruption or compromise of DHS employees or systems that relate to securing the nation's borders including the smuggling of drugs, weapons, and people.
- Open 100% of referrals of corruption of DHS employees or compromise the integrity of systems relating to the nation's federally regulated transportation systems.
- Open 100% of referrals of corruption or compromise of the immigration process.

Protect Civil Rights and Civil Liberties

- [redacted] of ICE detainee deaths, which involve suspicious or unusual circumstances
- Investigate credible referrals of the physical abuse of detainees, suspects, or prisoners
- [redacted] shooting incidents involving DHS employees (excluding accidental discharges which are absent unusual circumstance, e.g. personal injury).
- Investigate credible allegations of criminal abuse of Authority including, but not limited to those that result in deprivation of rights or large scale thefts.

Protect the Integrity of Departmental Programs, as well as the Assets, Information and Infrastructure of the Department

- Investigate significant Grant, Procurement and Contract fraud allegations
- Investigate FEMA fraud that involves contractors, claimants or FEMA employees
- Investigate gross misuse or abuse of Classified Information, Privacy Information, or Law Enforcement Information
- Investigate allegations of corruption or criminal misconduct of DHS employees in the processing of immigrant and non-immigrant documents
- Exercise oversight of DHS component element internal affairs investigations

Strengthen the DHS OIG Law Enforcement Mission

- Establish a reputation for Excellence by producing thorough and timely investigations and reports.
- Participate fully in Task Force operations involving Border Corruption, and work to promote a corporate identity as the agency associated with conducting DHS employee corruption investigations.
- Ensure recruitment, development and opportunity for a quality and diverse workforce and enhance employee communication.
- Administer a robust Training program with innovative training initiatives, and routinely evaluate operational needs in order to procure and maintain leading edge law enforcement equipment.
- Enhance relationship and communication with DHS Law Enforcement component Internal Affairs Offices to advance intelligence gathering and information sharing.

Investigative Standards

INV investigations will be conducted in accordance with the *Quality Standards for Investigations* issued by the Council of the Inspectors General on Integrity and Efficiency (CIGIE), and the Attorney General (AG) Guidelines for Offices of the Inspector General with Statutory Law Enforcement Authority (AG Guidelines). Copies of this handbook are made available to all OI Special Agents (SAs).

Investigations conducted by INV can result in criminal prosecutions, civil monetary penalties, administrative sanctions and personnel actions against offenders and act as a deterrent against those contemplating fraud against DHS bureaus/agencies.

2.5 LAW ENFORCEMENT AUTHORITY

SAs of the OIG are empowered with law enforcement authorities pursuant to 5 USC app. 3, the Inspector General Act of 1978 as amended, the Homeland Security Act of 2002, and AG Guidelines, dated December 8, 2003. **(Exhibit 2-4)**

These authorities may be exercised when reasonably related to the performance of the duties, functions, and responsibilities assigned to the Inspector General. Agents are authorized, therefore, in order to prevent and detect fraud and abuse in the programs and operations of, and official misconduct within, the DHS to:

- carry firearms;
- seek and execute arrest warrants;
- seek and execute search warrants;
- arrest without a warrant any person for any offense committed in their presence or for any felony offense if they have reasonable grounds to believe that the person to be arrested has committed or is committing such felony;
- serve subpoenas issued under authority of the Inspector General Act or issued by a federal grand jury or federal court;

- serve legal writs, summons, and complaints;
- have access to records, reports, audits, reviews, documents, papers, recommendations, and other material which relate to the programs and operations of the DHS;
- administer or take from any person an oath, affirmation, or affidavit.

2.6 PROCEDURES GOVERNING MEMORANDA OF UNDERSTANDING

A Memorandum of Understanding (MOU) committing the involvement and/or resources of more than one OIG division can be entered into only by the IG.

The IG, DIG or the AIGI may enter into an MOU with another governmental (or private sector) entity for the purpose of delineating responsibilities for handling particular cases or projects of mutual interest. Any Special Agent in Charge (SAC) seeking such an MOU should convey the proposal to the AIGI by memorandum.

Office of Counsel will review all proposed MOU.

MOUs affecting INV operations are maintained in the appropriate administrative file.

At the local level, SACs may enter into less formal agreements on working relationships and arrangements concerning joint investigative activity with other agencies. SACs will consult with the DAIGI, Field Operations, prior to entering into any written agreements.

2.7 CURRENT MEMORANDA OF UNDERSTANDING

The IG has entered into MOUs with DHS components and other agencies to prevent duplication of effort and ensure the most effective and efficient deployment of resources.

The MOU between the IG and the Under Secretary for Border and Transportation Security (BTS), dated March 25, 2003 **(Exhibit 2-5)**, and the MOU between the IG and the Director of the U.S. Citizenship and Immigration Services (CIS), dated April 17, 2003 **(Exhibit 2-6)**, provide that allegations of criminal misconduct and certain categories of serious non-criminal misconduct shall be referred to the IG for determination whether to conduct an investigation. The MOUs also provide that the IG, for certain categories of misconduct, will determine within one business day of the referral whether to investigate the allegation or refer that matter back to the component.

The IG and the Department of Justice (DOJ) Civil Rights Division, Criminal Section, have entered into an MOU pertaining to investigations of civil rights violations. (Chapter 19.0). **(Exhibit 2-7)**

The IG and the U.S. Coast Guard (USCG) have entered into an MOU pertaining to the investigation of allegations of criminal misconduct and certain categories of serious non-criminal misconduct. **(Exhibit 2-8)**

The IG and the U. S. Secret Service (USSS) have entered into an MOU pertaining to the investigation of allegations of criminal misconduct and certain categories of serious non-criminal misconduct. **(Exhibit 2-9)**

The IG and the Chief Privacy Officer (CPO) of the DHS have entered into an MOU pertaining to the coordination between the IG and the CPO regarding allegations of criminal misconduct and serious non-criminal misconduct. **(Exhibit 2-10)**

2.8 DHS MANAGEMENT DIRECTIVE

Not withstanding any MOU entered into by the OIG and other DHS components or agencies, on June 10, 2004, the Deputy Secretary for the Department of Homeland Security (DHS) issued Management Directive Number 0810.1 (MD 0810.1) which established the DHS policy regarding the scope and authorities of the OIG to include those categories of misconduct that must be reported to the OIG. (Chapter 7.4) MD 0810.1 further specifies that any instruction or agreement of any kind issued by or entered into by any DHS official or component that is inconsistent in any respect with this directive will be superceded, to the extent it is in consistent, with this directive**. (Exhibit 2-11)**

Further reference is made to the Secretary's Memorandum titled Cooperation with the Office of Inspector General, dated April 8, 2008, reminding all DHS employees of the requirement to cooperate fully with the OIG. **(Exhibit 2-12)**

2.9 ORGANIZATION OF THE OFFICE OF INVESTIGATIONS

INV consists of Headquarters Operations and Field Operations. Headquarters Operations is comprised of the Operations and Planning Division (OPD), Inspection Division (ISD), Special Investigations Division (SID) and Ombudsman. Field Operations consists of Field Offices (FO), Resident Offices (RAC) and Sub-Offices; and the Disaster Oversight and Operations Division (DOD).

2.10 HEADQUARTERS OPERATIONS

Headquarters Operations is supervised by a DAIGI and is responsible for:

Operations and Planning Division, which is supervised by a SAC and is responsible for the following:

- Overseeing and coordinating the INV budget and confidential fund, managing training (including firearms and defensive tactics), equipment and law enforcement database management.

Inspections Division, which is supervised by a SAC and is responsible for the following:

- Overseeing and conducting inspections of DHS internal affairs components,
- Desk Officers who maintain liaison with DHS components, review investigative referrals and coordinate responses to DHS components regarding disposition of allegations.
- Management of the Hotline and the complaint referral process.

Special Investigations Division, which is supervised by a SAC and is responsible for the following:

- Conducting sensitive investigations, to include allegations made against Presidential Appointees (PA), Presidential Appointees with Senate Confirmation (PAS), Congressional inquiries, and other matters deemed high interest by the IG or the AIGI.
- Conducting investigations on allegations against DHS OIG employees.
- Conducting routine periodic inspections of DHS OIG INV offices.

The Ombudsman Program and Committee is directed by a SAC and is responsible for ensuring an alternate channel of communication for employees to discuss or seek guidance about workplace concerns. The Ombudsman Committee consists of INV employees who volunteer and are trained to assist employees in resolving work-related issues or problems.

2.11 FIELD OPERATIONS

Field Operations is supervised by a DAIGI.

Disaster Oversight and Operations Division, which is supervised by a SAC and is responsible for the following:

- Ensure that INV is fully prepared to respond to all federally declared disasters
- Develop strategic plans and ensure that INV's disaster training needs are met
- Primary INV interface with OIG Emergency Management Oversight (EMO) and the Federal Emergency Management Agency (FEMA)
- Review all FEMA ROI's and manage cases from headquarters perspective

Each office is responsible for conducting investigations in assigned geographical areas as reflected in **Exhibit 2-3**.

Atlanta FO ATL

Biloxi	SO	BLX
Hattiesburg	SO	HAT
Mobile	SO	MOB
Chicago	FO	CHI
Dallas	FO	DAL
Baton Rouge	RAC	BTN
Detroit	FO	DET
El Paso	FO	ELP
Houston	FO	HOU
Del Rio	SO	DRT
McAllen	FO	MCA
Laredo	SO	LAR
Miami	FO	MIA
San Juan	RAC	SNJ
Orlando	SO	ORL
Philadelphia	FO	PHL
New York	SO	NYC
Boston	SO	BOS
Buffalo	SO	BUF
San Diego	FO	SND
El Centro	RAC	ELC
Los Angeles	RAC	LAX
San Francisco	FO	SFO
Seattle	FO	SEA
Bellingham	SO	BEL
Tucson	FO	TUC
Yuma	SO	YUM
Washington	FO	WFO

The OIG has the authority to investigate allegations involving DHS employees who are assigned to posts of duty outside of the Continental United States (CONUS). Field

Office jurisdiction will be determined based upon the CONUS post of duty of the employee's supervisor. Generally, that jurisdiction will correspond to the Field Office geographical area of responsibility as reflected in **Exhibit 2-3.**

CHAPTER 2.0 - EXHIBITS

2-1 OIG Organizational Chart

2-2 INV Organizational Chart

2-2A Investigations Office Staffing Model

2-3 Map of Field Office Regions

2-4 Attorney General Guidelines for Offices of the Inspector General with Statutory Law Enforcement authority, dated December 8, 2003

2-5 Memorandum of Understanding between the IG and the Under Secretary for Border and Transportation Security dated March 25, 2003

2-6 Memorandum of Understanding between the IG and the Director of the Bureau of Citizenship and Immigration Services, dated April 17, 2003

2-7 Memorandum of Understanding between the OIG and DOJ, Civil Rights Division, Criminal Section, dated September 22, 2003

2-8 Memorandum of Understanding between the OIG and the U.S. Coast Guard, dated August 5, 2003

2-9 Memorandum of Understanding between the OIG and the U.S. Secret Service, dated December 8, 2003

2-10 Memorandum of Understanding between the OIG and DHS Chief Privacy Officer, dated March 25, 2008

2-11 DHS Management Directive Number 0810.1, dated June 10, 2004

2-12 Memorandum from the DHS Secretary, dated April 8, 2008

Exhibit 2-1, OIG Organizational Chart

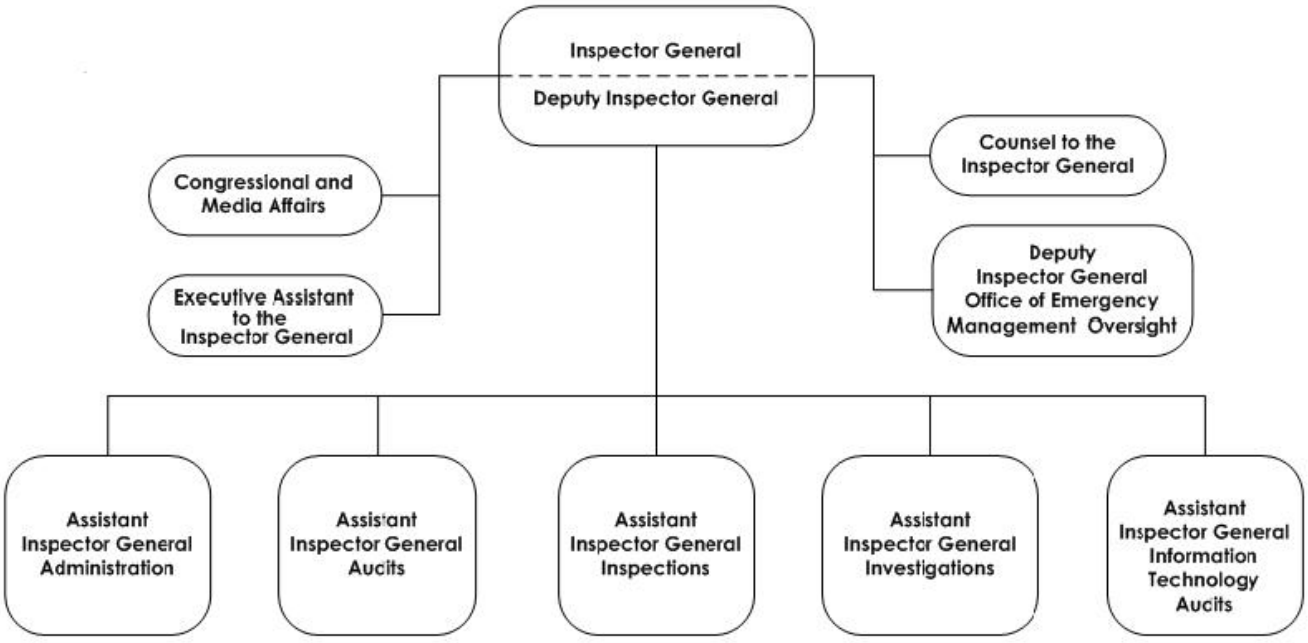


Exhibit 2-2, Investigations Organizational Chart

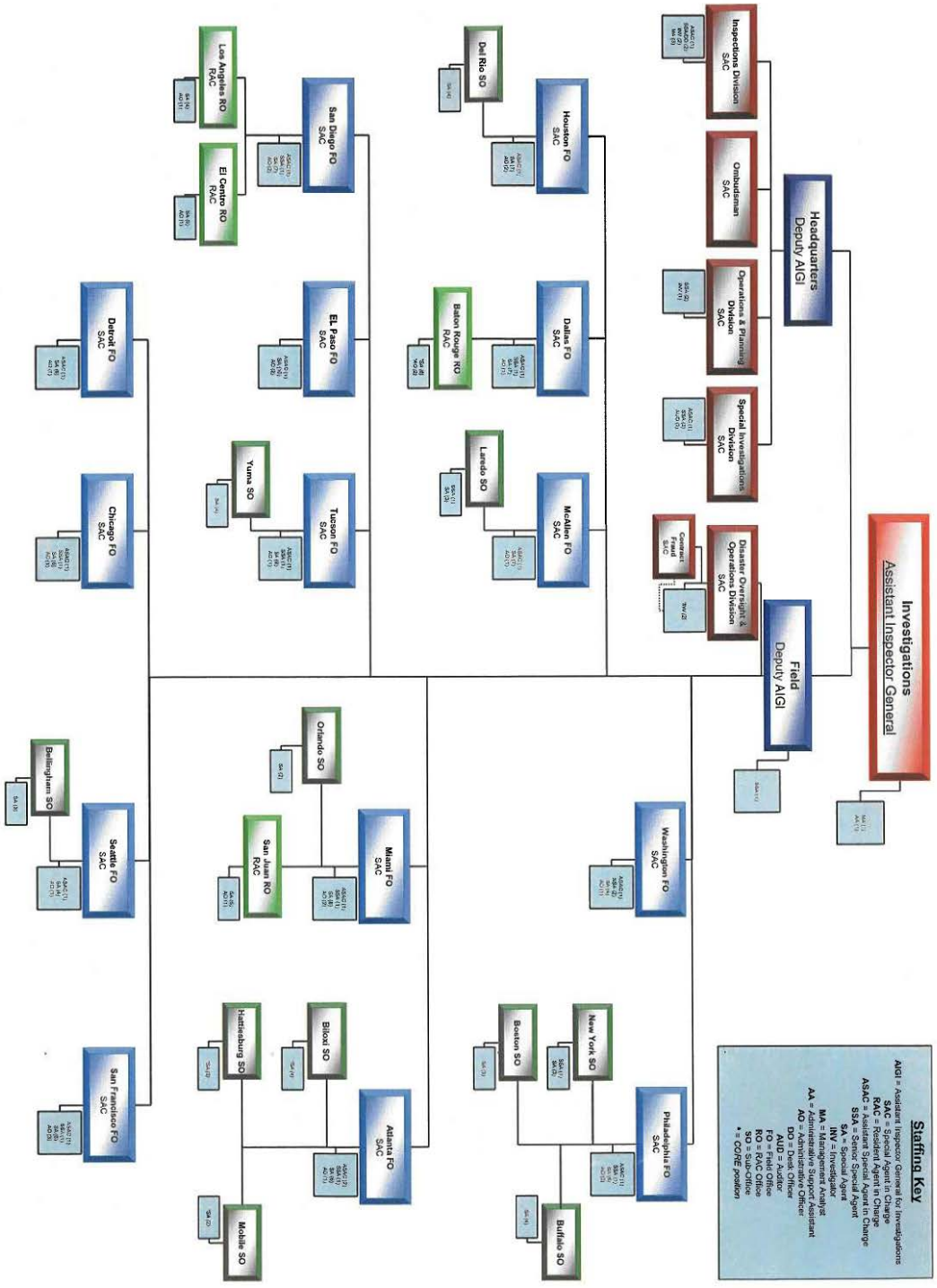


Exhibit 2-2A, Investigations Office Staffing Model

Field Office Model

SAC
ASAC
6 or more working SA (one of whom may be an SSA)
Administrative Officer

In addition, may have

Additional SAs (one SSA per 6 SAs)
Additional Administrative Support
STEP employee(s) as approved
RAC or Sub Office report

Resident Office Model

- RAC-Associate SAC
- 4-5 working SA
- Administrative Officer
- STEP employee as approved

Sub Office Model

- SSA working agent
- 1-3 additional working SA
- STEP employee as approved

Exhibit 2-3, Map of Field Office Regions

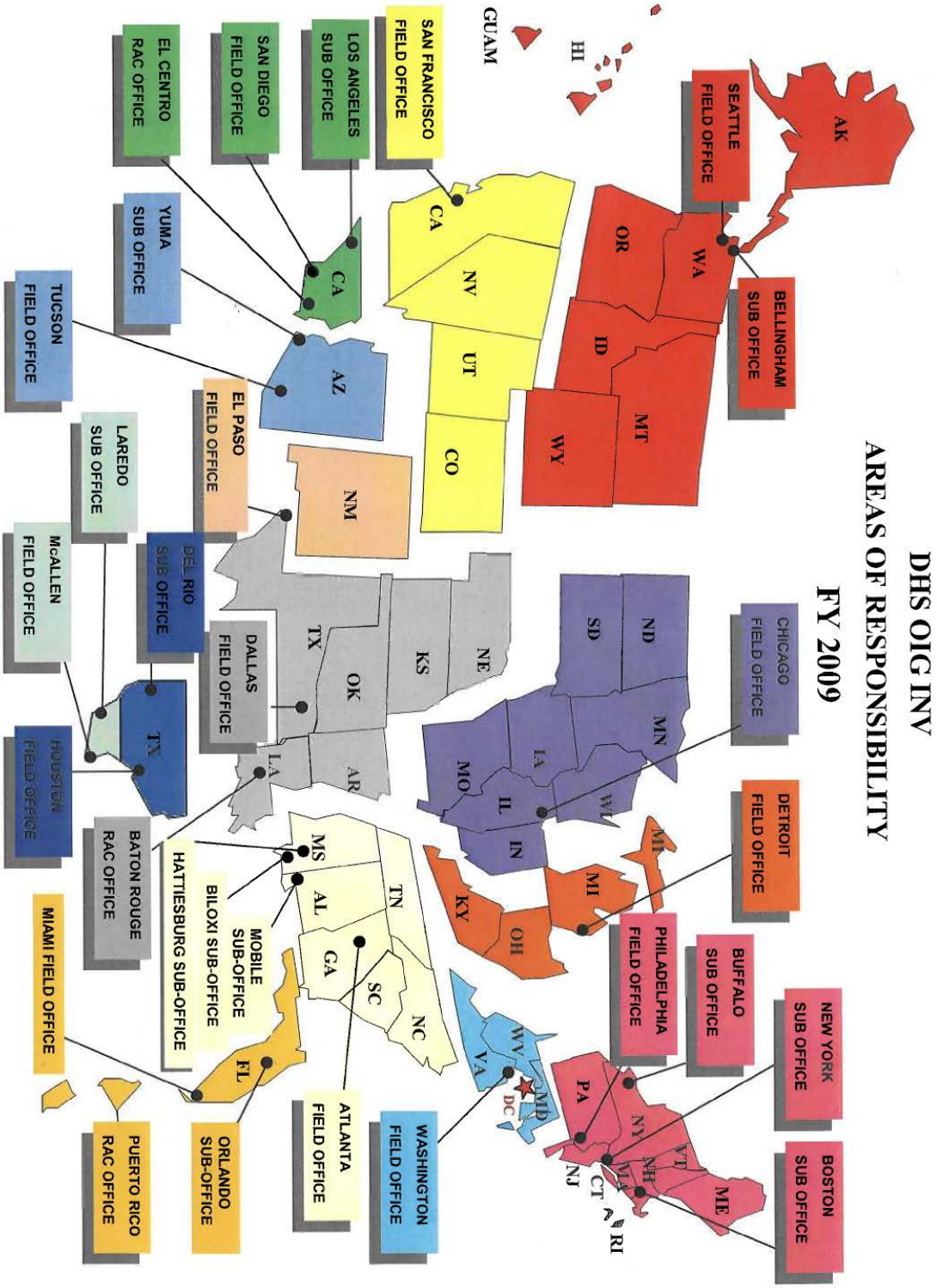


Exhibit 2-4, Attorney General Guidelines

Office of the Attorney General
Washington, D. C. 20530

ATTORNEY GENERAL GUIDELINES FOR OFFICES OF INSPECTOR GENERAL WITH STATUTORY LAW ENFORCEMENT AUTHORITY

I. PURPOSE

These guidelines, required by section 6(e)(4) of the Inspector General Act of 1978 (the "Act"), as amended in 2002, govern the exercise of law enforcement authorities for those Offices of Inspector General that have been granted statutory law enforcement authorities pursuant to that Act. These Guidelines replace the Memoranda of Understanding under which the Department of Justice deputized certain Office of Inspector General investigators as Special Deputy United States Marshals and that described the training and operational requirements applicable to the deputized Office of Inspector General investigators.

II. BACKGROUND

The Department of Justice has primary responsibility for enforcement of violations of federal laws by prosecution in the United States district courts. The Federal Bureau of Investigation is charged with investigating violations of federal laws. Offices of Inspector General have primary responsibility for the prevention and detection of waste and abuse, and concurrent responsibility for the prevention and detection of fraud and other criminal activity within their agencies and their agencies' programs. The Inspector General Act of 1978, 5 U.S.C. app. 3, established criminal investigative jurisdiction for the offices of presidentially appointed Inspectors General. However, prior to enactment of section 812 of the Homeland Security Act of 2002 (Pub. L. No. 107-296), the Inspector General Act did not provide firearms, arrest, or search warrant authorities for investigators of those offices.[1] The Inspectors General of the various executive agencies relied on Memoranda of Understanding with the Department of Justice that provided temporary grants of law enforcement powers through deputations. As the volume of investigations warranting such police powers increased, deputations were authorized on a "blanket" or office-wide basis.

With the enactment of section 6(e) of the Inspector General Act, the Attorney General, after an initial determination of need, may authorize law enforcement powers for eligible personnel of each of the various offices of presidentially appointed Inspectors General. The determination of

[1] Certain Offices of Inspector General had (prior to 2002) and continue to have OIG-specific grants of statutory authority under which they exercise law enforcement powers.

need hinges on the respective office meeting the three prerequisites enumerated in section 6(e)(2). Those Offices of Inspector General listed in section 6(e)(3) of the Act are exempt from the requirement of an initial determination of need by the Attorney General.

Offices of Inspector General receiving law enforcement powers under section 6(e) must exercise those authorities in accordance with Guidelines promulgated by the Attorney General. This document sets forth the required Guidelines.

III. APPLICATION OF GUIDELINES

These Guidelines apply to qualifying personnel in those offices of presidentially appointed Inspectors General with law enforcement powers received from the Attorney General under section 6(e) of the Inspector General Act of 1978, as amended. Qualifying personnel include the Inspector General, the Assistant Inspector General for Investigations under such Inspector General, and all special agents supervised by the Assistant Inspector General for Investigations, provided that those individuals otherwise meet the training and qualifications requirements contained in these Guidelines. These mandatory guidelines do not limit Offices of Inspector General from exercising any statutory law enforcement authority derived from a source other than section 6(e). These Guidelines may be revised by the Attorney General, as appropriate. These Guidelines may be supplemented by agency-specific agreements between an individual Office of Inspector General and the Attorney General.

If the Attorney General determines that an Office of Inspector General exercising law enforcement powers under section 6(e), or any individual exercising such authorities, has failed to comply with these Guidelines, the Attorney General may rescind or suspend exercise of law enforcement authorities for that office or individual.

IV. LAW ENFORCEMENT TRAINING AND QUALIFICATIONS

A Basic and Refresher Training

Each Office of Inspector General must certify completion of the Basic Criminal Investigator Training Program at the Federal Law Enforcement Training Center by each Inspector General, Assistant Inspector General of Investigations, and Special Agent/Investigator who will be exercising powers under these Guidelines. As an alternative, this training requirement may be satisfied by certification of completion of a comparable course of instruction to the Federal Law Enforcement Training Center Basic Criminal Investigator Training Program. Additionally, the Office of Inspector General will provide periodic refresher training in the following areas: trial process; federal criminal and civil legal updates; interviewing techniques and policy; law of arrest, search, and seizure; and physical conditioning/defensive tactics. The specifics of these programs should conform as much as

practicable to standards such as those set at the Federal Law Enforcement Training Center or the Federal Bureau of Investigation Training Academy at Quantico, Virginia.

B. Firearms Training and Qualification Requirements

All individuals exercising authorities under section 6(e) must receive initial and periodic firearms training and qualification in accordance with Federal Law Enforcement Training Center standards. This training will focus on technical proficiency in using the firearms the Special Agent will carry, as well as the policy and legal issues involved in the use of deadly force. The initial training for this requirement must be met by successful completion of an appropriate course of training at the Federal Law Enforcement Training Center or an equivalent course of instruction (that must include policy and law concerning the use of firearms, civil liability, retention of firearms and other tactical training, and deadly force policy).

In addition to basic firearms training, each covered Office of Inspector General will implement a program of quarterly firearms qualifications by all individuals exercising authorities under section 6(e). Such program will be conducted in accordance with recognized standards.

C. Deadly Force Policy

The Offices of Inspector General will abide by the deadly force policy established by the Department of Justice.

V. RANGE OF LAW ENFORCEMENT POWERS

Section 6(e) of the Act provides that the Attorney General may authorize covered individuals to:

1. carry a firearm while engaged in official duties as authorized under this Act or other statute, or as expressly authorized by the Attorney General;

2. make an arrest without a warrant while engaged in official duties as authorized under this Act or other statute, or as expressly authorized by the Attorney General, for any offense against the United States committed in the presence of such individual, or for any felony cognizable under the laws of the United States if such individual has reasonable grounds to believe that the person to be arrested has committed or is committing such felony; and

3. upon probable cause to believe that a violation has been committed, seek and execute warrants for arrest, search of a premises, or seizure of evidence issued under the authority of the United States.

Individuals exercising law enforcement authorities under section 6(e) may exercise those powers only for activities authorized under the Inspector General Act of 1978 or other statute, or as expressly authorized by the Attorney General.[2]

The Inspector General of each agency covered by these Guidelines, any Assistant Inspector General for Investigations under such Inspector General, and any special agent supervised by such an Assistant Inspector General are authorized to carry their firearms while off-duty when the Inspector General determines that they need to do so for operational or safety reasons.

The possession of firearms on aircraft while on official duty shall be governed by Transportation Security Administration guidelines and common carrier regulations applicable to the transport of firearms.

VI. ADHERENCE TO ATTORNEY GENERAL GUIDELINES

In addition to any other Department of Justice directives or guidance referenced in these Guidelines, Offices of Inspector General will adhere to the Attorney General's Guidelines on General Crimes, Racketeering Enterprise, and Terrorism Enterprise Investigations; the Attorney General's Guidelines Regarding the Use of Confidential Informants; the Attorney General's Memorandum on Procedures for Lawful, Warrantless Monitoring of Verbal Communications; any other Attorney General Guidelines applicable to criminal investigative practices; and updated or amended versions of any of the aforementioned documents.

VII. NOTIFICATION AND CONSULTATION REQUIREMENTS WITH RESPECT TO ALLEGATIONS OF CRIMINAL VIOLATIONS

The Inspector General Act directs expeditious reporting to the Attorney General whenever an Office of Inspector General has reasonable grounds to believe there has been a violation of federal criminal law.

A. Offices Of Inspector General/Federal Bureau of Investigation Mutual Notification Requirements

As the primary investigative arm of the Department of Justice, the Federal Bureau of Investigation has jurisdiction in all matters involving fraud against the Federal Government, and shares jurisdiction with the Offices of Inspector General in the

---

[2] Section 6(e) does not, of itself, provide plenary authority to make arrests for non-federal criminal violations. Legal authority for officers to respond to such offenses generally depends on state law. A federal agency may, however, as a matter of policy, permit its officers to intervene in serious criminal conduct that violates state law under certain circumstances.

investigation of fraud against the Office of Inspector General's agency. In areas of concurrent jurisdiction, the Offices of Inspector General and the Federal Bureau of Investigation must promptly notify each other in writing upon the initiation of any criminal investigation. The notification requirement is a continuing obligation when new subjects are added to an investigation. Absent exigent circumstances, "promptly" shall be considered to be within 30 calendar days. Notification by the Offices of Inspector General shall be in writing and addressed to the Federal Bureau of Investigation in the district in which the investigation is being conducted. Notification by the Federal Bureau of Investigation shall be in writing and shall be addressed to the appropriate regional office of the Office of Inspector General. Notifications shall include, at a minimum and where available, (a) subject name, date of birth, social security number, and (b) any other case-identifying information including, but not limited to, (i) the date the case was opened or the allegation was received, and (ii) the allegation that predicated the case. For investigations in which allegations arise that are beyond the scope of the Office of Inspector General's jurisdiction, the Office of Inspector General will immediately notify the appropriate investigative agency of the allegations.

B. Consultation with Prosecutors

In criminal investigations, a federal prosecutor must be consulted at an early stage to ensure that the allegations, if proven, would be prosecuted. Such consultation will also ensure coordination of investigative methods.

VIII. USE OF SPECIALIZED INVESTIGATIVE PROCEDURES AND TECHNIQUES

A. Court-Ordered Electronic Surveillance

Court-authorized interceptions of wire, oral, or electronic communications are among the most intrusive investigative techniques currently available to law enforcement. The rigors of the approval process, expenditures of financial and manpower resources, and the probability of challenges by the defense bar make this technique subject to intense scrutiny. Surreptitious electronic surveillance using closed-circuit television presents similar considerations. Accordingly, any investigation involving the interception of communications pursuant to 18 U.S.C. §§ 2510, *et seq.*, electronic surveillance using closed-circuit television in situations where a warrant is required, or any other court-ordered electronic surveillance, shall be conducted only after consulting with the Federal Bureau of Investigation and appropriate United States Attorney's Office (or Criminal Division litigating component). Subsequent to such notification, the Federal Bureau of Investigation may choose to join the investigation, but is not required to do so. However, in an instance in which the Office of Inspector General intends to engage in court-authorized electronic surveillance without the participation of the Federal Bureau of

Investigation, one of the following federal investigative agencies must participate in the investigation and supervise the application for and use of the surreptitious electronic surveillance: the Drug Enforcement Administration; Bureau of Alcohol, Tobacco, Firearms, and Explosives; Bureau of Immigration and Customs Enforcement; United States Postal Service; United States Secret Service; or Internal Revenue Service.

B. Undercover Investigative Operations

The Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations (the "Undercover Guidelines") ensure that the Federal Bureau of Investigation considers the efficacy, as well as the legal and policy implications, of every proposed undercover operation, and ensure that the use of the undercover investigative technique is subject to a management on-site review and oversight on a regular basis. It is the intent of this provision that undercover operations conducted by the Offices of Inspector General be subject to the same standards that govern the use of this investigative technique by the Federal Bureau of Investigation.

Accordingly, the community of Inspectors General granted law enforcement powers under section 6(e) of the Inspector General Act shall establish an Undercover Review Committee (the Committee) composed of 6 senior headquarters managers selected by the community of Inspectors General, with no two members of the Committee being employed by the same Office of Inspector General, for the purpose of reviewing undercover operations involving sensitive circumstances[3] in investigations that are not being conducted jointly with the Federal Bureau of Investigation. The Committee shall also include such representatives from the litigating sections of the Criminal Division of the Department of Justice as are designated by the Assistant Attorney General of the Criminal Division. If an undercover investigation being reviewed by the Committee is being conducted by an Office of Inspector General that is not represented on the Committee, a representative of that Office of Inspector General who is a senior management official shall be added as a full member of the Committee to review that undercover operation. The Federal Bureau of Investigation may designate a representative to participate in the Committee in a consultative role.

Before conducting an undercover operation lasting longer than six months, or involving any of the sensitive circumstances set forth in the Undercover Guidelines, the Office of Inspector General must first notify the Federal Bureau of Investigation. The Federal Bureau of Investigation may choose to join the investigation, in which case the

[3] "Sensitive circumstances" are set forth in the Undercover Guidelines, and include investigations involving certain public officials, a significant risk of violence, authorized criminal activity, operation of a proprietary business, the risk for significant civil liability, and other circumstances as defined in those Guidelines.

undercover operation would be subject to review by the Criminal Undercover Operations Review Committee of the Federal Bureau of Investigation. If the Federal Bureau of Investigation opts not to join the case, the undercover operation will be reviewed by the Committee. No undercover operation involving sensitive circumstances may be conducted without the approval of one of these committees.

The approval for each undercover operation involving sensitive circumstances must be renewed for each six-month period, or less, during which the undercover operation is ongoing. The standards of the Committee for approval of the undercover operation shall be the same as those set forth in the Undercover Guidelines. The Committee shall operate in the same fashion as the Criminal Undercover Operations Review Committee as outlined in the Undercover Guidelines.

Each Office of Inspector General whose law enforcement effort contemplates the use of the undercover investigative technique in investigations not involving the sensitive circumstances set forth above shall establish procedures that are consistent with the procedures established for such undercover investigations not involving sensitive circumstances as are set forth in the Undercover Guidelines.

C. Especially Sensitive Targets

(1) Upon notification pursuant to Part VII, Subpart A of these Guidelines, or otherwise, the Federal Bureau of Investigation may choose to join, but would not be required to join, any investigation that involves:

(a) especially sensitive targets, including a member of Congress, a federal judge, a member of the executive branch occupying a position for which compensation is set at Executive Level IV or above, or a person who has served in such capacity within the previous two years;

(b) a significant investigation of a public official for bribery, conflict of interest, or extortion relating to the official's performance of duty;

(c) a significant investigation of a federal law enforcement official acting in his or her official capacity; or

(d) an investigation of a member of the diplomatic corps of a foreign country.

(2) Investigations involving certain other classes of persons may result in serious security concerns, especially regarding the operation of the Federal Witness Security Program. Therefore, an Office of Inspector General investigation will be coordinated with the

Office of Enforcement Operations of the Criminal Division, Department of Justice, when the investigation:

(a) involves a person who is or has been a member of the Witness Security Program if that fact is known by the Office of Inspector General;

(b) involves a public official, federal law enforcement officer, or other government employee or contract employee who is or has been involved in the operation of the Witness Security Program;

(c) involves the use or targeting, in an undercover capacity, of a person who is in the custody of the Federal Bureau of Prisons or the United States Marshals Service, or is under Federal Bureau of Prisons' supervision; or

(d) involves the use or targeting, in an undercover capacity, of a Federal Bureau of Prisons employee, if any part of the activity will occur within the confines of, or otherwise would be likely to affect the security of, a Bureau of Prisons-administered facility.

Investigations that require coordination with the Office of Enforcement Operations pursuant to Part VIII, Subpart C.(2)(a)-(d) may be conducted without the participation of the Federal Bureau of Investigation. In such instances, notification of the investigation should not be made to any other agency without the explicit approval of the Office of Enforcement Operations.

D. Consensual Monitoring in Certain Situations

Consensual monitoring of conversations in some circumstances can present unusual problems. Accordingly, if the Office of Inspector General contemplates the use of consensual monitoring involving a consenting or non-consenting person in the custody of the Bureau of Prisons or the United States Marshals Service, the use of any type of consensual monitoring in the investigation, whether telephonic or non-telephonic, must be coordinated with the Office of Enforcement Operations at the Department of Justice.

Consistent with the Attorney General's Memorandum on Procedures for Lawful, Warrantless Monitoring of Verbal Communications, the use of any non-telephonic consensual monitoring in an Office of Inspector General investigation requires the prior approval of the Director or an Associate Director of the Office of Enforcement Operations if any of the following sensitive circumstances are present:

(a) the monitoring relates to an investigation of a member of Congress, a federal judge, a member of the Executive Branch occupying a position for which compensation is set at Executive Level IV or above, or a person who has served in such capacity within the previous two years;

(b) the monitoring relates to an investigation of the Governor, Lieutenant Governor, or Attorney General of any State, or Territory, or a judge or justice of the highest court of any State or Territory, and the offense investigated is one involving bribery, conflict of interest, or extortion relating to the performance of his or her official duties;

(c) any party to the communication is a member of the diplomatic corps of a foreign country;

(d) any party to the communication is or has been a member of the Witness Security Program and that fact is known to the agency involved or its officers;

(e) the consenting or non-consenting person is in the custody of the Bureau of Prisons or the United States Marshals Service; or

(f) the Attorney General, Deputy Attorney General, Associate Attorney General, any Assistant Attorney General, or the United States Attorney in the district where an investigation is being conducted has requested the investigating agency to obtain prior written consent before conducting consensual monitoring in a specific investigation.

IX. PROSECUTOR CONCURRENCE FOR CERTAIN TECHNIQUES

The use and control of informants, sources, and cooperating witnesses is recognized by the courts as lawful and often essential to the effectiveness of properly authorized law enforcement investigations. However, certain guidelines must be applied because the use of informants and cooperating witnesses may involve intrusion into the privacy of individuals, or cooperation with individuals whose reliability and motivation can be open to question. In the following situations, *inter alia*, the prior concurrence of a federal prosecutor must be obtained to avoid problems such as entrapment, danger to the public, and abuse of police authority:

1. when an informant is authorized to participate in criminal activities;

2. when an informant or cooperating witness is a person entitled to claim a federally recognized legal privilege of confidentiality, such as an attorney, member of the clergy, or psychiatrist;

3. when aggregate payments for services or expenses to be made to a source who could be a witness in a legal proceeding exceed $25,000; or

4. when the use of any member of the news media as a source is planned (and in such a situation the prior written approval of a federal prosecutor must be obtained).

X. RELATIONS WITH THE NEWS MEDIA

The Department of Justice has issued guidelines that prescribe policy and instructions concerning the release of information by Department of Justice employees relating to criminal and civil proceedings (*see* 28 C.F.R. § 50.2). Office of Inspector General personnel must familiarize themselves with and follow these guidelines. In addition, in the course of joint investigations between an Office of Inspector General and the Federal Bureau of Investigation, wherever a "news release" would be permitted pursuant to the guidelines noted above, the Office of Inspector General must coordinate the release with the Federal Bureau of Investigation and the Department of Justice.

XI. REPORTING REQUIREMENTS

Each Office of Inspector General shall make an annual written report to the Attorney General due on November 1 of each year, detailing the investigative and prosecutive activities of that Office of Inspector General. The report shall, at a minimum, contain information on the number of (1) federal criminal investigations initiated, (2) undercover operations undertaken, and (3) times any type of electronic surveillance was used. Additionally, the report shall provide information on all significant and credible allegations of abuse of authorities conferred by section 6(e)(1) of the Inspector General Act by Office of Inspector General investigative agents and what, if any, actions were taken as a result. The names of the agents need not be included in such report.

XII. PEER REVIEWS

In accordance with section 6(e)(7) of the Inspector General Act, covered Offices of Inspector General must implement a collective memorandum of understanding, in consultation with the Attorney General, under which each Office of Inspector General will be periodically reviewed by another Office of Inspector General or a committee of Offices of Inspector General. Reviews should occur no less often than once every 3 years. The purpose of the review is to ascertain whether adequate internal safeguards and management procedures exist to ensure that the law enforcement powers conferred by the 2002 amendments to the Inspector General Act are properly exercised. Results of the review will be communicated to the Attorney General, as well as to the applicable Inspector General.

XIII. NO THIRD-PARTY RIGHTS CREATED

These Guidelines are adopted for the purpose of the internal management of the Executive Branch. These Guidelines are not intended to, do not, and may not be relied upon to, create any rights, substantive or procedural, enforceable at law or in equity by any party in any matter civil or criminal, nor do these Guidelines place any limitations on otherwise lawful investigative or litigation prerogatives of the Department of Justice or otherwise lawful investigative prerogatives of the covered Offices of Inspector General.

Dec. 8, 2003
Date

John Ashcroft
Attorney General

Exhibit 2-5, MOU between IG and Under Secretary, BTS

MEMORANDUM OF UNDERSTANDING
BETWEEN
THE UNDER SECRETARY FOR BORDER AND TRANSPORTATION SECURITY
AND THE INSPECTOR GENERAL

The Under Secretary for Border and Transportation Security (USBTS) of the Department of Homeland Security (Department) is the head of the Directorate of Border and Transportation Security (BTS). USBTS' authority and responsibility are described in Title IV of the Homeland Security Act of 2002, as amended, (the Act) and include authority and responsibility acquired pursuant to Section 1512 of the Act and by delegation from the Secretary of the Department.

The Inspector General (IG) of the Department is the head of the Office of Inspector General. The IG's authority and responsibility are described in Title VIII, Subtitle B of the Act, as amended, and the Inspector General Act of 1978, as amended, and include authority and responsibility acquired pursuant to section 1512 of the Act.

To prevent duplication of effort and ensure the most effective, efficient and appropriate deployment of resources, the USBTS and the IG enter into this memorandum of understanding.

The following categories of misconduct shall be referred to the IG for its determination whether to conduct an investigation. The referral to the IG shall be made immediately upon receipt of the allegation and no investigation shall be conducted prior to the referral. The IG will determine within one business day of the referral whether to investigate the allegation itself or to refer the matter back to USBTS or one of its subordinate entities for investigation. This list is representative of the types of matters appropriate for IG investigation but is not intended to represent an exhaustive or all-inclusive identification of such matters:

- All allegations of criminal misconduct against a BTS employee;

- All allegations of serious, noncriminal misconduct against a law enforcement officer. "Serious, noncriminal misconduct" is conduct that, if proved, would constitute perjury or material dishonesty, warrant suspension as discipline for a first offense, or result in the loss of law enforcement authority. A "law enforcement officer" is defined as any individual who is authorized to carry a weapon, make arrests, or conduct searches;

- All allegations of noncriminal misconduct against employees at the GS-15, GM-15 level or higher, and all political and Schedule C appointees;

- All allegations of noncriminal misconduct against an employee in the internal affairs division of an entity under USBTS authority;

- All allegations regarding misuse or improper discharge of a firearm (other than accidental discharge during training, qualifying or practice);

- All allegations of fraud committed by contractors, grantees or other individuals or entities receiving Department funds or otherwise engaged in the operation of Department programs or operations;

- All allegations of visa fraud by BTS employees in the visa issuance process.

In addition, it shall be presumed that the IG will investigate allegations against individuals or entities who do not fit into the categories identified above if, in the judgment of the IG, the allegations reflect systemic violations, such as abuses of civil rights, civil liberties, or racial and ethnic profiling; serious management problems within the Department, or otherwise represent a serious danger to public health and safety.

With regard to categories of misconduct not specified above, USBTS or the entity receiving the allegation should initiate investigation upon receipt of the allegation, and shall notify in writing, within five business days, the IG's Office of Investigations of such allegation. The IG shall notify the USBTS or investigating entity if the IG intends to assume control or become involved in an investigation, but absent such notification, the USBTS or investigating entity shall maintain full responsibility for these investigations.

USBTS or any of its subordinate entities shall provide a monthly report to the IG on all open investigations. This report, at a minimum, shall identify the subject, the issues under investigation, the identity of the investigating agent, and the status of the investigation. USBTS or the subordinate entity shall provide the IG with a complete copy of the Report of Investigation, including all exhibits, at the completion of the investigation or upon referral of the matter to the Department of Justice for prosecution (either criminal or civil) or to a component of the Department to determine appropriate administrative action. USBTS also shall advise the IG promptly of the resolution of any such referrals. The IG shall have the right to request more frequent or detailed reports on any investigations and to reassert at any time exclusive authority or other involvement over any matter, whether or not initially referred by the IG to USBTS or presumptively within USBTS jurisdiction.

This MOU shall be effective upon the signature of both parties and shall remain in effect until revoked by one party, upon thirty day's written notice to the other.

Under Secretary for Border and
And Transportation Security

Dated: 3/25/03

Acting Inspector General

Dated: 3/25/03

Exhibit 2-6, MOU between IG and Bureau of Citizenship and Immigration Services

Special Agent Handbook
Chapter 2

Exhibit 2-6, MOU between IG and Director, BCIS

MEMORANDUM OF UNDERSTANDING
BETWEEN
THE DIRECTOR OF THE BUREAU OF CITIZENSHIP AND IMMIGRATION SERVICES AND THE INSPECTOR GENERAL

The Director of the Bureau of Citizenship and Immigration Services (Director) of the Department of Homeland Security (Department) is the head of the Bureau of Citizenship and Immigration Services (BCIS). The Director's authority and responsibility are described in Title IV, Subtitle E of the Homeland Security Act of 2002, as amended (the Act), and include authority and responsibility acquired pursuant to Section 1512 of the Act and by delegation from the Secretary of the Department.

The Inspector General (IG) of the Department is the head of the Office of Inspector General. The IG's authority and responsibility are described in Title VIII, Subtitle B of the Act, as amended, and the Inspector General Act of 1978, as amended, and include authority and responsibility acquired pursuant to section 1512 of the Act.

To prevent duplication of effort and ensure the most effective, efficient and appropriate deployment of resources, the Director and the IG enter into this memorandum of understanding.

The following categories of misconduct shall be referred to the IG for its determination whether to conduct an investigation. The referral to the IG shall be made immediately upon receipt of the allegation and no investigation shall be conducted prior to the referral. The IG will determine within one business day of the referral whether to investigate the allegation itself or to refer the matter back to the BCIS, one of its subordinate entities, or other appropriate DHS component for investigation:

- All allegations of criminal misconduct against a BCIS employee;
- All allegations of noncriminal misconduct against employees at the GS-15, GM-15 level or higher, all attorneys, and all political and Schedule C appointees;
- All allegations of noncriminal misconduct against an employee in the internal affairs division of an entity performing an internal affairs function for the Director;
- All allegations of fraud committed by contractors, grantees or other individuals or entities receiving Department funds or otherwise engaged in the operation of Department programs or operations;
- All allegations of fraud, corruption, or similar misconduct in the administration of immigration benefits by BCIS employees.

In addition, it shall be presumed that the IG will investigate allegations against individuals or entities who do not fit into the categories identified above if, in the judgment of the IG, the allegations reflect systemic violations, such as abuses of civil rights, civil liberties, or racial and ethnic profiling; serious management problems within the Department, or otherwise represent a serious danger to public health and safety.

With regard to categories of misconduct not specified above, the Director or the entity receiving the allegation should initiate investigation upon receipt of the allegation, and shall notify in writing, within five business days, the IG's Office of Investigations of such allegation. The IG shall notify the Director or investigating entity if the IG intends to assume control or become involved in an investigation, but absent such notification, the Director or investigating entity shall maintain full responsibility for these investigations.

BCIS or any of its subordinate entities shall provide a monthly report to the IG on all open investigations. This report, at a minimum, shall identify the subject, the issues under investigation, the identity of the investigating agent, and the status of the investigation. BCIS or the subordinate entity shall provide the IG with a complete copy of the Report of Investigation, including all exhibits, at the completion of the investigation or upon referral of the matter to the Department of Justice for prosecution (either criminal or civil) or to a component of the Department to determine appropriate administrative action. BCIS also shall advise the IG promptly of the resolution of any such referrals. The IG shall have the right to request more frequent or detailed reports on any investigations and to reassert at any time exclusive authority or other involvement over any matter, whether or not initially referred by the IG to the Director or presumptively within the Director's jurisdiction.

This MOU shall be effective upon the signature of both parties and shall remain in effect until revoked by one party, upon thirty day's written notice to the other.

Director of the Bureau of Citizenship and Immigration Services

Dated: April 17, 2003

Acting Inspector General

Dated: 4/8/03

Exhibit 2-7, MOU between IG and DOJ Civil Rights Division

Special Agent Handbook
Chapter 2

Exhibit 2-7, MOU between OIG and DOJ, Civil Rights Div. Criminal Section

MEMORANDUM OF UNDERSTANDING
BETWEEN THE U.S. DEPARTMENT OF JUSTICE,
CIVIL RIGHTS DIVISION, CRIMINAL SECTION (Criminal Section)
AND
THE U.S. DEPARTMENT OF HOMELAND SECURITY
OFFICE OF THE INSPECTOR GENERAL (DHS OIG)

1) Scope of Agreement

This memorandum is intended to cover the receipt, transmission, and investigation of complaints involving possible criminal misconduct by employees of the Department of Homeland Security which are within the jurisdiction of the Civil Rights Division Criminal Section.

2) Incidents to be Reported

This memorandum covers all incidents that suggest the possibility that the following conduct may have occurred under color of law:

a) Use of excessive force;
b) False arrest, planting evidence; or institution of false charges;
c) Coercion of a statement from a witness or arrestee;
d) Coerced sexual contact;
e) Shootings resulting in injury or death (other than unintentional discharges occurring during firearms training, cleaning of a weapon, or training exercises).

3) Method of Reporting

a) DHS OIG will maintain appropriate internal procedures to ensure that it receives timely notice of covered incidents from all agencies and bureaus within its jurisdiction.

b) Within 24 hours, or the next business day, of receiving notice of an incident, DHS OIG will fax to the Criminal Section at (202) 514-8336 a copy of the DHS OIG complaint form. Where possible, the complaint form should be accompanied by any official reports by governmental personnel concerning the incident; witness statements; and photographs and medical documentation of the victim's injuries. If other

Page 1 of 3

Special Agent Handbook
Chapter 2

information concerning the incident exists (such as videotapes), the existence of such other information should also be noted.

c) If the incident is a particularly sensitive or high profile matter, DHS OIG will immediately notify the appropriate Criminal Section Deputy Chief of the incident by telephone and/or email.

d) The Criminal Section will contact DHS OIG within 48 hours with a decision to initiate or decline a criminal investigation, or to request more information. If additional investigation is requested, the Criminal Section will notify DHS OIG within 48 hours after receipt of such information with a prosecutive decision.

4. Conduct of Investigations

a) If the decision is made to decline a criminal investigation, DHS OIG is free immediately to initiate an administrative investigation or take whatever further action is deemed appropriate.

b) If the Criminal Section decides to initiate a criminal investigation, any administrative proceedings shall be suspended pending the outcome of the criminal investigation.

c) When a criminal investigation is initiated, no compelled statement can be taken from any witness without the authorization of the Criminal Section.

d) When a criminal investigation is initiated, an initial investigative report should be forwarded to the Criminal Section as soon as it is completed or no later than 30 days after the date of the request for investigation. A status report updating the progress of the investigation should be sent every 30 days thereafter.

e) A criminal investigation into allegations of misconduct covered by ¶2 may be undertaken by investigators from DHS OIG, the FBI, or a combination of DHS OIG and the FBI. The composition of the criminal investigative team will be determined by DHS OIG and the FBI Civil Rights Unit.

Special Agent Handbook
Chapter 2

5. Prosecutive Decisions

a) As soon as practicable, the Criminal Section will determine and advise DHS OIG whether a matter under criminal investigation should be closed or presented to a federal grand jury for further investigation.

b) If the Criminal Section determines that a matter does not warrant presentation to a federal grand jury, the Criminal Section will refer the matter back to DHS OIG for administrative investigation and either close the criminal investigation or suspend it to await the results of the administrative investigation. In either case, DHS OIG may complete its administrative investigation, which may include obtaining compelled statements, without consultation with the Criminal Section. If at any time during the administrative investigation, DHS OIG becomes aware of information that suggests the resumption of a criminal investigation is warranted, DHS OIG will notify the Criminal Section. At the end of an administrative investigation of a matter that was previously investigated criminally, DHS OIG will notify the Criminal Section of the administrative action taken.

Albert N. Moskowitz
Section Chief
Criminal Section, Civil Rights Division
U.S. Department of Justice

Date 8/27/03

Clark Kent Ervin
Acting Inspector General
U.S. Department of Homeland Security

Date 9/22/03

Page 3 of 3

TEAMS & CONTACT INFORMATION
CRIMINAL SECTION, CIVIL RIGHTS DIVISION

SECTION CHIEF MARK J . KAPPELHOFF

(b) (6) Red	(b) (6) Blue	(b) (6) Yellow	(b) (6) Green
Alabama (1, 2, 3) Alaska (6) Arizona (8) Arkansas (9, 10) California (11,11E,12, 12C) Colorado (13) Connecticut (14) Delaware (15) District of Columbia(16) Florida (17, 17M, 18)	Georgia (19, 19M, 20) Hawaii (21) Idaho (22) Illinois (23, 24, 25) Indiana (26, 26S) Iowa (27, 28) Kansas (29) Kentucky (30, 31) Louisiana (32,32M,33) Maine (34) Maryland (35) Massachusetts (36) Michigan (37, 38) Minnesota (39) Mississippi (40, 41)	Missouri (42, 43) Montana (44) Nebraska (45) Nevada (46) New Hampshire (47) New Jersey (48) New Mexico (49) New York (50, 51, 52, 53) North Carolina (54,54M, 55) North Dakota (56) Ohio (57, 58) Oklahoma (59, 60) Oregon (61) Pennsylvania (62, 63, 64) Puerto Rico (65) Rhode Island (66)	South Carolina (67) South Dakota (69) Tennessee (70, 71, 72) Texas (73, 74, 75, 76) Utah (77) Vermont (78) Virginia (79, 80) Washington (81, 82) West Virginia (83, 84) Wisconsin (85, 86) Wyoming (87) Virgin Islands (90) Guam (91) American Samoa (94)
ATTORNEYS (b) (6)	**ATTORNEYS** (b) (6)	**ATTORNEYS** (b) (6)	**ATTORNEYS** (b) (6)

Revised: 4/2/08

Human Trafficking Prosecution Unit
Robert Moossy, Director
(b) (6) Chief Counsel (detail)
pecial Litigation Counsel
Special Litigation Counsel

Attorneys
(b) (6)

Victim/Witness Coordinators
(b) (6)

Administrative Deputy
(b) (6)

Special Litigation Counsels
(b) (6)

Special Legal Counsel
(b) (6)

Mailing Address
950 Pennsylvania Avenue, NW
Washington, DC 20530
Main Phone: (202) 514-3204 & Fax: (202) 514-8336

Street Address
(b) (6)

Exhibit 2-8, MOU between OIG and DOJ, Civil Rights Div. Criminal Section

MEMORANDUM OF UNDERSTANDING BETWEEN THE UNITED STATES COAST GUARD AND THE OFFICE OF THE INSPECTOR GENERAL OF THE DEPARTMENT OF HOMELAND SECURITY

I. PARTIES

The parties to this Memorandum of Understanding (MOU) are the United States Coast Guard (USCG) and the Office of Inspector General (OIG) of the Department of Homeland Security (DHS).

II. PURPOSE

This MOU's purpose is to describe the roles and relationship between the USCG and OIG relating to the conduct of investigations. To prevent duplication of effort and ensure the most effective, efficient and appropriate deployment of resources, the USCG and the OIG enter into this MOU.

III. AUTHORITY

a. Agreements between the USCG and the OIG are permitted under the authority of 14 U.S.C. 141.

b. The USCG derives its authority to perform the responsibilities described in this MOU from sections 103(c) and 888 of the Homeland Security Act of 2002, as amended, (the DHS Act), the Uniform Code of Military Justice (10 U.S.C. 801 *et. seq.*,), 14 U.S.C. 2, 89, 93, 95 and 46 U.S.C. Chapter 63, among others.

c. The OIG exercises authorities and responsibilities specified in sections 103(b) and 811 of the DHS Act, as amended, and in the Inspector General Act of 1978, Pub.L. No. 95-452 (5 U.S.C. App. 3), as amended.

IV. COORDINATION AND COOPERATION

The USCG and the OIG shall implement the provisions of this MOU using their best efforts, in a spirit of cooperation, recognizing that maximum communication and coordination are essential for success. Such coordination is critical in those areas where investigative jurisdiction may overlap to ensure that a comprehensive DHS effort is made to address any instances of wrongdoing. Where combined resources can create efficiencies in the investigative process, these combined resources should be used whenever appropriate.

V. BACKGROUND AND PURPOSE

a. The USCG is the nation's primary law enforcer in the maritime arena. It enforces or assists in the enforcement of all applicable U.S. laws on, over, and under the

high seas and waters and vessels subject to U.S. jurisdiction. Under the above referenced authorities, the USCG has regulatory, investigative, and enforcement responsibilities in the following mission areas: counter-narcotics, illegal immigration, living marine resources (including fisheries), environmental crimes (including waterborne shipment of hazardous materials), recreational boating safety enforcement (including boating while intoxicated), enforcement of marine safety and navigation laws (including vessel documentation and merchant mariner licensing), firearms laws, and, to a lesser extent, investigation and enforcement of "common law" Federal crimes such as murder, assault, and rape committed in a maritime environment as well as the investigation of offenses under the Uniform Code of Military Justice (UCMJ) committed by persons who are subject to the Code.

b. USCG investigative authority includes all necessary authority to conduct inquiries and examinations leading to criminal, civil, and administrative actions. To carry out its diverse missions, the USCG may request assistance from any Federal or State agency having capabilities useful to the USCG. Further, Federal or State agencies may request USCG investigative or enforcement assistance when needed.

c. The OIG is responsible for conducting, supervising, coordinating, and providing policy guidance for the conduct of criminal, civil, and administrative investigations relating to DHS programs and operations, as specified in section 4(a)(1) of the Inspector General Act of 1978 ("the IG Act"), as amended.

d. Under section 3(a) of the IG Act and section 811 of the DHS Act, the Inspector General reports to, and is under the general supervision of the DHS Secretary and Deputy Secretary. Section 4 of the IG Act provides additional reporting requirements applicable to the Inspector General. Section 4(a)(5) requires that the Inspector General keep the Secretary and the Congress fully and currently informed concerning fraud and other serious problems relating to the administration of DHS programs. Section 4(d) of the IG Act requires that the Inspector General report expeditiously to the Attorney General whenever the Inspector General has reasonable ground to believe a violation of criminal law may have occurred.

e. Given the broad investigative authority and jurisdiction of both the USCG and the OIG, which may overlap to some extent, this MOU clarifies the distinct investigatory roles of the parties and provides guidance for cooperative investigations under 14 U.S.C. 141 and sections 6(a)(1), 6(a)(3), and 6(b)(1) of the IG Act.

VI. DEFINITIONS

For the purposes of this MOU:

a. "External field investigation" means an investigation that has as its subjects persons other than employees, military personnel, members of the Coast Guard Auxiliary, contractors, borrowers, grantees or others receiving DHS funds or otherwise

engaged in programs and operations of DHS. For OIG, an external field investigation may also be an investigation conducted on behalf of another agency.

b. "Internal investigation" means an investigation that has as one of its subjects employees, military personnel, members of the Coast Guard Auxiliary, contractors, borrowers, grantees or others receiving DHS funds or otherwise engaged in programs and operations of DHS.

c. "Military personnel" means members of the USCG subject to the UCMJ and Department of Defense or any other Federal agency personnel who are subject to the UCMJ and detailed to perform duties with the USCG.

VII. COORDINATION OF USCG EXTERNAL FIELD INVESTIGATIONS

a. Since the USCG has statutory responsibilities to conduct various investigations described in paragraph V-a above, the USCG shall assume the lead role in coordinating investigative functions in support of its mission area responsibilities. The USCG may request assistance from the OIG under 14 U.S.C. 141 in the conduct of its investigations if OIG expertise in a particular area would benefit the investigation or if OIG's investigatory resources are needed to supplement available USCG resources. In such cases, the USCG will retain the lead on such investigations.

b. In the event the OIG receives initial information from any source outside the USCG concerning allegations of wrongful conduct in areas of USCG mission area responsibilities, the OIG will forward the information to the Director, Coast Guard Investigative Service (CGIS), 4200 Wilson Boulevard, Suite 740, Arlington, VA 22203, Phone: (202) 493-6600 and Facsimile: (202) 493-6619. Director, CGIS shall review the information referred by the OIG and determine whether the issues or allegations warrant investigation by CGIS or referral to the appropriate Coast Guard command or staff element for action or investigation and disposition. CGIS shall review copies of all Coast Guard investigations conducted in response to an OIG referral prior to the submission of a Coast Guard report to OIG. Director, CGIS shall coordinate Coast Guard requests for any specialized or criminal investigative assistance related to such OIG referrals.

c. If the OIG desires to remain involved in an investigation after making a referral, Director, CGIS shall work with the OIG to coordinate OIG's continued participation.

d. This section does not limit OIG's authority to conduct audits, assessments or investigations involving its oversight responsibilities for USCG personnel, policies, or procedures.

e. If the Department of Justice or a multi-agency task force asks the OIG to conduct an external field investigation in a USCG mission area, as described in paragraph V-a above, the OIG shall promptly notify the CGIS under the procedures described in paragraph VII-b above, so that the investigative activities of the two parties may be

appropriately coordinated. The OIG shall cooperate with the CGIS in the conduct of the investigation in a manner that is mutually agreed upon by the parties. The OIG shall notify the Department of Justice or the task force that the USCG has already initiated an investigation.

VIII. COORDINATION OF OIG EXTERNAL FIELD INVESTIGATIONS

a. The OIG shall assume the lead role in coordinating investigative functions in support of its investigative responsibilities described in paragraph V-c above. The OIG may request assistance from the USCG under 14 U.S.C. 141 in conducting its investigations if USCG expertise in a particular area would benefit the investigation or if USCG investigatory resources are needed to supplement available OIG resources. If the OIG chooses, it will retain the lead on the investigation. It may also refer a matter of direct interest to the USCG as provided in paragraph VII-b.

b. In the event the USCG receives initial information from any source outside the OIG concerning allegations of wrongful conduct in areas of OIG investigative responsibilities, Director, CGIS will forward the information to the OIG for evaluation or investigation. Director, CGIS shall also refer to the OIG all allegations of suspected violations that constitute fraud, waste, mismanagement, or abuse relating to the programs and operations of the USCG or DHS, except as noted in paragraph IX-c below. The referral to the OIG shall be made immediately upon receipt of the allegation, and no USCG investigation shall be conducted prior to the referral. However, the USCG need not refer to OIG incidents such as false official statements made in the course of a USCG boarding or inspection, if the USCG will deal with such statements in the ordinary course of its own investigation. Examples of suspected violations generally within the range of activity that the USCG must refer to the OIG for evaluation or investigation are listed below. These examples are illustrative of the types of matters that the USCG must refer to the OIG. They are not intended to represent an exhaustive or all-inclusive identification of such matters:

(1) False or fraudulent claims, statements, or certifications by employees, contractors, borrowers, grantees or others receiving DHS funds or otherwise engaged in the operation of DHS programs.

(2) False or fraudulent claims for payment involving goods or services not delivered or involving the delivery of nonconforming goods.

(3) Unlawful manipulation of the competitive bidding process.

(4) Unauthorized concealment, removal, obliteration, alteration or destruction of official documents.

(5) Misappropriation or embezzlement of Government funds or conversion of Government property or Government-funded property.

(6) Unauthorized use or fraud involving Government issued purchase or travel cards.

(7) Bribery or corruption of Government employees or officials.

(8) Conflicts of interest, including violations of Standards of Ethical Conduct.

(9) Allegations against individuals or entities who do not fit into the categories identified above if, in the judgment of the OIG, the allegations reflect systemic violations, such as abuses of civil rights, civil liberties, or racial or ethnic profiling; serious management problems within the Department, or otherwise represent a serious danger to public health and safety.

c. For the matters listed above, the Inspector General will determine within three business days of the referral whether to investigate the allegation itself or to refer the matter back to the CGIS for investigation.

d. In the event that an OIG external field investigation also involves areas of USCG mission area responsibilities, as described in paragraph V-a, the OIG and the CGIS shall coordinate investigative functions on a case-by-case basis.

IX. COORDINATION OF INTERNAL INVESTIGATIONS

a. The OIG shall lead internal investigations involving allegations of fraud, waste or abuse (including theft and corruption) committed by USCG civilian employees, members of the Coast Guard Auxiliary or non-affiliated civilians unless OIG elects to refer such matters to the USCG for appropriate action. Director, CGIS shall forward all such allegations to OIG.

b. The OIG shall lead internal investigations involving the alleged criminal misconduct of GS-15 or comparable level senior civilian employees, members of the Senior Executive Service, political appointees, and military personnel above the rank of Captain (O-6) unless the OIG elects to refer the matter to the USCG for appropriate action. Director, CGIS shall forward all such allegations to OIG.

c. CGIS may investigate and prosecute any incident or suspected incident of fraud, waste or abuse involving military personnel, provided that only military personnel are involved in such crimes as principals or accessories, and any principal victims are subject to the UCMJ. If the preceding conditions are not met, the CGIS shall promptly refer such offenses to the OIG for investigation.

d. If OIG elects to refer a DHS Hotline Complaint, the Director, CGIS, shall be the appropriate point of contact for such referrals.

X. REPORTING AND NOTIFICATION REQUIREMENTS

a. Director, CGIS shall provide a quarterly report to OIG describing the status of all open Hotline Complaint investigations conducted under paragraph IX-d above. The report, at a minimum, shall identify the subject, the case control number, the Hotline Complaint number, a brief description of the investigative results, and the projected completion date if the case is still on-going. Director, CGIS shall provide copies of all completed investigations, to include case disposition and prosecution action taken, for those Hotline Complaints referred to the USCG by the OIG for action. If the matter has been referred to the Department of Justice or to the United States Attorney's Office for civil or criminal proceedings, the report shall also describe the resolution of any such referrals.

b. Subject to the limitations in section 811 of the DHS Act, as amended, the OIG shall retain the right to request more frequent or detailed reports on any investigations and to reassert at any time exclusive authority or other involvement over any matter, whether or not initially referred by the OIG to the USCG or presumptively within the USCG's jurisdictional authority.

XI. COORDINATION OF REFERRAL OF CRIMINAL CASES TO THE DEPARTMENT OF JUSTICE

a. In cases where a significant potential for criminal prosecution exists, early involvement of the Department of Justice (DOJ) and/or the cognizant United States Attorney's Office (USAO) is desirable to ensure timely, effective and efficient use of investigative resources. However, the formal criminal referral process described in 33 CFR 1.07-90 for the USCG and in 5 U.S.C. App. III 4(d) for the OIG is an important part of the decision making process, designed to ensure that the policy interests of the USCG and the OIG are protected. DOJ and/or the appropriate USAO remain the ultimate decision maker on whether to prosecute a case. If doubt exits, the parties to this MOU will refer the matter to DOJ and/or the USAO.

b. For cases where either the USCG or the OIG has the investigative lead, as determined by paragraph VII-IX above, that party shall also have the lead in determining whether a referral should be made. In cases where the party supporting the investigation does not concur with the referral decision, the parties shall follow the procedures in paragraph XI-c.

c. For cases where both the USCG and OIG are investigating concurrently, either the OIG or the USCG may make a referral. However, before such action every effort should be made to communicate and coordinate the decision to make a referral with the other concerned party. Consensus on the form of the referral should be reached whenever feasible. If consensus cannot be reached, a full explanation of the different views of each party should be described in the referral.

XII. OTHER PROVISIONS

This MOU is not intended to limit the jurisdiction of the parties, or to conflict with current law, regulations or directives of DHS, the USCG, or the OIG. If a term of this MOU is inconsistent with such authority, then that term shall be invalid, but the MOU's remaining terms and conditions shall remain in full force and effect. Paragraph headings are for convenience only and shall not be used in construing this memorandum. This document represents the entire agreement between the parties.

XIII. EFFECTIVE DATE

This MOU shall become effective when approved and signed by both parties and shall remain in effect until revoked by either party, upon thirty day's written notice to the other party.

XIV. MODIFICATION

Either party may request modification of this MOU at any time, and it shall be modified upon mutual written consent of both parties.

XV. APPROVED BY

Admiral T. H. Collins
Commandant
United States Coast Guard

Date: 7/21/03

Clark Kent Ervin
Acting Inspector General
Department of Homeland Security

Date: 8/5/03

Exhibit 2-9, MOU Between OIG and U.S. Secret Service

MEMORANDUM OF UNDERSTANDING
BETWEEN
THE UNITED STATES SECRET SERVICE
AND THE OFFICE OF THE INSPECTOR GENERAL
DEPARTMENT OF HOMELAND SECURITY

The United States Secret Service (USSS), an organizational component of the Department of Homeland Security (DHS), operates within the Department under the authority and responsibilities enumerated in Title VIII, Subtitle C of the Homeland Security Act of 2002, as amended (the Act), and includes those responsibilities described generally in Section 1512 of the Act, as well as in various delegations of authority issued by the Secretary of DHS (the Secretary). The agency's dual statutory missions of protection and criminal investigations are more fully enumerated at Title 18, United States Codes, Section 3056 (Section 3056), and Title 3, United States Code, Section 202 (Section 202), and various other statutes.

The Office of the Inspector General (OIG), an organizational component of DHS, operates within the Department under the authority and responsibilities enumerated in Title VIII, Subtitle B of the Act, as amended, and the Inspector General Act of 1978, as amended, and includes authority and responsibility acquired pursuant to Section 1512 of the Act.

To prevent duplication of effort and ensure the most effective, efficient and appropriate use of resources, the Secret Service and the OIG enter into this Memorandum of Understanding.

The categories of misconduct listed below shall be referred to the OIG. Such referrals shall be transmitted by the USSS Office of Inspection immediately upon the receipt of adequate information or allegations by the USSS Office of Inspection to reasonably conclude that misconduct may have occurred, and no investigation shall be conducted by the USSS Office of Inspection prior to the referral. In cases involving exigent circumstances, if the OIG decides to investigate the allegation but is unable to do so immediately, the USSS Office of Inspection will conduct the investigation until the OIG is able to take it over. In cases not involving exigent circumstances, the OIG will determine within one business day of the referral whether to investigate the allegation itself or to refer the matter back to the USSS Office of Inspection for investigation. If no determination is communicated to the USSS Office of Inspection within one business day of the referral, the USSS Office of Inspection may initiate the investigation. The acceptance of a referral by the OIG reflects a determination that available investigative resources will be able to conclude the referred investigation within a reasonable time. This will afford the agency a reasonable opportunity to act expeditiously, if necessary, regarding the allegations.

All allegations of criminal misconduct against a USSS employee;

All allegations of misconduct against employees at the GS-15, GM-15 level or higher, or against employees in the USSS Office of Inspection;

All allegations regarding misuse or improper discharge of a firearm (other than accidental discharge during training, qualifying or practice);

All allegations of fraud by contractors, grantees or other individuals or entities receiving Department funds or otherwise engaged in the operation of Department programs or operations.

In addition, the IG will investigate allegations against individuals or entities who do not fit into the categories identified above if the allegations reflect systemic violations, such as abuses of civil rights, civil liberties, or racial and ethnic profiling; serious management problems within the Department, or otherwise represent a serious danger to public health and safety.

With regard to categories of misconduct not specified above, the USSS Office of Inspection should initiate investigation upon receipt of the allegation, and shall notify within five business days the OIG's Office of Investigations of such allegation. The OIG shall notify the USSS Office of Inspection if the OIG intends to assume control or become involved in an investigation, but absent such notification, the USSS Office of Inspection shall maintain full responsibility for these investigations.

Pursuant to Section 811(a) of the Act, OIG audits, investigations, and subpoenas which, in the Secretary's judgment, constitute a serious threat to the protection of any person or property afforded protection pursuant to Section 3056 or Section 202, or any provision of the Presidential Protection Assistance Act of 1976, may be prohibited. Accordingly, to assure proper and timely responses to OIG requests for information or records, all OIG plans for audits involving the Secret Service shall be communicated via entrance letter by the OIG either directly to the USSS Office of Inspection or to the Office of the Deputy Director; any OIG investigation shall be communicated orally or via e-mail to the same entities. Any Secret Service Headquarters' concern under section 811(a) regarding the scope or direction of a planned audit or investigation will be raised and resolved expeditiously with OIG officials, or immediately communicated to the Secretary in the absence of resolution.

The USSS Office of Inspection shall provide a monthly report to the OIG on all open investigations. In addition, the USSS Office of Inspection, upon request, shall provide the OIG with a complete copy of the Report of Investigation, including all exhibits, at the completion of the investigation. Similarly, the OIG shall provide the USSS Office of Inspection, upon request, with a complete copy of any Report of Investigation relating to the Secret Service, including all exhibits, at the completion of the investigation. The OIG shall have the right to request more frequent or detailed reports on any investigations and to reassert at any time exclusive authority or other involvement over any matter within its jurisdiction.

This MOU shall be effective upon the signature of both parties and shall remain in effect until revoked by one party upon thirty day's written notice to the other.

W. Ralph Basham
Director of the United States Secret Service
Dated: 12/5/03

Acting Inspector General
Dated: 12/8/03

Exhibit 2-10, MOU Between the Chief Privacy Officer and the Inspector General

MEMORANDUM OF UNDERSTANDING BETWEEN THE CHIEF PRIVACY OFFICER AND THE INSPECTOR GENERAL

I. The Parties

A. The Chief Privacy Officer (CPO) of the Department of Homeland Security is the head of the Privacy Office. The CPO's authority and responsibility are described in Title II of the Homeland Security Act of 2002, as amended, (the Act) and include authority and responsibility acquired by delegation from the Secretary of the Department.

B. The Inspector General (IG) of the Department is the head of the Office of Inspector General. The IG's authority and responsibility are described in Title VIII, Subtitle B of the Act, as amended, and the Inspector General Act of 1978, as amended.

II. Purpose of MOU

Pursuant to section 802(c) of the Implementing the Recommendations of the 9/11 Commission Act of 2007, which requires coordination between the CPO and the IG, this memorandum of understanding is intended to establish procedures for coordination between the Parties.

III. Coordination on Investigations.

To prevent duplication of effort and ensure the most effective, efficient, and appropriate deployment of resources, the CPO and the IG enter into this memorandum of understanding.

Before initiating any investigation relating to possible violations or abuse concerning the administration of any program or operation of the Department affecting privacy, the CPO shall refer the matter and all related complaints, allegations, and information to the IG (including a copy of any complaint). The information will be provided to the IG as soon as possible but no later than 30 days following receipt of the allegation. The IG will determine as soon as possible, but no later than 30 days after receiving the referral, whether to investigate the allegation itself, or to refer the matter back to the CPO for handling. This list is representative of the types of matters appropriate for IG investigation but is not intended to represent an exhaustive or all-inclusive identification of such matters:

- All allegations of criminal misconduct against a Department employee, contractor, grantee or other individual or entity receiving funds from the Department or engaged in Departmental programs or operations;

- All allegations of noncriminal misconduct against employees at the GS-15, GM-15 level or higher, and all political and Schedule C appointees.

In addition, it shall be presumed that the IG will investigate allegations against individuals or entities who do not fit into the categories identified above only if, in the judgment of the IG, the allegations reflect systemic violations; serious management problems within the Department, or otherwise represent a serious danger to public health and safety.

The IG will initiate investigation of any matter it retains within 90 days of the decision to investigate. If the IG has not initiated investigation by the 93rd day of such decision, he shall notify the CPO, who may determine to investigate the matter in lieu of the IG or to refer the matter elsewhere.

IV. IG Reporting

The IG shall provide a monthly report to the CPO identifying all allegations the IG has received that reflect possible violation or abuses concerning the administration or any DHS program or operation affecting privacy. This report, at a minimum, shall identify the subject(s) and the issue(s) under investigation by the IG. The CPO shall not provide a copy of this report to any other entity without express permission from the IG. The IG shall not report any information about any open investigation if, in the sole judgment of the IG, such reporting would be inappropriate or potentially deleterious to the rights of individuals or entities or to the conduct of the investigation.

V. Training

Any employee of the Office of Inspector General who audits or investigates any matter referred under Article III, shall receive adequate training on privacy laws, rules, and regulations, to be provided by an entity approved by the Inspector General in consultation with the CPO.

VI. Effective Date

This MOU shall be effective upon the signature of both parties and shall remain in effect until revoked by one party, upon thirty day's written notice to the other.

Chief Privacy Officer

Dated: 3-25-08

Inspector General

Dated: 3-25-08

Exhibit 2-11, DHS Management Directive Number: 0810, Inspector General

Department of Homeland Security
Management Directive System
MD Number: 0810.1

THE OFFICE OF INSPECTOR GENERAL

1. Purpose

This directive establishes Department of Homeland Security (DHS) policy regarding the Office of Inspector General (OIG). Any prior Management Directive and any instruction or agreement of any kind issued by or entered into by any DHS official or component that is inconsistent in any respect with this directive is hereby superseded to the extent it is inconsistent with this directive.

2. Scope

This directive applies to all DHS organizational elements (OEs), including all employees, contractors, and grantees.

3. Authorities

A. The Inspector General Act of 1978, as amended

B. The Homeland Security Act of 2002, as amended, codified in Title 6, US Code

4. Definitions

OE Offices - As used in this Management Directive, the term OE offices include all Organizational Element offices of internal affairs, inspections, audits or Professional Responsibility. This term also includes the DHS Office of Security.

DHS Organizational Element – As used in this directive, the term DHS Organizational Element (OE) shall have the meaning given to the term DHS Organizational Element in DHS MD 0010.1, Management Directives System and DHS Announcements. This includes Elements such as the Bureau of Customs and Border Protection, the United States Coast Guard, the Federal Emergency Management Agency, etc. It also includes entities that report to DHS Organizational Elements, such as National Laboratories.

5. Responsibilities

A. ***The heads of DHS Organizational Elements*** shall:

1. promptly advise the OIG of allegations of misconduct in accordance with the procedures described in Appendix A, and when they become aware of any audit, inspection or investigative work being performed or contemplated within their offices by or on behalf of an OIG from outside DHS, the General Accounting Office, or any other law enforcement authority, unless restricted by law;

2. ensure that, upon request, OIG personnel are provided with adequate and appropriate office space, equipment, computer support services, temporary clerical support and other services to effectively accomplish their mission;

3. provide prompt access for auditors, inspectors, investigators, and other personnel authorized by the OIG to any files, records, reports, or other information that may be requested either orally or in writing;

4. assure the widest possible dissemination of this directive within their OEs. They may issue further instructions as necessary to implement this policy. Any such further instructions shall not conflict with this MD and shall be provided to the OIG immediately upon issuance;

5. assist in arranging private interviews by auditors, inspectors, investigators, and other officers authorized by the OIG with staff members and other appropriate persons;

6. advise the OIG when providing classified or sensitive information to the OIG to ensure proper handling.

B. ***DHS employees*** shall report suspicions of violations of law or regulation to the DHS Office of Inspector General or the appropriate OE offices, and will likewise:

1. cooperate fully by disclosing complete and accurate information pertaining to matters under investigation or review;

2. inform the investigating entity of any other areas or activities they believe require special attention;

3. not conceal information or obstruct audits, inspections, investigations, or other official inquiries;

4. be subject to criminal prosecution and disciplinary action, up to and including removal, for knowingly and willfully furnishing false or misleading information to investigating officials; and

5. be subject to disciplinary action for refusing to provide documents or information or to answer questions posed by investigating officials or to provide a signed sworn statement if requested by the OIG, unless questioned as the subject of an investigation that can lead to criminal prosecution.

6. Policy and Procedures

A. The OIG, while organizationally a component of the DHS, operates independent of the DHS and all offices within it. The OIG reports to the Secretary. Under circumstances specified by statute, the Secretary, upon written notification to the OIG which then must be transmitted to Congress, can circumscribe the OIG's access to certain types of sensitive information and exercise of audit, investigative, or other authority. The DHS Inspector General is the head of the OIG.

The OIG is authorized, among other things, to:

1. administer oaths;

2. initiate, conduct, supervise and coordinate audits, investigations, inspections and other reviews relating to the programs and operations of the DHS;

3. inform the Secretary, Deputy Secretary, and the Congress fully and currently about any problems and deficiencies relating to the administration of any DHS program or operation and the need for, and progress of, corrective action;

4. review and comment on existing and proposed legislation and regulations relating to DHS programs, operations, and personnel;

5. distribute final audit and inspection reports to appropriate authorizing and oversight committees of the Congress, to all headquarters and field officials responsible for taking corrective action on matters covered by the reports and to Secretarial officers, office heads, and other officials who have an official interest in the subject matter of the report;

6. receive and investigate complaints or information from employees, contractors, and other individuals concerning the possible existence of criminal or other misconduct constituting a violation of law, rules, or

regulations, a cause for suspension or debarment, mismanagement, gross waste of funds, abuse of authority, or a substantial and specific danger to the public health and safety, and report expeditiously to the Attorney General whenever the Inspector General has reasonable grounds to believe there has been a violation of Federal criminal law;

7. protect the identity of any complainant or anyone who provides information to the OIG, unless the OIG determines that disclosure of the identity during the course of the investigation is unavoidable.

Further, the OIG shall:

8. follow up on report recommendations to ensure that corrective actions have been completed and are effective;

9. prepare a semiannual report to the Secretary and the Congress, summarizing OIG audit and investigative activities within DHS. Section 5(a) of the Inspector General Act of 1978, as amended, requires this report.

B. Allegations received by the OIG or OE offices shall be retained or referred in accordance with Appendix A of this MD. The only exception to this requirement is that the OIG and the United States Secret Service will adhere to the terms of the Memorandum of Understanding entered into between those two entities on December 8, 2003, and as may be amended from time to time.

C. ***Standards.*** Audits shall be conducted consistent with the standards issued by the Comptroller General of the United States. Inspections and investigations shall be conducted consistent with the quality standards issued by the President's Council on Integrity and Efficiency (PCIE).

D. ***Questions or Concerns.*** Any questions or concerns regarding this directive should be addressed to the OIG.

J.M. Loy, ADM
Deputy Secretary

Issue date: JUN 10 2004

MD 0810.1

APPENDIX A

The categories of misconduct identified below shall be referred to the OIG. Such referrals shall be transmitted by the OE offices immediately upon receipt of the allegation, and no investigation shall be conducted by the OE offices prior to referral unless failure to do so would pose an imminent threat to human life, health or safety, or result in the irretrievable loss or destruction of critical evidence or witness testimony. In such extraordinary situations, the OIG will be contacted as soon as practical, and all information and evidence collected by the OE office shall then be provided to the OIG as part of the OE referral to the OIG. The OIG will accept and retain all such allegations for investigation subsumed under this exigent circumstance exception.

- All allegations of criminal misconduct against a DHS employee;
- All allegations of misconduct against employees at the GS-15, GM-15 level or higher, or against employees in the OE offices;
- All allegations of serious, noncriminal misconduct against a law enforcement officer. "Serious, noncriminal misconduct" is conduct that, if proved, would constitute perjury or material dishonesty, warrant suspension as discipline for a first offense, or result in loss of law enforcement authority. For purposes of this directive, a "law enforcement officer" is defined as any individual who is authorized to carry a weapon, make arrests, or conduct searches;
- All instances regarding discharge of a firearm that results in death or personal injury or otherwise warrants referral to the Civil Rights Criminal Division of the Department of Justice;
- All allegations of fraud by contractors, grantees or other individuals or entities receiving DHS funds or otherwise engaged in the operation of DHS programs or operations;
- All allegations of visa fraud by DHS employees working in the visa issuance process.

In addition, the OIG will investigate allegations against individuals or entities that do not fit into the categories identified above if the allegations reflect systemic violations, such as abuses of civil rights, civil liberties, or racial and ethnic profiling, serious management problems within the department, or otherwise represent a serious danger to public health and safety.

With regard to categories not specified above, the OE offices will initiate the investigation upon receipt of the allegation, and shall notify within five business days the OIG's Office of Investigations of such allegations. The OIG shall notify the OE offices if the OIG intends to assume control over or become involved in such an investigation, but absent such notification, the OE office shall maintain full responsibility for these investigations.

Any allegations received by the OIG that do not come within the categories specified above, or that the OIG determines not to investigate, will be referred within five business days of receipt of the allegation by the OIG to the appropriate OE office along with any confidentiality protections deemed necessary by the OIG.

The OE offices shall provide monthly reports to the OIG on all open investigations. In addition, upon request, the OE offices shall provide the OIG with a complete copy of the Report of Investigation, including all exhibits, at the completion of the investigation. Similarly, the OIG shall provide the OE offices, upon request, with a complete copy of any Report of Investigation relating to its OE, including all exhibits, at the completion of the investigation. The OIG shall have the right to request more frequent or detailed reports on any investigations and to reassert at any time exclusive authority or other involvement over any matter within its jurisdiction.

EXHIBIT 2-12 MEMORANDUM FROM DHS SECRETARY TO ALL EMPLOYEES, DATED APRIL 8, 2008.

Secretary
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

April 8, 2008

MEMORANDUM FROM THE SECRETARY

TO: All DHS Employees

SUBJECT: Cooperation With the Office of Inspector General

The Office of Inspector General (OIG) of the Department of Homeland Security serves an important role in helping the Department prevent and detect fraud, waste, mismanagement, and abuse. The OIG does so by conducting independent and objective audits, investigations, and inspections, thereby improving the economy, effectiveness, and efficiency of our programs and activities. The OIG needs information from Department offices to conduct its work effectively.

This memorandum is a reminder that I expect all DHS employees to cooperate fully with the OIG in its valuable endeavors, and should provide prompt access to requested materials and information. These expectations for DHS employees also extend to requests from any contractor hired by the OIG, such as the firm hired by the OIG to audit the Department's financial statements. This cooperation includes:

- Promptly providing materials responsive to a request and other relevant information (even if not specifically requested);
- Honoring OIG requests for interviews with program officials in a timely manner;
- Respecting employees' rights to speak directly and confidentially with the OIG in accordance with legal requirements;
- Refraining from inappropriate activity that might inhibit or chill an employee or contractor's communication or cooperation with the OIG.

Production of requested materials should be prompt, and the vast majority of such materials may be produced to the OIG directly and immediately upon request. DHS employees should advise the OIG when requested materials contain classified national security information, privacy-protected materials, attorney-client or deliberative (pre-decisional and draft) communications, and other sensitive information, or materials from agencies outside the Department. If there is any question about the status of certain materials or how to handle them, employees should consult with their supervisors or the Office of the General Counsel to ensure that documents are properly identified, marked and treated, and that records obtained from outside the Department are properly coordinated with the other agency, but doing so should not unduly delay delivery to the OIG. The production of these materials to the OIG does not waive our ability to assert privileges or other protections in any forum.

www.dhs.gov

DHS employees are not to conceal information or obstruct audits, inspections, investigations, or other OIG inquiries. Doing so is against Department directives and can lead to serious consequences.

The OIG has important obligations in the conduct of its audits, investigations, and inspections, and will:

- Honor requests for confidentiality to the extent permitted by law;
- Coordinate with agency managers and supervisors to avoid disrupting ongoing work;
- Respect sensitive materials that are segregated (and be watchful for documents that have not been segregated), so that Department privileges and other obligations are not compromised (thus allowing the Department to assert applicable claims prior to any production outside the Department); and
- Comport with all other responsibilities under the DHS Management Directive.

If you have any questions regarding your obligations regarding the OIG or the OIG's authorities, you should consult with your supervisor or the Office of the General Counsel.

Department of Homeland Security
Office of Inspector General

Office of Investigations Special Agent Handbook

September 2015

SPECIAL AGENT HANDBOOK
INDEX

Table of Contents

Table of Contents

Table of Contents

Table of Contents

3.0 RESPONSIBILITIES AND CONDUCT

3.1 STANDARDS OF ETHICAL CONDUCT

The *Standards of Ethical Conduct for Employees of the Executive Branch*, codified in Title 5, C.F.R., Part 2635, apply to all employees of the Executive Branch of government, except for enlisted members of the armed services. Violations of these standards can lead to disciplinary action up to and including removal from federal service. All OIG Special Agents (SAs) must be familiar with these standards not only as they apply to themselves but also their applicability to employee violations under investigation. All INV employees will be administered an Oath of Office in accordance with Standard Form 61.

An employee should avoid any action that might result in, or create the appearance of:

- Using public office for private gain
- Giving preferential treatment to anyone
- Impeding government efficiency or economy
- Losing complete independence and/or impartiality
- Making a government decision outside of official channels
- Adversely affecting the confidence of the public in the integrity of the government.

3.2 CONFLICT OF INTEREST

In addition to the standards of ethical conduct, conflict of interest statutes prohibit certain conduct. Criminal conflict of interest statutes of general applicability to all employees must be taken into consideration in determining whether conduct is proper (e.g. 18 U.S.C. § 201, 203, 205, 207, 208, and 209). Further reference is made to the web site of the U.S. Office of Government Ethics at www.usoge.gov. OGE regulations at 5 CFR 2638.603 require concurrent notification to OGE of any referral to the Department of Justice of violation any of the above statutes by current or former employees of the executive branch.

If an SA suspects that a conflict of interest exists which might affect their objectivity in carrying out an investigation or assignment, notification to the SAC should be made as soon as possible. Similarly, if an SA suspects that circumstances exist, which may create an appearance of a conflict, the SAC should be notified.

After receiving notification of an actual or apparent conflict, the SAC will determine whether the SA should be excluded from an investigation or assignment.

3.3 AGENCY REGULATIONS ON CONDUCT

All OIG employees shall comply with the regulations governing employee conduct issued by the Department of Homeland Security as outlined in DHS Management Directive (MD) #0810.1, Section 5. **(Exhibit 2-11)** Questions regarding standards should be directed to the employee's supervisor.

3.4 EMPLOYEE VIOLATIONS OF THE STANDARDS OF CONDUCT

A violation of the standards of ethical conduct or of supplemental agency regulations may be cause for corrective or disciplinary action under applicable government-wide regulations or agency procedures. Such actions may be in addition to other action or penalty as prescribed by law.

Each SA is responsible for reporting to their supervisor any arrest or charge of violation of any federal, state, or foreign law. The supervisor will immediately notify the DAIGI of the incident. Minor traffic violations need not be reported.

The supervisor is responsible for reporting the resolution of the matter to the DAIGI, including conviction, acquittal, probation before judgment, or any other disposition.

Cases involving substantive allegations of criminal conduct or of egregious non-criminal misconduct by OIG employees will be referred directly to the AIGI.

3.5 CONDUCT WHILE ON OFFICIAL DUTY

The general reputation, credibility, and professional image of the OIG depend on the actions of each member of the organization. Daily contact by SAs and other OIG employees with the public, government agencies, law enforcement personnel, United States Attorneys, courts, and others, is an opportunity to create and maintain a professional image and reputation.

Below are guidelines that should be followed at all times. SAs:

Will exercise their authority only in connection with matters of official interest to the OIG.

Will not engage in the abuse of investigative authority or unnecessary interference in the operations of others during the conduct of an investigation. Databases including the OIG Enforcement Data System (EDS), a law enforcement database, should only be accessed in pursuit of official purposes, while strictly adhering to all banner warnings. Misuse or unauthorized use of any official database, including EDS may constitute a criminal violation and in addition to possible prosecution may be cause for disciplinary action including dismissal.

Will not display or use badges, credentials, firearms, restraint devices, or any other law enforcement equipment except when acting within the scope of their authority. Unauthorized use of law enforcement equipment can result in disciplinary action, including removal from federal service.

Will avoid expressing personal opinions on controversial social, or political matters while on official business.

Will fully cooperate with other law enforcement agencies conducting investigations with the
OIG

The advent of social networking sites such as Facebook, present potential problems for law enforcement personnel. Participating in these sites by posting photographs or messages that are inappropriate or unprofessional can lead to their dissemination and possibly be used to discredit the agent in court proceedings. Although utilizing these sites is not prohibited, personnel should exercise caution when posting profiles and other personal opinions and information.

Additionally, the use of email has become widespread. It is important to keep in mind that emails are not private property and can be monitored, stored and recovered. You should be circumspect and professional in what you write in an email message and you should not include anything that you would not want to see on the front page of the newspaper the following day or sometime later in court. (Chapter 8.7)

3.6 RESTRICTED DUTY

It is the SAs' responsibility to request temporary light duty through the submission of a memorandum to the AIGI through the SAC with appropriate medical documentation attached. This documentation will include evaluations, diagnosis, and a medical opinion regarding the ability of the employee to perform specific duties. It is the SAC's responsibility to forward this request with a recommendation for approval or disapproval.

3.7 SURRENDER OF BADGE, CREDENTIAL, AND FIREARM

SAs who are placed on suspension or administrative leave for disciplinary reasons are required to surrender their badge, credentials and firearm to their supervisor before serving the suspension or being placed on administrative leave.

If for any reason the SA's supervisor believes that the SA should not be required to surrender their badge, credentials, and/or firearm, the supervisor may request, in writing, that the AIGI waive the requirement. Such request shall set forth the reasons for the waiver request.

3.8 OUTSIDE EMPLOYMENT AND ACTIVITIES

Due to the importance of avoiding conflicts of interest, or the appearance of conflicts of interest, by OIG employees, all outside employment and certain activities such as the examples below, whether for compensation or not, require the prior written approval of the employee's supervisor. Employees of INV should not engage in any activity that could cause embarrassment to, or call into question, the integrity or objectivity of the OIG. When in doubt about the appropriateness of an outside activity, the employee should seek advice from Counsel.

Examples of outside activities requiring prior written approval include:

> Certain types of professional and consultative services.
>
> Certain teaching, lecturing, writing, editing, and certain office-holding activities in professional societies.
>
> All activities for which OIG employees are financially compensated and which are considered employment or business.
>
> All legal services and all outside law enforcement activities, including volunteer work, with the exception of temporary legal services to relatives (for example, drawing a will or handling a traffic violation, eviction notice, or mortgage transaction).

Outside employment is generally prohibited. However, an SA may, on a case-by-case basis, apply for approval to engage in outside employment or activities. The SA will prepare a memorandum to the AIGI through their SAC outlining a description of the employment position or activity, the expected number of hours per week, the reason for the employment or activity (e.g. professional, monetary, charitable, etc.). (Chapter 4.3)

The SAC will recommend approval or disapproval prior to forwarding the memorandum to the AIGI. The AIGI, who may consult with Counsel, will approve or disapprove the request.
After approval, if the scope of employment changes, the employee must submit a new approval request. Failure to obtain approval may result in disciplinary action.

Employees are subject to political activity restrictions as governed by law in accordance with the Hatch Act. Specific information outlining permissible and impermissible activities are outlined in detail at www.opm.gov.

3.9 DRUG AND ALCOHOL USE

INV's law enforcement mission requires that INV employees engage in activities that require the ability to think and react quickly, free of any impairment attributable to the use of alcohol or drugs. Such activities include, but are not limited to:

- Carrying and using firearms.

- Executing search warrants.
- Operating motor vehicles while on Government business.
- Dealing with other Government agencies, including other law enforcement agencies.
- Dealing with the public.

Administrative sanctions may be imposed against SAs who, without authorization, consume alcohol while on duty or report for duty under the influence of alcohol. Sanctions may be imposed against SAs who violate this prohibition, whether or not their performance or capacity to perform is impaired.

An exception to the prohibition against alcohol use may be authorized in instances where it is necessary to maintain the integrity of an undercover assignment or a surveillance position. Such exceptions may be authorized by the SA's SAC, or ASAC.

It is the personal responsibility of SAs to remove themselves from any official operation if they become impaired due to the consumption of alcohol or any other substance, including drugs and/or medications.

Any SA who senses (or reasonably anticipates) impairment attributable to legal drug use must report that condition to their supervisor and request leave or assignment to other duties.

INV prohibits the use of illegal drugs by any INV employee at any time. INV employees may be subject to random or specific drug testing as a condition of employment.

INV employees who abuse alcohol or drugs, or who feel that they may have an alcohol or drug-related problem, are encouraged to seek corrective professional help.

3.10 EMPLOYEE ASSISTANCE PROGRAM (EAP)

All INV employees have access to the Employee Assistance Program (EAP), which can help them obtain appropriate assistance. EAP is a professional counseling and referral service designed to help employees with problems both on and off the job. It is free and confidential within the limits of the law. Assistance is available in some cases to immediate family members. EAP can be reached at telephone number 1-800-222-0364 or at www.FOH4you.gov

3.11 DISCLOSURE OF INFORMATION

Information in the possession of INV will be disclosed only as authorized by law and regulation. This includes requests from the Office of Audit, other Offices of Inspector General, other law enforcement agencies, federal, state, and local agencies, the public, Congress, and the courts. All releases pursuant to FOIA and Privacy Act requests will be authorized by and coordinated through OIG Counsel. (Chapter 21.2)

INV personnel in possession of sensitive information are responsible for protecting such information from unauthorized disclosure. (Chapter 8.16)

Media requests will be handled under procedures outlined in Chapter 4.14.

3.12 GIGLIO/HENTHORN POLICY

BACKGROUND

OIG receives requests for potential impeachment information, also known as Giglio/Henthorn reviews, for both OIG employees and employees of other DHS components. This policy addresses the disclosure of potential impeachment information regarding employees of all DHS components who are affiants or witnesses in a criminal investigation or case to the United States Attorney's Office (USAO) and DOJ criminal litigating sections. It is intended to ensure that prosecutors in a Federal criminal proceeding receive sufficient information to meet their obligation under *Giglio v. United States*, 405 U.S. 150 (1972), while protecting the legitimate privacy rights of DHS OIG employees. It has been updated to reflect DOJ's May 12, 2014, amendment of Section 9-5.100 of the United States Attorney's Manual (the "*Giglio* Policy").

AUTHORITY

Memorandum from James M. Cole, Deputy Attorney General, to the Associate Attorney General, et al., Amendment of Section 9-5.100 of the United States Attorneys' Manual ("The *Giglio* Policy"), (May 12, 2014).

DEFINITIONS

1. Impeachment information- The exact parameters of potential impeachment information are not easily determined. Potential impeachment information, however, has been generally defined as impeaching information that is material to the defense. This information may include, but is not limited to:

   (a) any finding of misconduct that reflects upon the truthfulness or possible bias of the employee, including a finding of lack of candor during a criminal, civil, or administrative inquiry or proceeding;

   (b) any past or pending criminal charge brought against the employee;

   (c) any allegation of misconduct bearing upon truthfulness, bias, or integrity that is the subject of a pending investigation;

   (d) prior findings by a judge that an agency employee has testified untruthfully, made a knowing false statement in writing, engaged in an unlawful search or seizure, illegally obtained a confession, or engaged in other misconduct;

(e) any misconduct finding or pending misconduct allegation that either casts a substantial doubt upon the accuracy of any evidence—including witness testimony—that the prosecutor intends to rely on to prove an element or any crime charged, or that might have a significant bearing on the admissibility of prosecution evidence. Accordingly, agencies and employees should disclose findings or allegations that relate to substantive violations concerning:

i. failure to follow legal or agency requirements for the collection and handling of evidence, obtaining statements, recording communications, and obtaining consents to search or to record communications;

ii. failure to comply with agency procedures for supervising the activities of a cooperating person (CI, CS, etc.);

iii. failure to follow mandatory protocols with regard to the forensic analysis of evidence;

(f) information that may be used to suggest that the agency employee is biased for or against a defendant. *See U.S. v. Abel*, 469 U.S. 45, 52 (1984). The Supreme Court has stated, "[b]ias is a term used in the 'common law of evidence' to describe the relationship between a part and a witness which might lead the witness to slant, unconsciously or otherwise, his testimony in favor of or against a party. Bias may be induced by a witness' like, dislike, or fear of a party, or by the witness' self-interest."); and

(g) information that reflects that the agency employee's ability to perceive and recall truth is impaired.

2. Requesting Official- The official that requests potential impeachment information from an investigative agency on behalf of the prosecuting office.

3. Agency Official- For DHS OIG, this is the Counsel to the Inspector General (Counsel). The Counsel will serve as the point of contact concerning potential impeachment information.

POLICY

DHS employees are obligated to inform prosecuting attorneys with whom they work of any potential impeachment information as early as possible prior to providing a sworn statement or testimony in any criminal investigation or case.

In the majority of investigations and cases in which agency employees may be affiants or witnesses, it is expected that the prosecuting attorney will be able to obtain all potential impeachment information directly from the agency witnesses during the normal course of investigations and/or preparation for hearings or trials.

Nevertheless, a prosecutor may also decide to request potential impeachment information from the employing agency. This policy sets forth procedures for those cases in which a prosecutor decides to make such a request.

PROCEDURES

1. When a Requesting Official Requests Potential Impeachment Information Relating to a DHS Non-OIG Employee

   A. Requests for potential impeachment information should be directed to the Counsel via e-mail, fax, or regular mail.

      Mailing address:
      DHS/Inspector General
      STOP 0305
      Name of Counsel/Telephone number
      245 Murray Lane, S.W.,
      Washington, D.C. 20528-0305

      Office of Counsel Fax Number: (202) 254-4398

   B. Upon receiving a request for potential impeachment information, Office of Counsel (OC) will ask INV to review its records and databases for all information related to the DHS employee that is the subject of the request.

   C. INV submits any information generated to OC for review for potential impeachment information.

   D. If potential impeachment information is found, OC will contact the Requesting Official and/or prosecutor directly.

2. When a Requesting Official Requests Potential Impeachment Information Relating to a DHS OIG Employee

   A. Requests for potential impeachment information should be directed to the Counsel via e-mail, fax, or regular mail as stated in Procedures Section 1.A. above.

   B. Upon receiving a request, OC will ask the following entities to review their records and databases for any potential impeachment information:

      a. The SA's SAC;

      b. INV to query EDS and SID;

      c. OIG Human Resources Division;

d. OIG Security Division; and

e. DHS Office of Personnel Security.

C. All potential impeachment information should be sent to OC for review.

D. If potential impeachment information is found, OC will contact the Requesting Official and/or prosecutor directly.

E. If OC reports potential impeachment information, OC must maintain judicial rulings and related pleadings on information that was disclosed to the Court or the defense in a manner that allows expeditious access upon the request of any Requesting Official.

F. If an OIG employee, on which potential impeachment information is reported to a prosecutor, is transferred to a new district, INV must inform OC. OC must ensure that a Requesting Official in the new district is advised of any potential impeachment material known to OIG when the OIG employee begins meaningful work on a case or matter within the prosecuting district or is reasonably anticipated to begin meaningful work on such a case or matter.

G. Only OC or personnel within an OIG employee's chain-of-command shall communicate any potential impeachment information to a Requesting Official or prosecutor.

3. Continuing Duty to Disclose for All DHS Employees

Once a request for potential impeachment information has been made, OIG, through OC, must report any additional potential impeachment information that arises after such request and during the pendency of the specific criminal case or investigation in which a DHS employee is a potential witness or affiant. OIG's duty to disclose will cease when the specific criminal case or investigation for which the request was made ends in a judgment or declination. OC will notify OIG offices that must report information when the duty to disclose has ceased.

4. Treatment of Allegations Which are Unsubstantiated, Not Credible or Have Resulted in Exoneration With Respect to All DHS Employees

Allegations that cannot be substantiated, are not credible, or have resulted in the exoneration of an employee, generally, are not considered potential impeachment information. Upon request, such information which reflects upon the truthfulness or bias of the employees, to the extent maintained by the agency, will be provided to the prosecuting office under the following circumstances:

A. when the Requesting Official advises the Agency Official that it is required by a Court decision in the district where the investigation or case is being pursued;

B. when, on or after the effective date of this policy:

   i. the allegation was made by a federal prosecutor, magistrate judge, or judge; or

   ii. the allegation received publicity;

C. when the Requesting Official and the Agency Official agree that such disclosure is appropriate, based upon exceptional circumstances involving the nature of the case or the role of the agency witness; or

D. when disclosure is otherwise deemed appropriate by the agency.

OIG is responsible for advising the prosecuting office, to the extent determined, whether any aforementioned allegation is unsubstantiated, not credible, or resulted in the employee's exoneration.

If you have any questions with regard to this policy, please contact OC.

CHAPTER 3.0 - EXHIBITS

No exhibits for this chapter.

4. 0 ADMINISTRATIVE PROCEDURES

4. 1 Employee Personnel Files

The INV manager of each office will establish an Employee Personnel File (EPF) for each individual that they supervise. Documents contained in the EPF will be filed according to a standardized filing system. The file will be annotated on the outside with the employee's name. Information will be filed on each side (side one being the inside of the front cover and side four being the inside of the back cover) as follows:

Section 1: Current Emergency Contact Information; and Employee's Position Description (initialed and dated by the employee annually at the time their annual performance appraisal is issued).

Section 2: Personal Certification Memoranda.

Section 3 Employee Property Inventory Log, INV Form 90. **(Exhibit 4-1)**

Section 4: Miscellaneous (such as Telework Agreements), Database Access Certifications, Ethics Opinion, and Code of Conduct.

These files will be stored in a locked file cabinet or safe.

The EPF will be sent to the employee's new post of duty upon the employee's transfer. When the individual terminates their employment with the OIG, the file will be destroyed.

4. 2 Annual Employee Certifications

At the beginning of each fiscal year, SAs are required to certify by dated memorandum the following certifications:

- SA is Available to work Law Enforcement Availability Pay (LEAP), INV Form 80 (**Exhibit 4-2).**
- SA has reviewed and is familiar with Special Agent Handbook (SAH) INV Form 97A (**Exhibit 4-2A)**
- SA has reviewed and is familiar with Standards of Ethical Conduct for Government Employees. Reference Chapter 3. INV Form 97A **(Exhibit 4-2A)**
- SA has reviewed and is familiar with TSA Regulations for flying Armed. (Reference Chapter 5. 6) INV Form 97A **(Exhibit 4-2A)**
- Requesting for authorization to participate in the physical training (PT) program. (Reference Chapter 6. 9) **(Exhibit 4-2B)**

Certifications for the current year only will be filed and maintained in the Employee Personnel File (EPF).

4. 3 LEAP Defined

Law Enforcement Availability Pay, as outlined in Title 5 U. S. C. § 5545a, *Law Enforcement Availability Pay Act of 1994*, is the 25% percent premium paid to ensure the "availability" of criminal investigators for unscheduled duty in excess of their 40-hour basic workweek. LEAP will be considered as part of basic pay for the computation of retirement benefits, lump sum annual leave, life insurance, and the value of subsistence and quarters where applicable.

Availability means that a criminal investigator shall be either performing official duties during unscheduled duty hours or considered generally and reasonably accessible to perform official duties during unscheduled duty hours based on the needs of the OIG. Unscheduled duty hours are those hours that are not a part of the 40 hours in the basic workweek or not regularly scheduled. Administrative workweek means a period of seven consecutive calendar days designated in advance by the head of an agency. Regular workday means each day in the basic workweek during which the investigator works at least four hours that are not regularly scheduled overtime hours or unscheduled duty hours.

All SAs, through General Schedule (GS) 15, are eligible to receive LEAP and are exempt from the *Fair Labor Standards Act of 1938*.

Involuntary reduction in pay resulting from a denial of certification and removal from LEAP is considered an adverse personnel action. All such actions must be coordinated through the AIGI.

4. 4 LEAP Administration

An SA shall continue to be paid LEAP if the annual daily average of unscheduled hours worked is equal to or greater than two hours per qualifying work day. Exemptions to the qualifying workday are holidays, regular days off and those days that include four hours or greater of annual leave, sick leave, time off award, and training.

Compensation, either by pay or compensatory time off, for unscheduled duty hours worked over the annual daily average is not authorized.

A supervisor who directs an SA to be available for duty during unscheduled duty hours may, at his/her discretion, authorize the SA to be away from the office or home, so long as the SA is reachable by phone and is able to respond back to duty in a reasonable amount of time.

4. 5 LEAP Reporting Requirements

Recording of unscheduled duty hours for LEAP purposes will be accomplished by the completion of the Time Tracking System (TTS) in EDS**.** The SA's supervisor will approve these reports.

At the beginning of each fiscal year, SAs are required to certify by memorandum that they agree to be available for unscheduled duty based on the needs of the OIG. The original memorandum will be maintained in the SA's EPF.

By October 31st of each year, each SAC will certify to the AIGI that all criminal investigators under their supervision met the LEAP requirements in the previous reporting period and are expected to meet the requirements in the upcoming reporting period. This certification memorandum, INV Form 81 **(Exhibit 4-3)** authorizes LEAP payments to the SA. The original memorandum will be forwarded to the FOD and a copy will be filed in the office administrative file number 2700.

4. 6 Reporting Hours within the Time Tracking System (TTS)

The TTS is designed to document employee work hours for all agent and INV personnel.

Time reported under the various categories will be rounded up or down, as appropriate, to the nearest one-half hour.

Time spent traveling outside the regular workday or basic workweek may be claimed as LEAP hours and should be charged to the activity to which the travel is associated. Time spent traveling to and from post of duty (office) during a regular day commute may not be counted as LEAP hours.

A base workday reduction is any day on which an agent took four or more hours of leave, training, or any legal public holiday designated by the federal government. If no reduction is taken under the above description, LEAP may be earned for that day, even if the SA took leave and/or participated in training.

The number of hours entered in TTS each pay period must match the number of hours reflected in the Web Time and Attendance (WebTA) for that pay period, except for LEAP hours which are reported only in TTS.

Employees may not enter hours in TTS that have not been entered in WebTA and certified by a supervisor.

TTS must be completed by the first Tuesday following the end of each pay period (i.e. within two business day of the end of the pay period), staff must submit completed TTS Timesheets to their supervisors via TTS for approval, or when practicable.

Supervisors must review and approve all TTS Timesheets by the first Thursday following the end of the pay period (i.e. within two business days of receipt of the timesheets), or when practicable.

Special Agents must receive prior approval from the SAC to work Scheduled Overtime in a pay period. Overtime requests and authorizations will be routed through WebTA.

OIG offices will be open to conduct official business from 8:30AM to 5:00PM, Monday through Friday.

4. 7 Property Accountability

DHS-OIG maintains three categories of issued personnel and/or office property: 1) Managed Property – equipment inventoried by the Office of Training i.e.: Duty Firearms, Tactical Firearms, AEDs, Technical Equipment, Radios; 2) Accountable Property – property inventoried annually by the Field Office SACs i.e.: Handcuffs, Batons, Credit Cards, Cell Phones; and 3) Non-Accountable Property - any property that through normal use is destroyed i e.: Batteries, DVDs, Safety Glasses or has little or no value. Items accounted for under the Property Inventory Management System (PIMS) are NOT included in this property definition, nor added to the Employee Property Inventory Log, INV Form 90 **(Exhibit 4-1)**.

All transfer of property between offices, employees or components (both permanent and temporary), will be recorded utilizing the Items Property Transfer Transaction Record, DHS-OIG Form 90.1 **(Exhibit 4-1A**). The transferor will complete the form; providing the Office of Training a copy of Form 90.1 if the property transferred is considered Managed Property or Accountable Property. The transfer will not be considered official until accepted by the Office of Training and properly documented.

Each employee is responsible for all issued Managed and Accountable property INV Form 90 **(Exhibit 4-1)** as listed on the Employee Property Inventory Log, which will be maintained in the EPF and certified annually. Other property may be added at the discretion of the SAC. The Office of Training will conduct an annual inventory of all Managed Property.

SACs will be responsible for all managed and accountable property issued to the office. Verification of all accountable property will be conducted annually and certified by the SAC. A record of the inventory and certification will be maintained in the Field Office administrative file for equipment (7720) as well as maintained by the Office of Training.

Excess or surplus property will be disposed of in accordance with OIG and General Services Administration (GSA) guidelines. Requesting SA will complete a Declaration of Excess Personal Property, DHS-OIG Form 90.6 (**Exhibit 4-1C**) and forward to the Office of Training for review. All technical Surveillance equipment due to its sensitive law enforcement status must be destroyed, INV Form 90.5 (**Exhibit 4-1B**). All other equipment requests will be reviewed by the SAC, Office of Training and disposition instructions provided within 60 days of receipt.

4. 8 Return of Accountable Property

The Employee Property Inventory Log INV Form 90 **(Exhibit 4-1)** will be amended to document the SA's return of accountable equipment or property upon notice to the Office of Training. When an employee separates from DHS OIG, the amended form will be printed, signed by the departing employee and supervisor, maintained in the EPF and a copy forwarded to the Office of Training.

4. 9 Loss/Theft of Accountable Equipment/Property

SAs will immediately report the loss of accountable equipment/property to their SAC. Within 24 hours the SA shall document by memorandum to the AIGI through the SAC the pertinent circumstances of the theft/loss. The SAC will notify the appropriate FOD of any loss of accountable property/equipment. Loss of technical investigative equipment will be reported to the appropriate FOD and the National Technical Program Manager. If it is readily apparent the property was stolen, the SAC who is reporting the loss will decide whether an investigation will be initiated. If the loss is due to SA negligence, the SAC will notify their FOD. The SA may be held liable for replacement costs and may be subject disciplinary action.

Sensitive law enforcement equipment shall not be entered into the National Crime Information Center (NCIC) system unless instructed to do so by the AIGI and the SAC, Office of Training.

4. 10 Retention of Badge and Credentials

SAs who are retiring from the agency and who have received at least a satisfactory performance appraisal for the most current rating period may be authorized to retain their OIG badge and credentials. The SA's SAC must send a memorandum to the DAIGI requesting the issuance of the inactive badge and credentials. **(Exhibit 4-4)**

At the completion of the SA's employment, the credentials will be marked "retired" or "inactive. " The badge will be deactivated in the INV's badge inventory with a remark stating the reason, i. e. retirement. In all instances, the original badge and credentials will be placed on a plaque prior to returning the items to the SA. In addition, the SA will receive a replica badge marked retired. INV is responsible for notifying OM that the credentials have been permanently retired and deactivated.

The ordering of the plaque through HQ will be the responsibility of the employee's SAC.

Retiring or separating SAs may also be issued a DHS OIG Law Enforcement Officer (LEO) Identification Card (ID) for the purposes of identification under Public Law 108-277, *Law Enforcement Officer Safety Act of 2004* (LEOSA), codified at Title 18 USC, Section 926C, will comply with DHS OIG Directive Number 257-01 **(Exhibit 4-4A)**. The LEOSA, with certain limitations and conditions, exempts qualified retired law enforcement officers from most State and local laws that prohibit the carriage of concealed firearms. LEOSA does not exempt individuals from other Federal laws or regulations nor does it extend any new authority for use of firearms or any new law enforcement powers. Field Offices will provide SAs about to retire a copy of DHS OIG Directive Number 257-01-001, **(Exhibits 4-4B)**

In order to receive a DHS OIG LEO ID Card a retired SA must meet the definition of a qualified law enforcement officer under 18 USC 926 (c) and be prohibited from receiving a firearm under 18 USC 922 (g) and (n). Retiring SAs must complete the DHS OIG Law Enforcement Officer Identification Card Application and submit the application to their SAC. **(Exhibit 4-5)**

Retirees who have received the DHS OIG LEO ID Card are required to certify annually to DHS OIG Office of Investigations in writing by completing the DHS OIG Federal Law Enforcement Officer Identification Card Recertification form, that Federal law does not prohibit him or her from receiving a firearm. **(Exhibit 4-5A)**

4. 11 Use of Official Vehicles

It is the policy of the U. S. Department of Homeland Security, Office of Inspector General (OIG), Office of Investigations (INV) to provide eligible employees with the use of a Government Owned Vehicle (GOV) to facilitate transportation related to the execution of their official duties, functions and responsibilities. The term "official duties" includes the investigation of criminal offenses and administrative violations, as well as approved training, official functions, official travel and any other transportation related to the economical and effective administration of the OIG.

The use of a GOV is a privilege that is extended to OIG employees. Most often, the privilege to use a GOV is extended to Special Agents (SAs) to facilitate their performance of the duties and responsibilities required by criminal investigators. Employees will be authorized to operate a GOV under such circumstances when it is determined to be in the best interest of the government, as well as the effective and efficient operation of the OIG.

Only OIG Criminal Investigators who are engaged in criminal law enforcement duties, and for whom such transportation is essential for the safe and efficient performance of those duties, may be authorized home-to-work (HTW) use of an official GOV.

It is the policy of the OIG to permit HTW transportation based on the April 7, 2004, memorandum signed by DHS Secretary Ridge approving HTW transportation for DHS OIG's criminal investigators. HTW transportation may not exceed 50 miles (one way) from an employee's official duty station and his or her permanent residence of record. Any request for HTW transportation in excess of 50 miles should be submitted to the AIGI for approval and should include a memorandum detailing the rationale for the specific exception.

Field Office SACs, Directors, the DAIGI, and the AIGI will review the duties and activities of SAs under their supervision on a continuing basis. Those SAs whose duties or activities do not conform to the criteria for receiving HTW authority will not be authorized use of a GOV for this purpose, or, if previously authorized, their authorization will be revoked. The authorization to use a GOV may be limited, suspended, or revoked at the discretion of the SAC, Director, DAIGI or AIGI to promote the economy and effectiveness of the organization

References

The unauthorized or improper use of a GOV has the potential to expose the government to significant financial liabilities resulting from tort claims. As such, the authorization to use a GOV conveys the investment of trust in an employee and requires him or her to ensure that the GOV is always operated in an authorized, safe, efficient, and responsible manner. Employees who are authorized to operate a GOV must be familiar with the statutes, regulations, and

policies that authorize and govern their use of a GOV. Specifically, each employee who operates a GOV must be aware of, and comply with, the following:

A. Title 31 U. S. C. 1344 – Federal law providing that GOVs may only be used to provide transportation for official purposes.
B. Title 31 U. S. C. 1349 – Federal law mandating that any employee who willfully misuses, or authorizes misuse of, a passenger motor vehicle owned or leased by the United States Government shall be suspended without pay for at least 30 days, and, when circumstances warrant, for a longer period, or summarily removed from office.

C. 41 CFR Part 102-5 – Home-to-Work Transportation – Government-wide regulations applying to the operation of GOVs for HTW.

D. 41 CFR Part 102-34, Subpart D – Official Use of Government Motor Vehicles.

E. 41 CFR Part 102-34, Subpart G – Motor Vehicle Crash Reporting.

F. 41 CFR Part 101-39, Subpart 101-39. 4 – Accidents and Claims.

G. OIG Directive 50-2 – Personal Property Management– Agency policy addressing the assignment and responsibility for accountable property.

H. OIG Administrative Procedures, AP #50-1 – Motor Vehicle Accident Reporting and Payment.

I. Homeland Security Manual 112-05-001 – Home-to-Work Transportation.

J. Homeland Security Directive 112-05 – Home-to-Work Transportation Programs.

K. Homeland Security Directive – Memorandum dated April 7, 2004, signed by Secretary Ridge approving home-to-work transportation for DHS OIG's criminal investigators.

L. DHS Motor Vehicle Fleet Program Manual 118-01-01, Subparts D and J.

Responsibilities of GOV Operators

Each employee who is authorized to operate a GOV must adhere to the following conditions:

A. Annual Certification – On an annual basis, each employee who is authorized to operate a GOV must acknowledge his or her receipt and understanding of this policy and the laws, regulations, and directives referenced above, and his or her intent to comply with them by signing a certification and submitting it to their supervisor before taking possession of their assigned GOV. INV Form 97A, Annual Employee Certifications **(Exhibit 4-2A,)** Additionally, employees authorized to use HTW transportation must acknowledge and sign an annual HTW transportation certification. INV Form 86B **(Exhibit 4-6B)**

B. Maintain a Valid Operator's License- Each employee who is authorized to operate a GOV must maintain and possesses a valid operator's license, issued by the competent authority in their state of residence, which has not been restricted or suspended as the result of traffic infraction(s) or criminal violation(s). Supervisors should verify annually that all INV personnel authorized to operate a GOV possess a valid operator's license. The field office should maintain a copy of the Special Agent's driver's license.

C. Safe and Efficient Operation- Each employee who is authorized to operate a GOV must ensure the proper care, repair, maintenance and cleanliness of a GOV subject to their control. INV Form 86C Vehicle Equipment Checklist **(Exhibit 4-6C)** Additionally, an employee authorized to operate a GOV may not:
    a. Use a cell phone while operating the GOV unless the State in which the employee is driving authorizes the use of hand-held devices, and then only using a "hands free" device;
    b. Text while driving;
    c. Drive without wearing a seatbelt;

D. Sobriety- An employee may not operate a GOV within 8 hours of having consumed an alcoholic beverage. Each employee who is authorized to operate a GOV must be free from impairment resulting from consumption of any over-the-counter or prescription medication that interferes with their ability to safely operate a motor vehicle.

E. Assumption of Personal Liabilities- Each employee who is authorized to operate a GOV is responsible for obeying all motor vehicle traffic laws of the State and local jurisdiction, except when the duties of the position require otherwise. Special Agent is personally responsible if he or she violates State or local traffic laws, and is personally and financially responsible offenses committed while performing official duties, unless the offense was *required* as part of the employee's official duties. Employees will not be reimbursed. Additionally, each employee who is authorized to operate a GOV will be held financially responsible for the restitution of damages when it is determined that the damages stemmed from the negligent or reckless care or operation of a GOV or the operation for the satisfaction of fines or penalties arising from traffic and parking of a GOV in violation of this policy.

F. Security- All SAs authorized for HTW use of an official GOV are responsible for the security of the vehicle. SAs must park or store the GOV in a manner that reasonably protects it from theft or damage. When not in use for official business, the GOV must be parked at the SA's permanent residence, and may not be left in overnight or long-term parking, or other locations. Equipment assigned to a SA for official use shall not be left in plain view in a GOV. SAs also must lock the GOV when it is unattended. (The only exception to this requirement is when fire regulations or other directives prohibit locking motor vehicles in closed buildings or enclosures.)

Authorized Uses of a GOV

While it is impossible to contemplate and anticipate every possible circumstance that is related to the performance of official duties, OIG employees are authorized to utilize a GOV to facilitate their transportation, as well as the transportation of other government employees and authorized contractor employees, in conjunction with the following activities:

A. Investigative Activity- Generally defined as directly related to or in response to or in furtherance of an investigation of criminal or administrative offenses or misconduct violations subject to the jurisdiction of the OIG, or those investigations conducted cooperatively with another law enforcement component of the United States government, or the investigation of any State felony offense in a joint or task force setting.

B. Official Meetings- Any hearing, proceeding, meeting, or trial relating to the investigative mission of the OIG or otherwise related to the administration, operation, and official interests of the OIG.

C. Training and Firearms Qualifications- Any official training function or scheduled firearm qualification.

D. Purchase of Meals and Sustenance While on Duty- Reasonable travel for the purpose of purchasing food or sustenance during official work hours, including scheduled and unscheduled overtime hours.

E. Official Travel, Meals, and Incidentals- Overnight travel for official purposes and to obtain meals, incidentals, and services that are not otherwise prohibited by law or OIG policy in an official travel status.

F. Certain Official or Quasi-Official Events- Transportation to attend law enforcement related functions, such as retirements or funerals, officially on behalf of the OIG.

G. Home to Work Transportation- Use of a GOV to transport an employee between his or her home and place of work. Such HTW authorization shall permit a single stop in the morning and evening along the most direct or expeditious route between the employee's residence and work location to obtain limited personal services. Only other federal employees who, at the time of the transport are operating in official business, are authorized to share space as passengers, provided that the GOV does not travel additional distances as a result and such sharing is consistent with OIG policies. For reasons of officer safety, SAs are permitted to change their usual route home and to work by making slight deviations in their routes.

H. Exigent Circumstances- The use of a GOV is authorized in exigent circumstances necessitating an immediate response to protect or preserve life and public safety. However, operators must remain aware that the use of a GOV under exigent circumstances is subject to the reporting requirements outlined in "Law Enforcement Use and Emergency Driving" below.

I. Repairs- Operators are expected to ensure that routine maintenance and other repairs are performed on each GOV. The use of a GOV is authorized to ensure that maintenance and repairs are performed timely.

J. Other Uses, as Approved by a SAC, Director or AIGI – Any purpose authorized by a SAC, Director or AIGI that is related to the mission, administration, operation and interest of the OIG.

Prohibited Use of a GOV

Just as it is impossible to contemplate and anticipate every possible circumstance that is related to the performance of the official duties, it is also impossible to anticipate every possible circumstance under which the use of a GOV would be prohibited. As such, OIG employees must develop and apply a "common sense standard" when contemplating the use of a GOV for purposes that are likely unrelated to the OIG mission. With this in mind, employees are advised to refrain from using a GOV for any purpose other than the circumstances specifically outlined in the above section "Authorized Uses of GOV".

To assist employees with applying a common sense standard, the following are examples of use of a GOV that are prohibited:

A. Personal Travel, Errands, and Shopping – Employees shall not use a GOV to facilitate personal conveniences associated with personal travel, errands, or shopping (other than permitted in circumstances outlined in the previous section, Authorized Uses of a GOV).

B. Transportation of Friends and Relatives – Employees are prohibited from transporting friends or relatives in a GOV for any other purpose than the exigent circumstances outlined in Authorized Uses of a GOV.

C. Transportation to Purchase Alcoholic Beverages – Employees are prohibited from using a GOV to travel to bars and liquor stores while engaged in the performance of their official duties, HTW transportation, or official travel. Employees also are prohibited from transporting alcohol in a GOV.

D. Response to Violations Not Subject to Federal Jurisdiction – Employees are prohibited from using a GOV to respond to or facilitate, or otherwise involve themselves with, the investigation of or citation for the violation of any state or local traffic infraction or petty offense. However, should the employee perceive an imminent danger to public safety due to the state or local traffic infraction or petty offense, he or she is authorized to utilize a GOV in accordance with Authorized Uses of a GOV, "Exigent Circumstances," above.

E. Any Other Purpose Not Related to the OIG Mission – Employees are prohibited from using a GOV for any other purpose that interferes with or does not facilitate the economical, effective, and efficient operation of the OIG, or for which they are not authorized.

Law Enforcement Use and Emergency Driving

[redacted]

SACs may authorize the installation of emergency equipment, to include lights and sirens, in the assigned GOVs. This installation will comply with applicable state or local ordinances and regulations governing this equipment.

The use of emergency equipment is governed by DHS Management Directive 11015 **(Exhibit 4-7)** (Emergency Signaling Devices in DHS Vehicles) which states that authorized DHS employees (Sworn Law Enforcement Officers) shall only use emergency signaling devices when required for the safe execution of their official duties in circumstances where the need to protect the public safety or other employees requires increased visibility for vehicle operation.

Emergency driving is defined as operating a GOV in a manner wherein the operator exceeds the posted legal speed limits or disobeys other traffic laws for the purpose of following a vehicle to apprehend a suspect, conduct surveillance or respond to an exigent circumstance. Emergency driving may be overt or covert and may or may not entail the activation of a signaling or warning device that serves to identify a GOV as an official law enforcement vehicle.

A. Authorization - Only SAs are authorized to engage in emergency driving. SAs may engage in emergency driving only under those circumstances where the seriousness of the emergency outweighs the risks and dangers created by such driving. Examples of such circumstances would be to respond to the threat of death or serious bodily injury to a fellow law enforcement officer or innocent party, to respond to the scene of an emergency, or to transport a seriously injured person to a medical facility. In all cases of emergency driving, SAs must continually evaluate the need to further continue driving in such a manner that is against safety considerations.

B. Use of Authorized Emergency Equipment - GOVs will be equipped with emergency light(s) to identify a vehicle as an official law enforcement vehicle and, financial resources permitting, may be equipped with a siren or other signaling device. The use of personally owned or purchased emergency equipment is specifically prohibited. SAs may activate authorized emergency equipment to facilitate emergency driving and their movement through traffic congestion or to initiate a traffic stop to apprehend or identify a violator.

C. Prohibition - Use of emergency signaling devices without due care or in an improper or illegal manner is considered improper use of a motor vehicle and may result in adverse personnel actions including removal as well as individual legal liability for the user. Emergency driving is not authorized for routine or non-emergency purposes.

Emergency driving and the use of any signaling or warning to identify a GOV as a law enforcement vehicle is not permitted to facilitate the SA's movement through traffic congestion. Additionally, emergency driving is prohibited under those circumstances where such driving would unnecessarily endanger the safety of the public.

D. Pursuits - A pursuit is a type of emergency driving wherein a Special Agent disregards the posted legal speed limits or other traffic laws while official law enforcement signaling or warning devices are activated for the sole purpose of following a vehicle to apprehend a suspect.

E. [redacted]

i. [redacted]

ii. [redacted]

iii. [redacted]

iv. [redacted]

v. [redacted]

F. Mandatory Factors for Consideration- SAs must consider the following factors before engaging in emergency driving (including pursuits or any other driving maneuver) that may place themselves, fellow law enforcement officers, the public, and suspects at risk of injury or death:

i. Nature of emergency;
ii. Imminent danger to public safety in the event of escape;

iii. Seriousness of offense;
iv. Identification of the suspect;
v. Probability of apprehending suspect at a later time;
vi. Location, weather, traffic speed and road conditions;
vii. Time of day;
viii. Presence of pedestrians;
ix. Special Agent's driving abilities;
x. Condition and equipment of the GOV;
xi. Condition of the suspect's vehicle
xii. Availability of assistance from uniformed police officer; and
xiii. Possible alternative courses of action.

G. Requirement to Demonstrate Responsibility- Due to the risks associated with emergency driving (pursuits included), SAs must do so with great responsibility. As such, SAs must adhere to the following requirements:

i. Activation of All Emergency Equipment- Appropriate emergency warning equipment must be utilized in all emergency situations. However, in the event of a pursuit, all available emergency warning equipment must be activated.

ii. Safety- When engaged in emergency driving, SAs must operate their GOV with the utmost regard for the safety of the public and fellow law enforcement officers.

iii. Continuous Evaluation- When engaged in emergency driving (pursuits in particular), SAs must continually weigh and evaluate the advantages of their continued participation against all potential hazards.

iv. Termination- SAs must terminate emergency driving when the risk to themselves, fellow law enforcement or the public outweighs the benefit to continuing a rapid response or endeavoring to make an immediate apprehension.

H. [redacted]

I. Liability - SAs must remain mindful that courts generally do not condone emergency driving in a manner that needlessly or carelessly endangers life or property or that demonstrates a total indifference to others who are legitimately using the streets. Further, SAs must remember that engaging in emergency driving may expose the OIG to liability

under the *Federal Tort Claim Act*, and themselves to personal liability. As such, a SA should engage in emergency driving only when necessary, and engage in a pursuit as a last resort.

J. Precedence of OIG Policy in Joint Operations- The OIG policy established herein takes precedence for OIG SAs over any other policy that may be applicable to any facet of operation of a vehicle owned or operated by any other federal, state or local agency.

Required Reports and Procedures

Each Field Office will maintain control over the use of GOVs as follows: the SAC or designee will ensure that a separate folder is maintained for each vehicle. The folder will contain copies of all documents for that vehicle, including registration documentation, maintenance bills, or other charges paid to maintain the vehicle and the following:

A. Vehicle Usage Log - All employees who are assigned a GOV will prepare a monthly report concerning the operation of their vehicle. Reports will include the starting and ending mileage for the month, an accounting of the expenses incurred on each day, and a notation concerning whether or not the GOV was used for home-to-work and work-to-home. The report will be signed by the employee to certify the GOV was used in accordance with this policy. It will be signed by the employee and approved by the employee's immediate supervisor. INV Form-86, Vehicle Usage Log **(Exhibit 4-6)**

B. Motor Vehicle Reporting Requirements and Accident Investigations - GSA leased vehicles and government owned vehicles will be equipped with Standard Form (SF) 91, "Motor Vehicle Accident Report" and SF-94, "Statement of Witness." Commercially leased vehicles may be equipped with accident forms provided by the leasing company, which may be utilized in lieu of the SF-91 and SF-94. SF-91 and SF-94 are available on the OPM web site.

In the case of an accident, SAs should first notify the appropriate law enforcement agency and render appropriate assistance to injured parties at the scene. SAs should not make any statements regarding their fault or culpability. SAs should do everything they can to record all the facts at the scene of an accident. SAs should request a statement from witnesses using the SF-94. SAs should take complete photos of the GOV; the other vehicle(s) involved, regardless of whether any damage is visible; license tag numbers; and the other party or parties involved. SAs should note how many people are in the other vehicle(s) and each occupant's condition. SAs should record the names of any responding police officers. SAs also should record the other party's insurance policy information.

SAs must notify their immediate supervisor as soon as practicable, and the SAC will notify the AIGI immediately. At the SAC's discretion, an SA may be dispatched to the scene to conduct a preliminary investigation of the circumstances of the accident, which will be reported to the SAC by memorandum within five working days. The SA involved in the accident is required to provide a memorandum to his or her SAC within five working days explaining the circumstances of the accident. At a minimum, the memorandum should state the date, time, and location of the accident, estimated speeds, and driver actions. It also

should state where the SA was coming from and going to; why the SA was driving the GOV at that time; whether the SA was transporting other occupants; and what the other party or parties said or did. Completed SF-91 and SF-94, or other authorized forms, as well as all photos, should be attached. When the special agent is incapacitated due to injury, the responding SA will complete the necessary paperwork.

In cases involving GSA fleet vehicles, the special agent or their supervisor will notify the GSA Maintenance Control Center, telephone number 1-866-400-0411, or the manager of the Regional GSA Fleet Management Center that assigned the vehicle. In the case of commercially leased vehicles, the leasing company will be notified.

GSA fleet vehicles are not insured because the federal government is a self-insurer. If the other party or parties claim personal injury, or if there is property damage, SAs should refer the other party or parties to the SF-95, "Claim for Damage or Injury," and advise them to contact the DHS OIG Office of Counsel. SF-95 is available on the OPM web site.

C. Report of Inexplicable Damage - On occasion, vehicles are subject to acts of vandalism or other damage that may be caused by such things as debris, road conditions or other drivers (who intentionally do not report damage). Upon discovery, employees must immediately report inexplicable damage to their supervisors, prepare documentation requested by the supervisor and endeavor to make the necessary repairs to the affected GOV.

D. Report of Activation of Emergency Equipment - As soon as it is safe and practical to do so (no more than two hours afterwards) SAs must verbally report the activation of emergency equipment for any reason to their supervisor, including those instances wherein they may stop to render aid and assistance to the public. Supervisors must report the activation of emergency equipment to their SAC, who may require a written report of the incident.

E. Report of Exigent Use - As soon as it is safe and practical to do so (no more than two hours afterwards) employees must make a verbal report to their supervisor after utilizing a GOV in exigent circumstances. Within 48 hours of the incident, employees must file a written report describing the exigent nature of the use of a GOV through their chain of command to the AIGI.

F. Report Contact with Law Enforcement - Employees who are contacted by law enforcement concerning the violation of traffic or criminal laws while operating a GOV must report such contact to their supervisor within one hour of the contact. This notification requirement does not include citations for parking offenses or other contacts that do not involve a citation or enforcement action. In turn, supervisors may require the employee to prepare a written report of the incident in the form of an email or a formal memorandum**.** *Note: For the safety of all parties involved, when armed SAs (whether on or off duty, whether in a GOV or privately owned vehicle) are confronted or come in contact with other law enforcement (i. e. , a traffic stop, etc.),they should, as soon as is practical, notify the officer that they are armed, and upon the officer's request, or as*

deliberately as possible so as not to provoke a "blue on blue" situation, produce their respective badge and credentials to the law enforcement official.

G. Report of Arrest for Certain Driving Offenses or the Suspension/Revocation of Driving Privileges - In order to minimize the potential for liability associated with the operation of its fleet, the OIG must ensure that its GOV operators remain responsible drivers. As such, employees who have been arrested for certain driving-related offenses or have been subject to a suspension or revocation of driving privileges pose significant financial liability to the agency. Any employee who has been arrested for Driving Under the Influence or Driving while Intoxicated, or has been subject to any limitation, suspension or revocation of driving privileges must report such action to their immediate supervisor within 48 hours of the occurrence. The operation of a GOV after having failed to report being the subject of such an action will be considered to be the willful misuse of a GOV and subject the affected employee to the penalties of Title 31 U. S. C. § 1349.

H. Annual Certification of Use - The employee's immediate supervisor must annually certify the eligibility for HTW use of a GOV for each employee that is authorized for such use. INV Form 86A **(Exhibit 4-6A)**

4. 12 News Media Inquiries

The OIG will conform to DOJ guidelines concerning the release of information relating to criminal and civil proceedings as outlined in 28 CFR § 50. 2. Additionally, in the course of any joint investigation with the Federal Bureau of Investigations (FBI), any news release must be coordinated with the FBI and DOJ. SACs should refer any media inquiries or potential press releases to the AIGI.

Within the scope of the above referenced guidelines, SACs shall have the authority to participate in media events held by the United States Attorney's Offices (USAO) to speak about DHS OIG involvement in an investigation. Prompt notification will be made to the DAIGI pursuant to any media inquiry or prior to any participation in a media event. Likewise, if contacted by the media on a matter of public information (e. g. arrest, indictment), SACs have the authority to clarify and provide factual comment on DHS OIG involvement related to the public information.

All media inquiries should be directed to the media affairs officer at (202) 254-4100.

4. 13 Congressional Inquiries

It is the IG's responsibility to keep the Department of Homeland Security and Congress fully informed concerning matters of mutual interest. All congressional letters addressed to the IG, or forwarded to the OIG by DHS, will be referred to IQO Intake Division, who is responsible for tracking Congressional inquiries relating to INV matters.

4. 14 Official Passports

All INV SAs may obtain an Official Passport as needed. The procedures for obtaining/renewing an Official Passport are coordinated through the HOD.

- SAs shall complete the appropriate Department of State (DOS) Passport Application Form (DS-11), or Passport Renewal Form (DS-82). These forms can also be obtained on line at www. state. gov. (**Exhibits 4-8 and 4-9)**
- The completed passport application form and photographs (if renewal, old passport must also be submitted) will be provided to HOD for processing. Additionally, if this is the SAs initial application for a passport, either personal or official, an original birth certificate must also be provided with the application.
- If an SA transfers from another federal agency and has an active passport with that agency, he/she is eligible to transfer their passport to DHS-OIG. To transfer a passport, the FO shall contact HOD and provide the name of their former agency, passport inquiry contact information for their former agency, and a completed DS-4085**. (Exhibit 4-10)** This form can also be obtained online at www. state. gov. HOD shall coordinate with the former agency to have the active passport returned to DS. HOD shall complete a letter acknowledging the transfer of the passport (signed by the DAIGI) and send it to DOS.
- HOD shall be responsible for obtaining the new, renewed or transferred passports from DOS and sending them to the appropriate FO.

4. 15 Reporting Requirements for Foreign Travel

Personal Travel
All employees must report any foreign travel, official or personal, to the Office of Security within the OIG Office of Management. The travel should be reported 30 days in advance whenever possible with a detailed travel itinerary and list of anticipated foreign contacts. Employees are required to provide the Notification of Foreign Travel (DHS Form 11053-1). **(Exhibit 4-11)**

Official Travel
No investigation shall be conducted by SAs outside of the United States without the approval of the AIGI. SA's are not authorized to carry weapons outside the U. S. on official business unless approved in advance by the AIGI, DOS, and the host country.

All official foreign travel requires prior coordination by the affected office with the U. S. Department of State (DOS) Regional Security Officer (RSO) for the country to be visited to request country clearance. Diplomatic Security (DS) Command Center: 571-345-3146
Country Clearance: https://ecc. state. gov/security/EccLogin. aspx

If Country Clearance is obtained through the DOS automated system, written e-mail notification to the DAIGI is required. **(Exhibit 4-12)** DHS employees will adhere to all DOS requirements and regulations for the specific country visit. For example, if traveling to Mexico we shall comport with the Brownsville MOU.

4. 16 VOLUNTARY POST OF DUTY TRANSFER POLICY

An employee interested in a self-funded Voluntary Transfer to another investigative office, that has a position/Full Time Equivalent (FTE) available, need to notify his/her SAC/local management via memorandum. The local SAC shall route the request through the appropriate Director. (Should a position not be available in the requested location an employee may still submit the memorandum to express his/her office of preference so that they may be considered when a position becomes available.)

To be eligible an employee needs:

1. To have completed at least one (1) official rating cycle.
2. Must have achieved a performance rating of at least Achieved Expectations in the most recent rating cycle.
3. Must have no pending internal investigations or disciplinary actions.

The memorandum should state the desired transfer location, proof of performance rating, and an attached signed waiver in which the employee agrees to be personally responsible for all expenses related to the transfer and agrees that the OIG is not liable for any of those expenses.

If the employee's current (losing) SAC determines that the transfer is in the best interest of the OIG's investigative mission in that office's area of responsibility, and verifies the employees eligibility, he/she will contact the requested office (gaining) SAC to determine if that SAC is agreeable to the transfer. This can be done verbally or through email. Once the two SACs have agreed this will be documented in a memorandum to the DAIGI signed by both SACs. The DAIGI will make the decision regarding the transfer after reviewing the memorandum from the SACs and consultation with other management officials which may be in verbal, email and/or written memorandum.

The DAIGI will provide written response of the decision in memorandum format to the employee seeking the voluntary transfer self-funded transfer. The operational needs of the OIG will be the deciding factor. The DAIGI will notify the involved SACs of the decision.

If the transfer is approved, the reporting date will be determined and agreed upon by the affected SACs. Only the IG can grant the transferring employee a maximum of 40 hours administrative leave (with pay).

The losing SAC is responsible for notifying the appropriate Headquarters entities (security, Information Technology Division (ITD), Human Resources), so that the appropriate physical field office accesses are reassigned, all ITD systems can be accessed at the gaining office and Human Resources can make the appropriate payroll adjustments to reflect the new location/state. The losing office will forward the employee's personnel file to the gaining office.

A list of career openings will be posted on the internet OIG central and OIG INV employees will be notified via email of career openings.

If more than one (1) employee is interested in a voluntary self-funded transfer to an available position in the same location, the decision will be made by the DAIGI based on, but not limited to, the following factors:

1. Seniority within DHS OIG INV
2. Employee Performance history
3. Any specialized skills or knowledge
4. The operational needs of the office with the opening
5. Length of service at a particular location.

The employee receiving the transfer cannot make a claim against the agency for reimbursement following the move to any governmental agency, to include OPM, or through legal action. The decision of the DAIGI is final and not subject to the OIG internal grievance policy.

4. 17 PROCEDURE FOR REPORTING THE DEATH OF A DHS OIG EMPLOYEE

Upon learning of an OIG employee's death, the employee's supervisor should immediately notify the appropriate FODs and Human Resources.

Email notification of the employee's death will be forwarded to all employees by INV.

4. 18 PROCEDURE FOR RECOMMENDING SOP AND POLICY CHANGES

Written Standard Operating Procedures (SOP) and policies are foundational elements of any system in which individual and units are held accountable to laws, rules, and regulations. INV requires a consistent methodology to propose, consider, and implement new or modified SOPs and policies and codify them in the SAH and the INV Administrative Manual.

INV shall utilize this defined process when seeking to create or modify SOPs and/or policies. INV shall utilize this SOP Proposal Form **(Exhibit 4-13)** when creating and amending SOP and/or policy as well as developing procedures designed to support existing policies.

Proposals can be derived from a myriad of sources including, but not limited to the following:

1. Internal/External Inspection Findings, Recommendations, or Observations
2. Field Offices
3. Supervisory & Non-Supervisory Working Groups
4. Changes in Law, Rules, Regulations
5. Changes in technology

Once the proposal is conceived and reduced to writing within this form, it shall be submitted to the FOD through the employee's respective supervisor. If the FOD determines is a viable proposal, then it will be reviewed by the following:

- Special Agent Handbook Committee
- HOD

- Counsel (legal sufficiency only)
- DAIGI
- AIGI

CHAPTER 4. 0 – EXHIBITS

4-10 D-4085, Application for Additional VISA Pages or Miscellaneous Passport Services

4-11 DHS Form 11053-1Notification of Foreign Travel

4-12 Country Clearance Memorandum

4-13 SOP Proposal Form

Exhibit 4-1, INV Form-90, Employee Property Inventory Log

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security
Washington, DC 20528 / www.oig.dhs.gov

EMPLOYEE PROPERTY INVENTORY LOG

EMPLOYEE :

Office:
]

[redacted]

Description	Serial Number	Date Received	S/A's Initials	Date Returned	Recipient's Initials	Remarks

INV FORM-90

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security
Washington, DC 20528 / www.oig.dhs.gov

EMPLOYEE PROPERTY INVENTORY LOG

EMPLOYEE :

Office:
]

Equipment Type	Description	Serial Number	Date Received	S/A's Initials	Date Returned	Recipient's Initials	Remarks
Laptop Computer							
Docking Station							

Exhibit 4-1A, INV Form-90.1, Items Property Transfer Transaction Record

Print Form

DEPARTMENT OF HOMELAND SECURITY
OFFICE OF INSPECTOR GENERAL

ITEMS PROPERTY TRANSFER TRANSACTION RECORD
(Submit in duplicate to the gaining Custodial Officer)

DOCUMENT CONTROL NUMBER

TO:	FROM: *(Transferor's Name and Office/Please Print or Type)*	CURRENT ORGANIZATIONAL SEGMENT CODE *(Specify Division Office FPC For Investigative Equipment)*
TECHNICAL PROGRAM MANAGER, OFFICE OF TRAINING	SIGNATURE	RELEASE DATE

ITEM NUMBER	PROPERTY ITEM IDENTIFICATION NUMBER (SERIAL NUMBER)	ITEM DESCRIPTION *(Include Make, Model, Accessories)*

TO BE COMPLETED BY THE GAINING OFFICE

RECEIPT OF THE ABOVE LISTED PROPERTY IS HEREBY ACKNOWLEDGED

TRANSFEREE'S NAME AND OFFICE *(Please Print or Type)*	NEW ORGANIZATIONAL SEGMENT CODE *(Specify Division Office For Investigative Equipment)*

SIGNATURE

DATE OF RECEIPT (m m d d y y)

DHS-OIG Form 90.1 (02-2011) **Page 1 of 1** **TECHNICAL SUPPORT SECTION**

Exhibit 4-1B INV Form 90.5, Authorization for Destruction of Investigative Property

OFFICE OF INSPECTOR GENERAL

AUTHORIZATION FOR DESTRUCTION OF INVESTIGATIVE PROPERTY

PAGE ☐ OF ☐

tOFFICE OF INSPECTOR GENERAL DEPARTMENT OF HOMELAND SECURITY	DATE SUBMITTED:
REQUESTING OFFICE/ADDRESS:	POINT OF CONTACT/PHONE NUMBER:

ITEM #	SERIAL NUMBER	CONDITION	DESCRIPTION	APPROVED
t				

INV FORM 90.5 03/15/12

Exhibit 4-1C OIG Form 90.6 Declaration of Excess Personal Property

U. S. Department of Homeland Security
Office of Inspector General

Declaration of Excess Personal Property

4. Location of Property	5. Reporting Official (Signature)	1. Reporting Office	2. Date	3. Page___ of ___
	6. Contact Person, Address, Telephone/Fax Numbers	7. Special Instructions		
		8. Approving Official Signature and Title		

9. Property Identification

Item No. (a)	Name and Description of Article *(make, model, serial number)* (b)	Condition (c)	Quantity (d)	Acquisition Cost (e)

DHS-OIG Form 90.6 (07/2012)

Exhibit 4-2, INV Form-80, Annual Availability Pay Certification

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

AVAILABILITY PAY CERTIFICATION

MEMORANDUM FOR: Assistant Inspector General for Investigations

SUBJECT: *Availability Pay*

I, Special Agent , certify that I expect to be able to perform official duties during unscheduled duty hours and agree to be available for unscheduled duty based on the needs of the Office of Inspector General, U.S. Department of Homeland Security.

_____
(Printed Name)
Special Agent

_____
(Signature)

_____
(Date)

Concur: _____
(Signature)
Special Agent-in-Charge

Date: _____

INV FORM-80

Exhibit 4-2A, INV Form 97A, Memorandum, Annual Employee Certifications

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

MEMORANDUM – ANNUAL EMPLOYEE CERTIFICATIONS
FISCAL YEAR 2015

The employee listed below has reviewed and is familiar with the following items:

Special Agent Handbook (SAH) – DHS/OIG – Office of Investigations
Standards of Ethical Conduct for Government Employees – (SAH, Section 4.2)
TSA Regulations for Flying Armed – (SAH, Section 5.6)
Use of Official Vehicles – (SAH, Section 4.11)

_____
(Printed Name of Special Agent)

_____ _____
(Signature of Special Agent) *(Date)*

_____ _____
(Signature of Special Agent-in-Charge) *(Date)*

Exhibit 4-2B, Request for Authorization to Participate in Physical Training

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

MEMORANDUM FOR: *(Name)*
SPECIAL AGENT IN CHARGE
OFFICE OF INVESTIGATIONS – *(Office Name)*

FROM: *(Name of Agent)*
Special Agent-(Office Name)

SUBJECT: **Physical Training Certification – Fiscal Year**

This memorandum is to request authorization to participate in physical training three hours per week during the workday as described in the Department of Homeland Security, Office of Inspector General, Special Agent Handbook. The physical training to be performed includes weight training, swimming, calisthenics, bicycling, and cardiovascular training such as the Stairmaster, treadmill, walking, jogging and running.

Approved:_____ ***Date:***_____

INV FORM-02

Exhibit 4-3, INV Form-81, Annual Certification of LEAP

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

ANNUAL CERTIFICATION OF AVAILABLE HOURS

DATE:

MEMORANDUM FOR: Assistant Inspector General for Investigations

FROM: Special Agent-in-Charge

SUBJECT: *Annual Certification of Availability Hours*

The personnel listed below performed official duties during this past year during unscheduled hours of duty or were available to perform work during unscheduled hours of duty and are qualified for availability pay in accordance with the Law Enforcement Availability Pay Act of 1994 (Section 633 of Public Law 103-329, 5 U.S.C. § 5545a).

By this report, I certify the agents listed below were under my supervision during this reporting period, and in accordance with requirements of their official duties, performed work during unscheduled hours of duty and qualify for availability pay. I also certify that the Special Agents listed below are expected to continue to meet these requirements:

INV FORM-81

Exhibit 4-4, Memorandum Requesting Issuance of Inactive Commemorative Credentials and Badge

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Specify Date

MEMORANDUM FOR: Deputy Assistant Inspector General
for Investigations

FROM: Special Agent in Charge
(Field Office Name)

SUBJECT: Request for Issuance of Inactive Credentials and to Retain the OIG Issued Badge

I am requesting your authorization for Special Agent (SA) _____, assigned to the field or sub-office name to be issued inactive credentials and (or) for him/her to retain their OIG issued wallet badge. The inactive credentials and OIG badge will be used on a plaque or other similar commemorative media as part of a commemorative presentation to be made to SA Jones on the occasion of his/her retirement. SA Jones is scheduled to retire on _____ (or has retired on_____). The requested credentials and (or) badge will not be issued as identification for purposes of carrying a concealed firearm under the Law Enforcement Officers Protection Act of 2004.

If you have questions concerning this request, please call me at (XXX) XXX-XXXX.

_____ _____
Approve Date

_____ _____
Disapprove Date

Exhibit 4-4A, DHS Management Directive 257-01, LEOSA

V. Policy and Requirements

A. The guidance set forth below is not intended to and does not create any rights, privileges, or benefits, substantive or procedural, enforceable by any party against the United States, its departments, agencies or other entities, its officers or employees, or any other person. Nothing in this Directive impairs or otherwise affects the right of an individual to keep and bear arms under the Second Amendment to the Constitution of the United States.

B. The provisions of LEOSA pertaining to qualified retired law enforcement officers will be implemented by DHS Components in as cost-effective and efficient manner as possible that meets the requirements and intent of the statute as well as the LEOSA concerns of DHS and predecessor agency law enforcement retirees.

C. LEOSA essentially exempts "a qualified retired law enforcement officer" (hereafter "retiree") who is carrying the required "identification" from most State and local laws that prohibit the carrying of concealed weapons. LEOSA permits carrying a concealed firearm that has been shipped or transported in interstate commerce, subject to certain restrictions.

D. LEOSA requires that, at least once each year, retirees carrying a concealed firearm under its provisions "be tested or otherwise be found ...to meet ...standards...to carry a firearm of the same type as the concealed firearm." LEOSA provides that this annual testing or otherwise being "found...to meet...standards" can be conducted either by the agency from which the retiree retired or by some other entity authorized to issue "a certification ...by the State in which the [retiree] resides" indicating that the retiree has "been tested or otherwise found by the State to meet the standards established by the State for training and qualification for active law enforcement officers..."

E. As explained below, as a matter of policy, DHS Components will not perform or assist with the required annual firearms testing for retirees.

F. The "identification" required to be carried by retirees tested under State standards includes both a photographic identification issued by the agency from which the retiree retired and an up-to-date "certification issued by the State" concerning annual testing and qualification.

LEOSA does not exempt covered retirees from other federal laws or regulations, including any restrictions on the carriage of firearms on transportation systems (such as commercial airlines) and does not confer on the retiree any law enforcement power or authority to use the firearm.

1. **Photographic Identification**: DHS Components currently allow law enforcement officers who are retiring in good standing to retain their credentials (containing their photograph, name, signature and position title) stamped or perforated with the word "Retired." To minimize costs and administrative burden, Components may utilize these "Retired" credentials as the "Photographic Identification" required by the LEOSA. Components are also authorized, but not required, to issue an additional photographic identification, specifically for LEOSA purposes, containing the retiree's photograph, name, signature, and the title of the law enforcement position from which he or she retired, proceeded by the word "Retired," and the name of the Component or Subcomponent from which the individual retired (e.g., "Retired Special Agent, U.S. Customs Service"). Components are authorized to issue these additional LEOSA identification cards to retirees from their present Components and to retirees from those parts of their predecessor agencies that were merged into their present Components (e.g., Border Patrol into U.S. Customs & Border Protection [CBP], Customs and INS investigational elements into U.S. Immigration & Customs Enforcement [ICE]). All LEOSA identification cards issued must meet Department-wide identification standards in effect at the time of issuance. Because of unavailability of or excessive cost/difficulty of retrieving older records, Components may establish cut-off dates, and advise retirees who retired before those dates that their requests for LEOSA identification cards cannot be honored.

2. **Certification Issued by the State**: Under no circumstances will DHS Components perform or assist with annual firearms testing for their retirees. To meet LEOSA requirements, law enforcement retirees from DHS Components and their predecessor agencies must "be tested or otherwise be found ...to meet ...standards" by a non-DHS entity authorized to issue "a certification ....by the State in which the [retiree] resides" indicating that the retiree has "been tested or otherwise found by the State to meet the standards established by the State for training and qualification for active law enforcement officers..." The availability of such "certifications" varies by State, and it is the responsibility of the individual DHS law enforcement retiree to determine and meet the requirements of his or her state of residence for obtaining this "certification."

G. Whenever the retiree experiences an event which would disqualify him or her from receiving a firearm under 18 U.S.C. 922(g) or (n), the retiree immediately notifies the Component and the certifying entity in the State of residence. On an annual basis, the retiree shall certify to the Component in writing, or in a manner acceptable to the Component, that the retiree is not subject to any of the disqualifiers in 18 U.S.C. 922(g) and (n) that would prohibit an individual from receiving a firearm.

VI. Questions

Address any questions regarding this Directive to the Director of Law Enforcement Policy in the Office of Policy Development.

Elaine Duke
Under Secretary for Management

10 Oct 2004
Date

Exhibit 4-4B, DHS Management Directive 257-01-001, Instruction Guide on the LEOSA

Department of Homeland Security
DHS Directives System
Instruction Number: 257-01-001
Revision Number: 00
Issue Date: 11/05/2008

INSTRUCTION GUIDE ON THE LAW ENFORCEMENT OFFICERS SAFETY ACT

I. Purpose

This Instruction implements the Department of Homeland Security (DHS) Directive 257-01, Law Enforcement Officers Safety Act, establishes procedures with respect to retiring and retired qualified law enforcement officers and the application of the provisions of the Law Enforcement Officers Safety Act of 2004 (LEOSA).

II. Scope

This Instruction applies to all DHS Components that have retired officers who meet the definition of "qualified retired law enforcement officers" set out in the Law Enforcement Officers Safety Act (LEOSA) and defined in Section IV below. This Instruction applies to DHS Components' handling of LEOSA matters with qualified law enforcement officers who have retired from DHS Components since DHS was formed in 2003, with future such retirees, and with such retirees from predecessor agencies when these retirees make LEOSA inquiries with appropriate DHS successor Components.

III. Background

A. The Law Enforcement Officers Safety Act of 2004 (hereinafter "LEOSA" or "the act") was signed into law July 22, 2004. With certain limitations and conditions, LEOSA exempts qualified retired law enforcement officers ("retirees") from most State and local laws that prohibit the carriage of concealed firearms. LEOSA extends this exemption to any qualified law enforcement officer, as that term is defined by the Act, including local, State, and Federal law enforcement personnel. LEOSA, however, does not exempt these individuals from other Federal laws or regulations, including any restrictions on firearms carriage on transportation systems such as commercial airlines, nor does it extend to these individuals any new authority for the use of firearms or any new law enforcement powers.

B. Although LEOSA preempts State and local laws prohibiting the carrying of concealed firearms, it contains two exceptions. First, it is not construed to supersede or limit State laws that "permit private persons or entities to prohibit or restrict the possession of concealed firearms on their property."[1] Second, it does not limit or supersede State laws that "prohibit or restrict the possession of firearms on any State or local government property, installation, building, base, or park."[2]

IV. Definitions

A. ***Identification***: Consistent with the provisions of LEOSA at 18 U.S.C. 926C(d)(2), identification for the purposes of this Instruction Guide and accompanying Directive is defined as:

1. A photographic identification issued by the organization or Component from which the individual retired from service as a law enforcement officer indicating that the individual is "retired"; and

2. A certification issued by the State in which the individual resides that indicates that the individual has, not less recently than one year before the date the individual is carrying the concealed firearm, been tested or otherwise found by the State to meet the standards established by the State for training and qualification for active law enforcement officers to carry a firearm of the same type as the concealed firearm.

DHS Components will not perform or assist with the required annual firearms testing for retirees.

B. ***Qualified Retired Law Enforcement Officer***: Consistent with the provisions of LEOSA at 18 U.S.C. 926C(c), a qualified retired law enforcement officer is an officer or agent retired from a DHS Component or predecessor agency who:

1. Retired in good standing from service with a public agency as a law enforcement officer, other than for reasons of mental instability;

2. Before such retirement, was authorized by law to engage in or supervise the prevention, detection, investigation, or prosecution of, or the incarceration of any person for, any violation of law, and had statutory powers of arrest;

---

[1] 18 U.S.C. § 926C(b)(1).

[2] 18 U.S.C. § 926C(b)(2).

3. Before such retirement, was regularly employed as a law enforcement officer for an aggregate of 15 years or more[3]; or

Retired from service with such organization or Component, after completing any applicable probationary period of such service, due to a service-connected disability, as determined by the organization or Component;

4. Has a nonforfeitable right to benefits under the retirement plan of the agency;

5. During the most recent 12-month period, has met, at the expense of the individual, the State's standards for training and qualification for active law enforcement officers to carry firearms;

6. Is not under the influence of alcohol or another intoxicating or hallucinatory drug or substance; and

7. Is not prohibited by Federal law from receiving a firearm.

The Department recognizes that individuals who meet the definition of a qualified retired law enforcement officer under the Act may or may not meet the definition of a law enforcement officer under the Civil Service Retirement System or the Federal Employees Retirement System.

C. ***Those Prohibited by Federal Law From Receiving a Firearm***: Consistent with the provisions of 18 U.S.C. 922(g) and (n), those prohibited from receiving a firearm include any person who[4]:

1. Has been convicted in any court of a crime punishable by imprisonment for a term exceeding one year;

2. Is a fugitive from justice;

3. Is an unlawful user of or addicted to any controlled substance (as defined in section 102 of the Controlled Substances Act (21 U.S.C. 802));

4. Has been adjudicated as a mental defective or who has been committed to a mental institution;

---

[3] The 15-year period includes any time in the U.S. armed forces specifically devoted to training for and full-time service in law enforcement military occupational specialties.

4 Federal law also precludes aliens from receiving a firearm if the alien is illegally or unlawfully present in the United States or, except as provided in 18 U.S.C. 922(y)(2), has been admitted to the United States under a non-immigrant visa (as that term is defined in section 101(a)(26) of the Immigration and Nationality Act, 8 U.S.C. 1101(a)(26)).

5. Has been discharged from the Armed Forces under dishonorable conditions;

6. Having been a citizen of the United States, has renounced his citizenship;

7. Is subject to a court order that:

a. Was issued after a hearing of which such person received actual notice, and at which such person had an opportunity to participate;

b. Restrains such person from harassing, stalking, or threatening an intimate partner of such person or child of such intimate partner or person, or engaging in other conduct that would place an intimate partner in reasonable fear of bodily injury to the partner or child; and

c. Includes a finding that such person represents a credible threat to the physical safety of such intimate partner or child; or by its terms explicitly prohibits the use, attempted use, or threatened use of physical force against such intimate partner or child that would reasonably be expected to cause bodily injury;

8. Has been convicted in any court of a misdemeanor crime of domestic violence; or

9. Is under indictment for a crime punishable by imprisonment for a term exceeding one year.

V. Content and Procedures

A. Law Enforcement Officers About to Retire from DHS Components:

Each Component will issue a copy of LEOSA and a LEOSA Fact Sheet (or similar informational document) to its law enforcement officers and agents about to retire, as part of their retirement processing and in accordance with Component procedures. That Fact Sheet will:

1. Include information regarding LEOSA provisions exempting qualified retired law enforcement officers from certain state and local statutes prohibiting the carrying of concealed weapons.

2. Include notice that LEOSA contains no exemption from Federal statutes and regulations relating to the carrying of firearms aboard commercial aircraft and that LEOSA does not confer upon retirees any law enforcement status or arrest powers.

3. Set out the list of requirements to be considered a "qualified retired law enforcement officer" under LEOSA as well as the list of conditions that would result in a retiring law enforcement officer or agent being prohibited by Federal law from receiving a firearm.

4. Caution retiring law enforcement officers that if at any time they no longer meet the definition of a qualified retired law enforcement officer, or fall within one of the categories of individuals prohibited by Federal law from receiving a firearm, they are no longer covered by LEOSA provisions or exemptions.

5. On an annual basis, the retiree shall certify to the Component in writing, or in a manner acceptable to the Component, that the retiree is not subject to any of the disqualifiers in 18 U.S.C. 922(g) and (n) that would prohibit an individual from receiving a firearm.

6. Make clear that, based upon Component-specific procedures, the "photographic identification" referred to in LEOSA will be either the credentials (stamped or perforated "Retired") that law enforcement officers who retire in good standing will be allowed to retain when they retire or a LEOSA-specific Retired identification credential. (If applicable, the Fact Sheet will include Component instructions on how retirees request the LEOSA-specific identification.)

7. Also, make clear that retirees must obtain their annual State firearms testing "certifications" from a non-DHS issuing authority in the State in which the retiree resides, and that it is the individual retiree's responsibility to determine the requirements of his or her state of residence regarding such certifications.

8. Emphasize the importance of retirees having their "photographic identification" and up-to-date annual State firearms testing certification in their possession at all times they will be carrying a concealed firearm under the authority of LEOSA.

B. Law Enforcement Officers Who Have Previously Retired from DHS Components (or their Predecessor Agencies):

1. Components will, in accordance with Component-specific procedures to be developed by each Component, issue a copy of the LEOSA and a LEOSA Fact Sheet (similar to the Fact Sheet described above) to law enforcement officers who have previously retired from the Component or the Component's predecessor agencies and who make inquiries about LEOSA.

2. Fact Sheets from Components electing not to issue additional LEOSA-specific Retired identification cards to law enforcement retirees who, based upon their retiring in good standing, were allowed to retain and still have their active-service credentials (stamped or perforated with the word "Retired") may advise such retirees that they need only obtain the annual State firearms testing certification to be covered by LEOSA, provided that they meet all the other requirements of LEOSA as set out in the statute itself and as highlighted in the Fact Sheet.

3. Fact Sheets from Components electing to issue additional LEOSA-specific Retired identification cards will include Component-specific instructions for requesting such cards. Retirees may be required to submit supporting documentation including results of up-to-date criminal history checks and undergo further vetting as the Component sees fit. Fact Sheets from Components that have established cut-off dates because of unavailability of or excessive cost/difficulty of retrieving older records should advise retirees who retired before those dates that their requests cannot be honored (and include an explanation of the records availability retrieval reasons why their requests cannot be honored).

4. It is within the discretion of DHS and its Components to determine whether to issue the retired law enforcement identification called for under the Act. Should the Component make a finding that the subject is not qualified, or enter into an agreement in which the subject agrees that he or she is not qualified, the subject is not issued the retired law enforcement officer identification described above. Any appeal concerning a retiree's eligibility for an identification credential is resolved at the Component level.

5. If the retiree believes that the records relied on by the Component to make its determination were not correct, the retiree can, consistent with the Privacy Act, 5 U.S.C. 552a, seek the records which formed the basis of the determination and ask the agency to correct the records if the retiree believes the records to be inaccurate. The resolution of any correction shall be made at the Component level.

VI. Questions

A. Address any questions regarding this Instruction to the Director of Law Enforcement Policy in the Office of Policy Development.

B. This Instruction Guide contains one appendix:

Appendix A: Sample LEOSA Fact Sheet

Stewart A. Baker
Assistant Secretary, Office of Policy

Date

APPENDIX A

SAMPLE LEOSA FACT SHEET

A copy of the Law Enforcement Officers Safety Act (LEOSA, Public Law 108-277, 18 U.S.C. 926B-C) is attached. Your attention is directed especially to the provisions of Section 3 of the Act (18 U.S.C. 926C) entitled "Exemption of Qualified Retired Law Enforcement Officers from State Laws Prohibiting the Carrying of Concealed Firearms".

You will note that Section 3 of LEOSA is essentially a State law preemption statute in that it exempts "a qualified retired law enforcement officer" (see the definition below) who is carrying the required "identification" (see the definition below) from most (but not all) state and local laws that prohibit the carrying of concealed weapons. It is important to note that LEOSA contains no exemption for retirees from Federal statutes and regulations (to include those relating to firearms aboard commercial aircraft).

"A Qualified Retired Law Enforcement Officer" is, consistent with the provisions of LEOSA at 18 U.S.C. 926C(c), an officer or agent retired from a DHS Component or predecessor agency who:

A. Retired in good standing from service with a public agency as a law enforcement officer, other than for reasons of mental instability;

B. Before such retirement, was authorized by law to engage in or supervise the prevention, detection, investigation, or prosecution of, or the incarceration of any person for, any violation of law, and had statutory powers of arrest;

C. Before such retirement, was regularly employed as a law enforcement officer for an aggregate of 15 years or more; or

Retired from service with such agency, after completing any applicable probationary period of such service, due to a service-connected disability, as determined by the Component;

D. Has a non-forfeitable right to benefits under the retirement plan of the Component;

E. During the most recent 12-month period, has met, at the expense of the individual, the State's standards for training and qualification for active law enforcement officers to carry firearms;

F. Is not under the influence of alcohol or another intoxicating or hallucinatory drug or substance; and

G. Is not prohibited by Federal law from receiving a firearm.

APPENDIX A

"Those Prohibited by Federal Law From Receiving a Firearm" include, consistent with the provisions of 18 U.S.C. 922(g) and (n), any person who[5]:

A. Has been convicted in any court of, a crime punishable by imprisonment for a term exceeding one year;

B. Is a fugitive from justice;

C. Is an unlawful user of or addicted to any controlled substance (as defined in section 102 of the Controlled Substances Act (21 U.S.C. 802));

D. Has been adjudicated as a mental defective or who has been committed to a mental institution;

E. Has been discharged from the Armed Forces under dishonorable conditions;

F. Having been a citizen of the United States, has renounced his or her citizenship;

G. Is subject to a court order that:

(1) Was issued after a hearing of which such person received actual notice, and at which such person had an opportunity to participate;

(2) Restrains such person from harassing, stalking, or threatening an intimate partner of such person or child of such intimate partner or person, or engaging in other conduct that would place an intimate partner in reasonable fear of bodily injury to the partner or child; and

(3) Includes a finding that such person represents a credible threat to the physical safety of such intimate partner or child; or by its terms explicitly prohibits the use, attempted use, or threatened use of physical force against such intimate partner or child that would reasonably be expected to cause bodily injury;

H. Has been convicted in any court of a misdemeanor crime of domestic violence; or

---

5 Federal law also precludes aliens from receiving a firearm if the alien is illegally or unlawfully present in the United States or, except as provided in 18 U.S.C. 922(y)(2), has been admitted to the United States under a non-immigrant visa (as that term is defined in section 101(a)(26) of the Immigration and Nationality Act, 8 U.S.C. 1101(a)(26)).

APPENDIX A

I. Is under indictment for a crime punishable by imprisonment for a term exceeding one year.

It is important to note that retirees who either now or at some future time no longer meet any one of the requirements or become subject to any one of these prohibitions set out above would no longer be covered under the exemptions from State and local firearms laws contained in LEOSA.

On an annual basis, the retiree shall certify to the Component in writing, or in a manner acceptable to the Component, that the retiree is not subject to any of the disqualifiers in 18 U.S.C. 922(g) and (n) that would prohibit an individual from receiving a firearm.

"Identification" is, for the purposes of DHS's implementation of the LEOSA, and consistent with the provisions of LEOSA at 18 U.S.C. 926C(d)(2), defined as:

A. A photographic identification issued by the Component from which the individual retired from service as a law enforcement officer; and

B. A certification issued by the State in which the individual resides that indicates that the individual has, not less recently than one year before the date the individual is carrying the concealed firearm, been tested or otherwise found by the State to meet the standards established by the State for training and qualification for active law enforcement officers to carry a firearm of the same type as the concealed firearm.

Certifications Issued By the State: To meet LEOSA requirements, law enforcement retirees from DHS Components and their predecessor agencies must annually "be tested or otherwise be found ...to meet ...standards" by a non-DHS entity authorized to issue "a certification ...by the State in which the [retiree] resides" indicating that the retiree has "been tested or otherwise found by the State to meet the standards established by the State for training and qualification for active law enforcement officers..." The availability of such "certifications" varies by State, and it is the responsibility of the individual DHS law enforcement retiree to determine and meet the requirements of his or her state of residence for obtaining this "certification." DHS Components will not perform or assist with annual firearms testing for their retirees.

Retirees are reminded:

A. That they must have their DHS Component (or predecessor agency) "photographic identification" **and** up-to-date annual State firearms testing "certification" in their possession at all times when they will be carrying a concealed firearm under the authority of LEOSA. Possession of the "photographic identification" alone does not authorize a retiree to carry a concealed firearm.

APPENDIX A

B. That, in order to carry a concealed weapon under the authority of LEOSA, they must, in addition to having the required "photographic identification" and current State firearms testing "certification" in their possession, also be in compliance with all of the other requirements (set out above) of the Act concerning being a "Qualified Retired Law Enforcement Officer" who is not "Prohibited by Federal Law From Receiving a Firearm".

C. That the required DHS Component (or predecessor agency) "photographic identification" is only for the purpose of identifying them as being a retired law enforcement officer from that Component or former agency. Neither that "identification" nor LEOSA confer law enforcement status or arrest authority. The identification and the LEOSA law enforcement status do not authorize retirees to engage in any law enforcement activities or investigations.

Exhibit 4-5, Application for Retired Law Enforcement Official Credentials

APPLICATION FOR RETIRED LAW ENFORCEMENT OFFICIAL CREDENTIALS

I _____, born _____ herby make application for the
(applicant) (date of birth)
issuance of Retired Law Enforcement Official Credentials. I certify that I retired in good standing as a special agent with the Department of Homeland Security, Office of Inspector general. I hereby attest that, to the best of my knowledge, I am not prohibited by Federal law from purchasing, receiving, or carrying a firearm. In so attesting, I understand that Title 18 of the United States Code prohibits the following persons from purchasing, receiving, or carrying a firearm.

(1) those under indictment for or convicted of a crime punishable by imprisonment for a term exceeding one year;
(2) fugitives from justice;
(3) unlawful users and/or addicts of any controlled substances;
(4) those adjudicated as mentally defective or who have been involuntarily committed to a mental institution or otherwise judged incompetent to handle their own affairs;
(5) illegal aliens or aliens admitted to the United States under a nonimmigrant visa;
(6) those dishonorably discharged from the U.S. Armed Forces;
(7) those who have renounced their U.S. citizenship;
(8) subjects of a protective order; and
(9) those convicted of a misdemeanor crime of domestic violence.

Name: _____ Date: _____

AUTHORIZATION TO PERFORM A NATIONAL CRIME INFORMATION CENTER (NCIC) DATABASE CHECK

I herby authorize the Department of Homeland Security, Office of Inspector General to perform the necessary investigation, including but not limited to, a National Crime Information Center (NCIC) database check to confirm that I am not prohibited by Federal law from purchasing, receiving or carrying a firearm.

My statements on this form are true, complete, and correct to the best of my knowledge and belief; and are made in good faith. I understand that a knowing and willful false statement on the application can be punishable by a fine or imprisonment or both.

_____
Applicant Signature

Subscribed to before on this _____day of _____20__, at _____
(city)

_____.
(state)

_____ _____
Notary Date My Commission Expires

Exhibit 4-5A, Annual Certification for Retired Law Enforcement Officer Credentials

ANNUAL CERTIFICATION FOR RETIRED LAW ENFORCEMENT OFFICIAL CREDENTIALS

I _____, hereby certify that the Department of Homeland Security, Office of the Inspector General previously issued me Retired Law Enforcement Official Credentials for purposes of identification under Public Law 108-277, the Law Enforcement Safety Act of 2004. I hereby attest that, to the best of my knowledge, I am not prohibited by Federal law from purchasing, receiving, or carrying a firearm. In so attesting, I understand that Title 18 of the United States Code prohibits the following persons from purchasing, receiving, or carrying a firearm.

(1) those under indictment for or convicted of a crime punishable by imprisonment for a term exceeding one year;
(2) fugitives from justice;
(3) unlawful users and/or addicts of any controlled substances;
(4) those adjudicated as mentally defective or who have been involuntarily committed to a mental institution or otherwise judged incompetent to handle their own affairs;
(5) illegal aliens or aliens admitted to the United States under a nonimmigrant visa;
(6) those dishonorably discharged from the U.S. Armed Forces;
(7) those who have renounced their U.S. citizenship;
(8) subjects of a protective order; and
(9) those convicted of a misdemeanor crime of domestic violence.

AUTHORIZATION TO PERFORM A NATIONAL CRIME INFORMATION CENTER (NCIC) DATABASE CHECK

I herby authorize the Department of Homeland Security, Office of Inspector General to perform the necessary investigation, including but not limited to, a National Crime Information Center (NCIC) database check to confirm that I am not prohibited by Federal law from purchasing, receiving or carrying a firearm.

My statements on this form are true, complete, and correct to the best of my knowledge and belief; and are made in good faith. I understand that a knowing and willful false statement on the application can be punishable by a fine or imprisonment or both.

Signature: _____ Date: _____

Exhibit 4-6, INV Form-86, Vehicle Usage Log

U.S. Department of Homeland Security
Office of Inspector General – Investigations

VEHICLE USAGE LOG

Vehicle Description _____ **Month & Year** _____
Vehicle Tag Number _____ **Office** _____

Complete in Longhand Check Boxes Below as Applicable					
Date	**Home-to-Work**	**Work-to-Home**	**After-Hours-Use**	**Miles Driven**	**Name**

VEHICLE USAGE TRACKING TOTALS

Ending Miles		HTW/WTH Days		Total Fuel Cost	
Beginning Miles		HTW Miles RT		Main. & Repair	
Total Miles Used		Gallons Used		Total Costs	
Description of Maintenance:					

(WTH = Work to Home and HTW = Home to Work)

Operator's Signature/Date	**Supervisor's Signature/Date**

Instructions on Completing and Submitting DHS OIG Vehicle Usage Log

- Law enforcement vehicle usage is for official use only.
- All monthly Vehicle Usage Logs and receipts must be completed and submitted for approval after the 8th of every month but no later that 15th. Receipts are to be forwarded to parties responsible for reconciliation and prompt payment.
- Vehicle logs are required for all law enforcement vehicles. All logs are to be retained for a period of three years in the vehicle file.

Home to Work and Extraordinary Use

Vehicle Description: Year, Make, and Model
Vehicle Tag Number: State or GSA License Plate Number
Month and Year: Month and year in which vehicle was operated
Office: Field Office: Code (e.g. WFO, HFO, SIU)
Date: Date is required for each day vehicle was used regardless if it involves HTW/WTH or after hours use.
Home-to-Work: Check box if vehicle is used strictly from Home to Work. Short stops for fuel, car wash, or minor maintenance is still considered HTW.
Work-to-Home: Same as above
Miles Driven: Total miles driven for that date
After-Hour-Use: Check box if vehicle is used after hours beyond the regular scheduled duty hours but not as a continuation of that day. Example of After Hours Use: Sat; & Sun. call out from home after ending your official workday.
Name: Operator's name using the vehicle for that day.

Vehicle Usage Tracking Totals. Information required for annual reports

Ending Miles: Ending miles on the last day of the month being reported
Beginning Miles: Beginning miles from the last month's prior Vehicle Usage Log
Total Miles: Total miles being reported for the month
HTW/WTH DAYS: Number of days in which both HYW and WTH boxes have been checked for that day
HTW MILES Round Trip: Round trip miles from HTW/WTH of vehicle operator if HTW/WTH is reported
Gallons Used: Total number of gallons used during the reporting period
Total Fuel Costs: Total fuel costs for vehicle during the reporting period
Maintenance and Repair Costs: ALL maintenance and repair costs performed during the reporting period. Attach copies of maintenance and repair receipts
Total Costs: Total costs for fuel maintenance and repairs during the reporting period
Description of Maintenance: Brief description of all maintenance performed during the reporting period
Operator's Signature/Date: Operator's signature who is responsible for submission of Vehicle Usage Log with date
Supervisor's Signature/Date: Supervisor's signature and date approving Vehicle Usage Log submitted

Exhibit 4-6A, INV Form-86A, Eligibility for Use of Government-Owned Vehicle for Home-to-Work Transportation

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

ELIGIBILITY FOR USE OF GOVERNMENT-OWNED VEHICLE (GOV) FOR HOME-TO-WORK TRANSPORTATION

OIG determines that _____ is eligible to operate a government-owned vehicle for home-to-work transportation between his or her official duty station and his or her permanent residence for a period of one year. Eligibility is based on the fact that the employee is actively engaged in criminal law enforcement duties, and transportation between the employee's residence and various locations is essential to the safe and efficient performance of those duties. Authorization is contingent upon the Secretary's approval.

OIG eligibility reviews will be conducted on a yearly basis.

_____	_____
Printed Name and Title of Employee	Printed Name and Title of Supervisor
_____	_____
Signature of Employee	Signature of Supervisor
_____	_____
Date	Date

Exhibit 4-6B, INV Form-86B, Review and Acknowledgement of Home-To-Work Transportation

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

ANNUAL CERTIFICATION
(Employee)

REVIEW AND ACKNOWLEDGEMENT OF HOME-TO-WORK TRANSPORTATION

I acknowledge that use of a government-owned vehicle, including for home-to-work transportation, is subject to the strict guidelines of 31 U.S.C. §§ 1344 and 1349, 41 C.F.R. Parts 102-5 and 102-34, Department of Homeland Security Directive 112-05, and OIG Special Agent Handbook provisions governing the use of official vehicles.

I acknowledge that the use of a government-owned vehicle for home-to-work transportation has been expressly authorized by the Secretary of Homeland Security for use in the conduct of official business only. I will strictly limit my use of Home-to-Work transportation in accordance with this authorization and the laws and policies identified above. I understand that I am not to use the vehicle for personal use of any kind, except for the limited personal use described in the OIG Special Agent Handbook, and that I am required to document all related use of the vehicle in sufficient detail in an OIG usage log.

I understand that Federal law requires a minimum one-month suspension without pay for any employee who willfully uses or authorizes the use of a government-owned vehicle for other than official purposes, or who otherwise violates 31 U.S.C. § 1344. Employees who violate this prohibition may also be suspended for a longer period or summarily removed from office (31 U.S.C. § 1349).

By my signature below, I certify that I have reviewed the OIG's policies and procedures related to the use of official vehicles for home-to-work transportation, as contained in Chapter 4 of the OIG Special Agent Handbook, and understand that I must comply with all applicable laws and policies.

_____ _____
(Employee Printed Name and Signature) (Date signed)

INV FORM 86B

Exhibit 4-6C, INV Form 86C, Vehicle Equipment Checklist

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

GOV EQUIPMENT CHECKLIST

Review Date:_____ **Office/Sub-Office:**_____

Vehicle GSA#:_____ **State Tag#:**_____ **State:**_____

Make:_____ **Model:**_____ **Yr:**_____ **Mileage:**_____

_____GSA Vehicle Accident Report Forms (SF-91a) [*required*]
_____Statement of Witness forms (SF-94) [*required*]
_____Vehicle Use Logs (INV-86) [*required*]
_____Assigned Voyager Fleet Card •
_____Current Vehicle State Registration (if applicable)
_____Current State Vehicle Inspection Sticker (if applicable)

Equipment
_____Emergency Response/First Aid Kit
_____Jumper Cables
_____Fire Extinguisher
_____Flash light
_____Warning Triangles
_____Spare Tire
_____Operating lights, signals, wipers, horn
_____Operating installed emergency equipment
_____Operating installed mobile radio equipment

Comments:

_____

_____

_____

Reviewer's Signature:_____ Date:_____

INV FORM 86-C

Exhibit 4-7, DHS MD Number 11015, (Emergency Signaling Devices in DHS Vehicles)

Department of Homeland Security
Management Directives System
MD Number: 11015
Issue Date: 09/11/2006

EMERGENCY SIGNALING DEVICES IN DHS VEHICLES

I. Purpose

This Management Directive (MD) establishes Department of Homeland Security (DHS) policy for the use of audio and visual emergency signaling devices in DHS owned or leased motor vehicles. It also sets forth the procedure for obtaining DHS Office of Security authorization for emergency signaling devices used by DHS employees other than Law Enforcement, Fire, or Emergency Medical Services (EMS) employees.

II. Scope

This MD applies to all DHS employees.

III. Authorities

Title 41, Code of Federal Regulations, Part 102-34, "Motor Vehicle Management," (2005).

IV. Definitions

A. ***Components***: All the entities that directly report to the Office of the Secretary, which includes the Secretary, Counselors and their staff, Deputy Secretary and his or her staff, and Chief of Staff and his or her staff.

B. ***Emergency Signaling Devices***: All devices used to warn other drivers of an emergency vehicle's approach, including horns, whistles, bells, lights, and sirens.

C. ***Emergency Vehicle Operations Course (EVOC)***: A course designed to enhance safe vehicle operation by stressing theory and principles of defensive driving in both emergency and non-emergency situations. The class does not teach the student to drive, but rather to explain how emergency driving differs from non-emergency driving.

D. ***Fire or Emergency Medical Service (EMS) Vehicle***: A motor vehicle primarily operated by Fire or EMS personnel and routinely used to respond to fires and medical emergencies.

E. ***Law Enforcement Vehicle***: A motor vehicle, primarily operated by law enforcement personnel of agencies of the federal government, and used for the purpose of law enforcement activities including, but not limited to, pursuit, apprehension, patrol, transport, or surveillance of people engaged or potentially engaged in unlawful activities.

F. ***Motor Vehicle***: Any vehicle, self-propelled or drawn by mechanical power, designed and operated principally for highway transportation of property or passengers.

V. Responsibilities

A. The ***Under Secretary for Management*** has Department-wide responsibility for ensuring DHS compliance with this MD.

B. The ***Director, Office of Asset Management (OAM)*** has responsibility for monitoring Component compliance with this MD.

C. The ***Chief Security Officer*** has responsibility for approving the installation of emergency signaling devices when required by this MD.

D. ***Heads of Components*** are responsible for:

1. Submitting requests for equipping non-Law Enforcement, Fire, or EMS vehicles with emergency signaling devices to the DHS Office of Security;

2. Ensuring that authorized employees are adequately trained to operate vehicles with emergency signaling devices through successful completion of an appropriate EVOC;

3. Ensuring that employees entrusted with the use of emergency signaling devices in government-owned or leased motor vehicles are aware of their responsibility for the exercise of due care for the safety of others when using those devices; and

4. Maintaining records of employees with authority to use emergency signaling devices that reflect their successful completion of EVOC training.

VI. Policy and Procedures

A. ***General***. DHS Employees shall only use emergency signaling devices when required for the safe execution of their official duties in circumstances where the need to protect the public safety or other employees requires increased visibility for vehicle operation.

B. ***Vehicles that may be equipped with emergency signaling devices***:

1. Only motor vehicles authorized in accordance with this MD shall be equipped with emergency signaling devices. Each Component shall equip only those vehicles necessary to meet its legitimate needs for emergency response capabilities. The installation of emergency signaling devices in a vehicle does not by itself constitute authority for their use.

2. Law Enforcement, Fire, and EMS vehicles are authorized to have emergency signaling devices.

3. Other vehicles may have emergency signaling devices only with approval of the DHS Office of Security. Requests for such approval will be submitted by the Component head or designee, in writing, to the DHS Office of Security and will include:

   a. The category of vehicles for which authorization is sought (for example, "FEMA emergency response vehicles").

   b. A detailed justification for why the vehicles require emergency signaling devices.

4. In areas other than under exclusive federal jurisdiction, Components should consider state and local law and regulations regarding the installation and use of emergency signaling devices. Components should seek guidance from the Office of the General Counsel as well as state and local authorities to ensure, to the extent possible, use consistent with applicable laws and regulations.

C. ***Personnel who may operate vehicles equipped with emergency signaling devices***:

1. Only authorized DHS employees, as determined pursuant to the below criteria, may operate a DHS vehicle with emergency signaling devices in use.

2. Sworn Law Enforcement Officers, Fire, and EMS personnel who have satisfied their component's EVOC training requirement are authorized to use emergency signaling devices in their vehicles. For purposes of this MD, the term "sworn law enforcement officer" includes all Coast Guard military and civilian personnel qualified to exercise the authority of 14 U.S.C. § 89 or § 95, or 46 U.S.C. § 70117.

3. EVOC instructors and student drivers are authorized to use emergency signaling devices as part of their EVOC training.

4. All other employees must have authorization from the DHS Office of Security and have completed an appropriate EVOC prior to using emergency signaling devices. Requests for such approval will be submitted by the Component head or designee, in writing, to the DHS Office of Security and will include:

a. The name and title of the employee from whom authorization is sought or the category of employee for which authorization is sought (for example, "FEMA Urban Search and Rescue vehicle drivers").

b. The anticipated situations which might require emergency response and the frequency with which these situations might occur.

c. A detailed justification for why the category of employee requires the use of emergency signaling devices.

d. A description of the EVOC training that the Component deems to be appropriate for the category of employee, and a statement acknowledging that all such employees will complete the EVOC training prior to using emergency signaling devices.

5. This MD does not authorize DHS employees to use such devices in privately owned vehicles.

6. Employees operating vehicles equipped with emergency signaling devices are responsible for their appropriate use and operation with due regard for the safety of others when such devices are in use.

7. Use of emergency signaling devices without due care or in an improper or illegal manner is considered improper use of a motor vehicle and may result in adverse personnel actions including removal as well as individual legal liability for the user.

D. ***Training***. Prior to operating emergency signaling devices, employees must successfully complete an appropriate EVOC course of instruction. The Federal Law Enforcement Training Center (FLETC) will establish standards for EVOC training with the assistance of DHS stakeholders and with concurrence from the DHS Office of Security. The standards will be provided to the respective stakeholders and the DHS Office of Security no later than six (6) months from the publication date of this MD.

E. ***Retroactive effect***. Vehicles and employees that do not meet the requirements of this MD must meet the requirements within twelve (12) months of the publication date of this MD.

VII. Questions

Address any questions or concerns regarding this MD to the DHS Office of Security.

Exhibit 4-8, DS-11 Passport Application Form

APPLICATION FOR A U.S. PASSPORT

OMB APPROVAL NO. 1405-0004
EXPIRATION DATE: 12-31-2010
ESTIMATED BURDEN: 85 MIN

Attention: see WARNING on page two of instructions

Please select the document (or documents) for which you are applying:

☐ U.S. Passport Book ☐ U.S. Passport Card

The U.S. passport card may only be used for international travel by land or sea between the United States, Canada, Mexico, the Caribbean and Bermuda. Please visit our website for detailed information.

☐ R ☐ D ☐ O ☐ DP
End. #_____ Exp _____

1. Name *Last*

First & Middle

2. Date of Birth *(mm/dd/yyyy)*

3. Sex ☐ M ☐ F

4. Place of Birth *(City & State **or** City & Country as it is presently known)*

5. Social Security Number

6. Mailing Address: *Street/RFD # **or** P.O. Box*

Apartment or unit #

City

State

Zip Code *(Zip + 4 if known)*

In Care Of or Country, if applicable

7. Contact Phone Number

☐ Home ☐ Cell ☐ Work

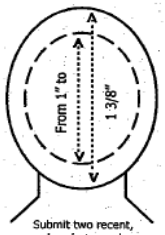
8. Email Address *(Optional)*

9. Have You Ever Used A Different Name *(Maiden, Previous Marriage, Legal Name Change)? If yes, please complete.* *(Attach additional pages if needed)*

1.

2.

STAPLE 2" X 2" STAPLE



STAPLE 2" X 2" STAPLE

Submit two recent, color photographs

10. Parents' Information

Father's Name - First & Middle

Last

Date of Birth *(mm/dd/yyyy)*

Father's Place of Birth

U.S. Citizen? ☐ Yes ☐ No

Mother's Name - First & Middle

Last (Maiden)

Date of Birth *(mm/dd/yyyy)*

Mother's Place of Birth

U.S. Citizen? ☐ Yes ☐ No

CONTINUE TO PAGE 2

DO NOT SIGN APPLICATION UNTIL REQUESTED TO DO SO BY PERSON ADMINISTERING OATH.

I declare under penalty of perjury all of the following: 1)I am a citizen or non-citizen national of the United States and have not, since acquiring U.S. citizenship or nationality, performed any of the acts listed under "Acts or Conditions" on the reverse side of this application (unless explanatory statement is attached); 2)the statements made on the application are true and correct; 3)I have not knowingly and willfully made false statements or included false documents in support of this application; 4)the photograph submitted with this application is a genuine, current, photograph of me; and 5)I have read and understood the warning on page two of the instructions to the application form.

x _____
Applicant's Signature - age 16 and older

x _____
Father's/Legal Guardian's Signature (if identifying minor)

x _____
Mother's/Legal Guardian's Signature (if identifying minor)

Identifying Documents - Applicant or Father (if identifying minor)

☐ Driver's License ☐ Passport ☐ Military ☐ Other _____

Issue Date _____ Expiration Date _____ Place of Issue _____

Name _____ ID No _____

Identifying Documents - Mother (if identifying minor)

☐ Driver's License ☐ Passport ☐ Military ☐ Other _____

Issue Date _____ Expiration Date _____ Place of Issue _____

Name _____ ID No _____

☐ Acceptance Agent ☐ (Vice) Consul USA ☐ Passport Services Staff Agent

Facility Name/Location _____

Subscribed and sworn to (affirmed) before me:

Facility/Agent ID Number

(Seal)

_____ Date _____
Signature of person authorized to accept applications

PPT Fee_____ EF_____ Postage_____ Other_____

DS 11 10 2007 1

DS-11 02-2008

Page 1 of 2

Name of Applicant *(Last, First & Middle)* | **Date of Birth** *(mm/dd/yyyy)*

11. Height | **12. Hair Color** | **13. Eye Color** | **14. Occupation** | **15. Employer**

16. Additional Contact Phone Numbers
☐ Home ☐ Cell ☐ Work ☐ _____ ☐ Home ☐ Cell ☐ Work ☐ _____

17. Permanent Address: *Street/RFD # (No P.O. Box)* | Apartment or unit #
City | State | Zip Code

18. Emergency Contact - *Provide the information of a person not traveling with you to be contacted in the event of an emergency.*
Name | Address: Street/RFD # or P.O. Box | Apartment or unit #
City | State | Zip Code | Phone Number | Relationship

19. Travel Plans
Date of Trip *(mm/dd/yyyy)* | Length of Trip | Countries to be visited

20. Have you ever been married? ☐ Yes ☐ No If yes, complete the remaining items in #20.
Current spouse's or most recent former spouse's name | Place of birth | Date of marriage *(mm/dd/yyyy)* | Widowed? ☐ Divorced? ☐ | Date *(mm/dd/yyyy)*

21. Have you ever been issued a U.S. Passport Book? ☐ Yes ☐ No If yes, complete the remaining items in #21.
Your name as listed on your most recent passport book | Most recent passport book number
Status of your most recent passport book
☐ In My Possession ☐ Stolen ☐ Lost ☐ Other _____
Approximate date your most recent passport book was issued or date you applied *(mm/dd/yyyy)*

22. Have you ever been issued a U.S. Passport Card? ☐ Yes ☐ No If yes, complete the remaining items in #22.
Your name as listed on your most recent passport card | Most recent passport card number
Status of your most recent passport card
☐ In My Possession ☐ Stolen ☐ Lost ☐ Other _____
Approximate date your most recent passport card was issued or date you applied *(mm/dd/yyyy)*

STOP! PLEASE DO NOT WRITE BELOW THIS LINE

FOR ISSUING OFFICE ONLY ☐ Sole Parent ☐ Both

Name as it appears on citizenship evidence _____

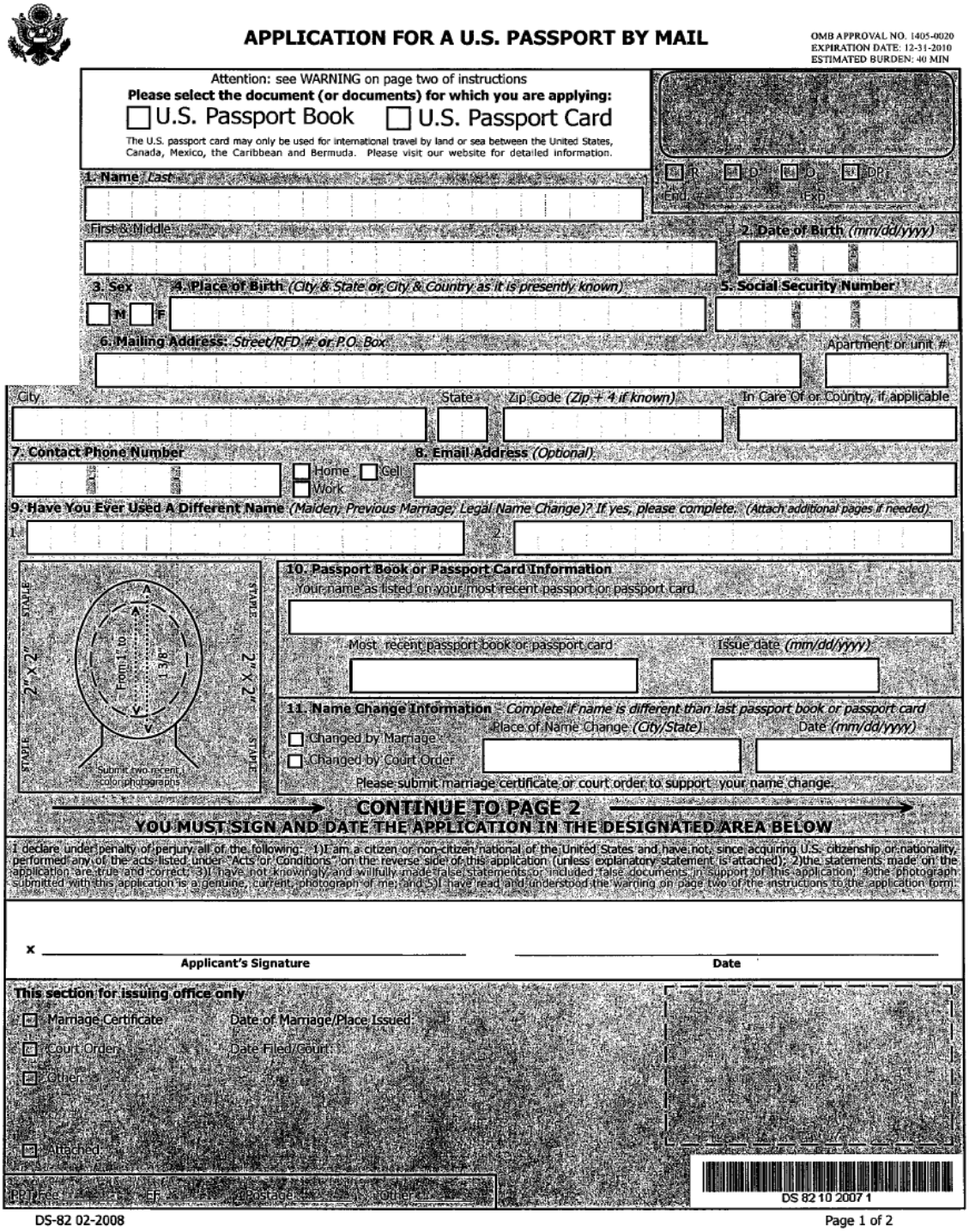
☐ Birth Certificate SR CR City Filed/Issued:
☐ Report of Birth 240 545 1350 Filed/City:
☐ Naturalization / Citizenship Certificate A# Date Acquired:
☐ Passport Issue Date:
☐ Other:
☐ Attached:

DS 11 10 2007 2

DS-11 02-2008 Page 2 of 2

Special Agent Handbook
Chapter 4

Exhibit 4-9, DS-82 Passport Renewal Form



APPLICATION FOR A U.S. PASSPORT BY MAIL

OMB APPROVAL NO. 1405-0020
EXPIRATION DATE: 12-31-2010
ESTIMATED BURDEN: 40 MIN

Attention: see WARNING on page two of instructions

Please select the document (or documents) for which you are applying:

☐ U.S. Passport Book ☐ U.S. Passport Card

The U.S. passport card may only be used for international travel by land or sea between the United States, Canada, Mexico, the Caribbean and Bermuda. Please visit our website for detailed information.

☐ R ☐ D ☐ O ☐ DRT
End. # Exp

1. Name *Last*

First & Middle

2. Date of Birth *(mm/dd/yyyy)*

3. Sex ☐ M ☐ F

4. Place of Birth *(City & State or City & Country as it is presently known)*

5. Social Security Number

6. Mailing Address: *Street/RFD # or P.O. Box*

Apartment or unit #

City

State

Zip Code *(Zip + 4 if known)*

In Care Of or Country, if applicable

7. Contact Phone Number

☐ Home ☐ Work ☐ Cell

8. Email Address *(Optional)*

9. Have You Ever Used A Different Name *(Maiden, Previous Marriage, Legal Name Change)? If yes, please complete. (Attach additional pages if needed)*

1.

2.

2" X 2" SQUARE

From 1" to 1 3/8"

Submit two recent, color photographs

10. Passport Book or Passport Card Information

Your name as listed on your most recent passport or passport card

Most recent passport book or passport card

Issue date *(mm/dd/yyyy)*

11. Name Change Information - *Complete if name is different than last passport book or passport card*

☐ Changed by Marriage ☐ Changed by Court Order

Place of Name Change *(City/State)*

Date *(mm/dd/yyyy)*

Please submit marriage certificate or court order to support your name change.

CONTINUE TO PAGE 2

YOU MUST SIGN AND DATE THE APPLICATION IN THE DESIGNATED AREA BELOW

I declare under penalty of perjury all of the following: 1) I am a citizen or non-citizen national of the United States and have not, since acquiring U.S. citizenship or nationality, performed any of the acts listed under "Acts or Conditions" on the reverse side of this application (unless explanatory statement is attached); 2) the statements made on the application are true and correct; 3) I have not knowingly and willfully made false statements or included false documents in support of this application; 4) the photograph submitted with this application is a genuine, current, photograph of me; and 5) I have read and understood the warning on page two of the instructions to the application form.

x _____ _____

Applicant's Signature Date

This section for issuing office only

☐ Marriage Certificate Date of Marriage/Place Issued

☐ Court Order Date Filed/Court

☐ Other

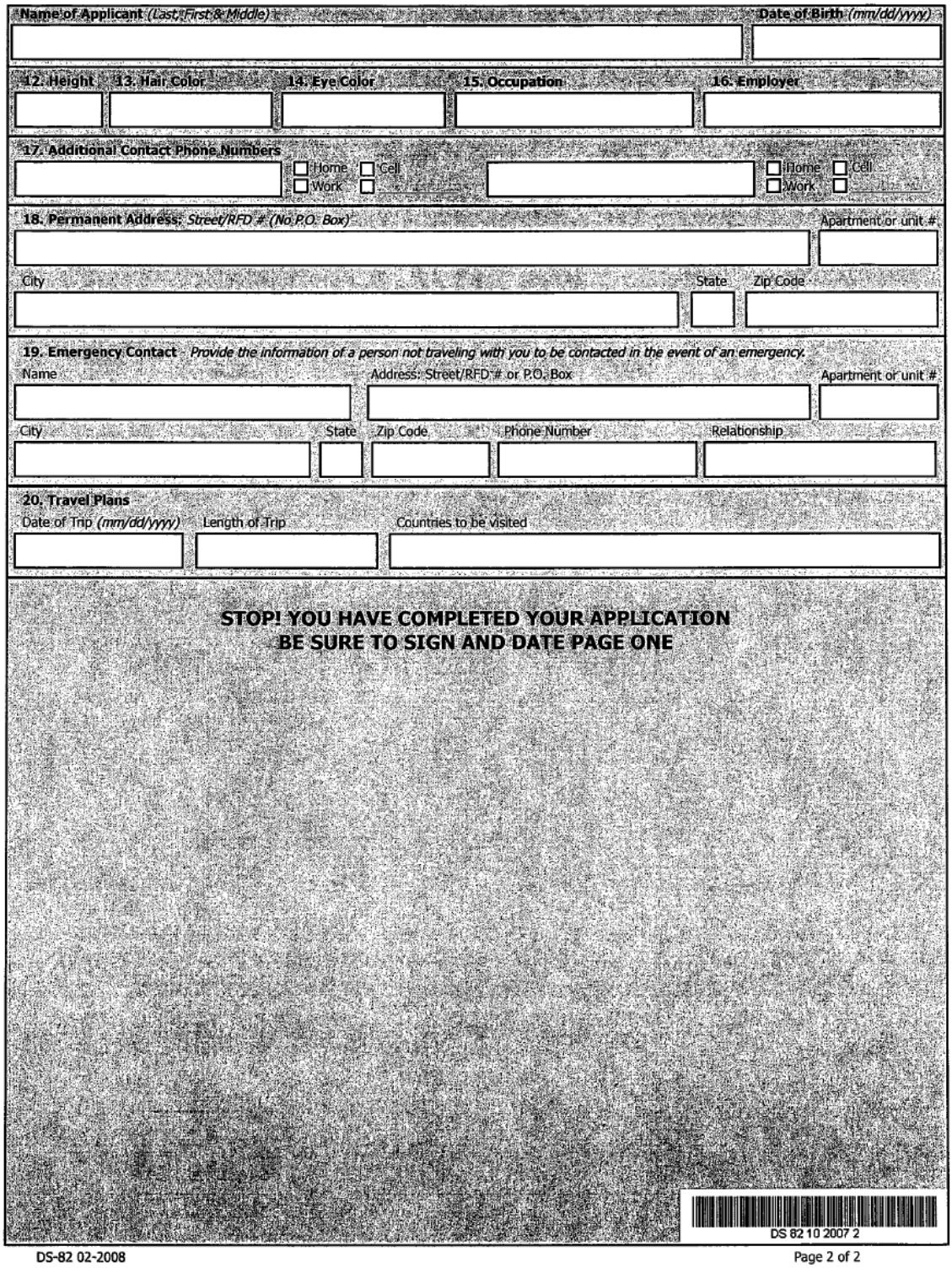
☐ Attached

PF Fee EF Postage Other

DS 82 10 2007 1

DS-82 02-2008

Page 1 of 2



Name of Applicant *(Last, First & Middle)* | **Date of Birth** *(mm/dd/yyyy)*

12. Height | **13. Hair Color** | **14. Eye Color** | **15. Occupation** | **16. Employer**

17. Additional Contact Phone Numbers
☐ Home ☐ Cell ☐ Work ☐ | ☐ Home ☐ Cell ☐ Work ☐

18. Permanent Address: *Street/RFD # (No P.O. Box)* | Apartment or unit #
City | State | Zip Code

19. Emergency Contact *Provide the information of a person not traveling with you to be contacted in the event of an emergency.*
Name | Address: Street/RFD # or P.O. Box | Apartment or unit #
City | State | Zip Code | Phone Number | Relationship

20. Travel Plans
Date of Trip *(mm/dd/yyyy)* | Length of Trip | Countries to be visited

STOP! YOU HAVE COMPLETED YOUR APPLICATION
BE SURE TO SIGN AND DATE PAGE ONE

DS 82 10 2007 2

DS-82 02-2008 Page 2 of 2

Exhibit 4-10, DS-4085, Application for Additional VISA Pages or Miscellaneous Passport Services

APPLICATION FOR ADDITIONAL VISA PAGES OR MISCELLANEOUS PASSPORT SERVICES

OMB APPROVAL NO. 1405-0159
EXPIRATION DATE: 12-31-2010
ESTIMATED BURDEN: 20 MIN

WARNING: False statements made knowingly and willfully in passport applications, including affidavits or other documents submitted to support this application, are punishable by fine and/or imprisonment under the provisions of 18 USC 1001, 18 USC 1542, and/or 18 USC 1621. Alteration or mutilation of a passport issued pursuant to this application is punishable by fine and/or imprisonment under the provisions of 18 USC 1543. The use of a passport in violation of the restrictions contained therein or of the passport regulations is punishable by fine and/or imprisonment under 18 USC 1544. All statements and documents are subject to verification.

1. Name *Last*

First & Middle

2. Date of Birth *(mm/dd/yyyy)*

3. Sex ☐ M ☐ F

4. Place of Birth *(City & State or City & Country as it is presently known)*

5. Social Security Number

6. Mailing Address: *Street/RFD # or P.O. Box*

Apartment or unit #

City

State

Zip Code *(Zip + 4 if known)*

In Care Of or Country, if applicable

7. Contact Phone Number

☐ Home ☐ Cell ☐ Work

8. Email Address *(Optional)*

9. Current Passport Number

Issue date *(mm/dd/yyyy)*

10. Permanent Address: *Street/RFD # (No P.O. Box)*

Apartment or unit #

City

State

Zip Code

11. Additional Contact Phone Number

☐ Home ☐ Cell ☐ Work ☐ _____

12. Occupation

13. Employer

14. Emergency Contact - *Provide the information of a person not traveling with you to be contacted in the event of an emergency.*

Name

Address: Street/RFD # or P.O. Box

Apartment or unit #

City

State

Zip Code

Phone Number

Relationship

15. Travel Plans

Date of Trip *(mm/dd/yyyy)*

Length of Trip

Countries to be visited

YOU MUST SIGN AND DATE THE APPLICATION IN THE DESIGNATED AREA BELOW

I declare under penalty of perjury all of the following: 1)I am a citizen or non-citizen national of the United States and have not, since acquiring U.S. citizenship or nationality, performed any of the acts listed under "Acts or Conditions" on the reverse side of this application (unless explanatory statement is attached); 2)the statements made on the application are true and correct; 3)I have not knowingly and willfully made false statements or included false documents in support of this application.

x _____
Applicant's Signature - age 16 and older

x _____
Parent's/Legal Guardian's Signature *(if identifying minor)*

_____
Date

EF_____ Postage_____ Other_____

This section for issuing office only

DS 4085 10 2007 1

DS-4085 02-2008

Page 1 of 1

Exhibit 4-11, Notification of Foreign Travel

DEPARTMENT OF HOMELAND SECURITY

NOTIFICATION OF FOREIGN TRAVEL

INSTRUCTIONS

Travel outside of the U.S. is a matter of security interest. Knowledge of your whereabouts can be of value in the event of an emergency. This form is designed for use by SCI-indoctrinated personnel to report official and unofficial travel to security, per DCID 1/20 requirements. Please complete the items below and return to your security officer 30 days prior to your departure. Your security officer will provide travel briefings if required. Upon return, report to your security officer any incident which implies a security threat.

1. THIS TRAVEL IS ☐ OFFICIAL ☐ PERSONAL

2. PURPOSE OF TRAVEL

3. NAME AND TITLE OF TRAVELER (LAST, FIRST, MI)	SSN	PASSPORT NUMBER AND EXPIRATION DATE

4. DHS ORGANIZATION	NON-DHS AGENCY OR COMPANY (if applicable)

WORK PHONE	E-MAIL ADDRESS

5. EMERGENCY POC NAME	PHONE NUMBER

6. SUPERVISOR'S NAME	WORK PHONE NUMBER

7. DESTINATION ITINERARY: If more than one foreign country is to be visited, list countries in schedule order of visit, together with all major cities, side trips and stopovers. First and last line should indicate United States departure and return. Attach itinerary if available.

Date (DD/MM/YY)	From (City, Country)	To (City, Country)	Flights/Cruise (Carrier and number)	Hotels (Name and phone)

DHS Form 11043-1 (4/05)

Pages 1 of 2

8. ANTICIPATED CONTACTS WITH FOREIGN GOVERNMENTS, COMPANIES, CITIZENS

Name	Organization	Citizenship	Nature of Contact (personal/professional)

Signature of Traveler _____ Date _____

Security Use Only:

			Security Officer	Date of Briefing
Defensive Security Briefing Required	☐ YES	☐ NO		
Country Specific Briefing Required	☐ YES	☐ NO		

Comments: _____

The Privacy Act, 5 U.S.C. 522a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. The collection of this information is authorized by EO 9397, 6 USC 341, 44 USC 3101, and DCID 1/20. Provision of the information concerning foreign travel is mandatory under the provisions of DCID 1/20. Failure to provide it may affect your travel plans and security clearance status. Provision of your social security number is voluntary; your SSN will be used to assist in identifying you as the reporting individual. Use of this information is for internal purposes only to monitor foreign travel by DHS personnel and ensure that security requirements are met.

DHS Form 11043-1 (4/05) Pages 2 of 2

Exhibit 4-12 Country Clearance Memorandum

Office of Inspector General
Office of Investigations
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

DATE

TO :
Regional Security Officer
United States Embassy
(City/Country)

THROUGH :
Assistant Inspector General for Investigations

FROM :
Special Agent in Charge
Office of Investigations
Field Office

SUBJECT : Request for Country Clearance

In accordance with the procedures and directive on requesting foreign travel by Office of Investigations personnel, the following is forwarded for approval.

1. TRAVELER(S) NAME(S)/TITLE(S):

2. SSN:

3. DOB:

4. OFFICIAL PASSPORT NUMBE/R(S):

5. DATE OF EXPIRATION OF OFFICIAL U.S. PASSPORT(S):

6. SECURITY CLEARANCE OF TRAVELER(S): Top Secret

7. BRIEF STATEMENT AS TO THE NECESSITY OF THE TRAVEL:

8. U.S. LAWS VIOLATED:

9. STAGE OF INVESTIGATION:

10. PERSONS OR FIRMS TO BE INTERVIEWED OR VISITED:

11. COUNTRIES TO BE VISITED:

12. DATES OF PROPOSED VISIT:

13. PROPOSED ITINERARY:

14. ESTIMATED TRAVEL COSTS:

15. AUSA AND DISTRICT HANDLING CASE:

16. NAMES AND AFFILIATION OF ANY FOREIGN NATIONALS OR LAW ENFORCEMENT COUNTERPARTS CONTACTED IN THIS MATTER:

17. LOCATION OF INTERVIEW OR INVESTIGATION:

18. DOMESTIC LAW ENFORCEMENT AGENCIES ASSISTING OR PARTICIPATING IN THE INVESTIGATION:

19. IF APPROPRIATE, DEA CABLE IS ATTACHED:

20. THE MATTER HAS BEEN DISCUSSED WITH:

Approved:

_____ Date: _____
Assistant Inspector General for Investigations

Exhibit 4-17, SOP Proposal Form

OFFICE OF INSPECTOR GENERAL *OFFICE OF INVESTIGATIONS*	SOP #_____ Date Issued: _____ Date Revised: _____ ☐ Interim
Type the Title of your document here	
Originating Office: Field Operations Division Contacts:	Approved by: John Dupuy Acting Assistant Inspector General for Investigations
Purpose: This procedure…	
Applicable Offices: indicate name of offices or say All Offices if this has OIG-wide applicability.	
Background: (if necessary):	
Procedures/Responsibilities:	

OFFICE OF INSPECTOR GENERAL OFFICE OF INVESTIGATIONS	SOP #_____ Date Issued: _____ Date Revised: _____ ☐ Interim

Type the Title of your document here

Procedures/Responsibilities (Continued):

2

OFFICE OF INSPECTOR GENERAL OFFICE OF INVESTIGATIONS	SOP #_____ Date Issued: _____ Date Revised: _____ ☐ Interim

Type the Title of your document here

Procedures/Responsibilities (Continued):

3

OFFICE OF INSPECTOR GENERAL OFFICE OF INVESTIGATIONS	SOP #_____ Date Issued: _____ Date Revised: _____ ☐ Interim

Type the Title of your document here

Definitions:

4

OFFICE OF INSPECTOR GENERAL OFFICE OF INVESTIGATIONS	SOP #_____ Date Issued: _____ Date Revised: _____ ☐ Interim

Type the Title of your document here

REVIEW:

GROUP	REVIEWING OFFICIAL	DATE REVIEWED	COMMENTS
Sponsor			
FOD EAST			
FOD WEST			
HOD			
Counsel			
DAIGI			
AIGI			

Attachments (list the titles of any attachments—if applicable—and then add/insert the attachments to the following pages of this template).

5

OFFICE OF INSPECTOR GENERAL OFFICE OF INVESTIGATIONS	SOP #_____ Date Issued: _____ Date Revised: _____ ☐ Interim

Type the Title of your document here

Attachment
Title

6

5.0 FIREARMS, USE-OF-FORCE POLICY, AND DEFENSIVE TACTICS

5.1 AUTHORITY TO CARRY FIREARMS

INV SAs have the statutory authority to make arrests, carry firearms, and execute warrants as authorized by the Attorney General pursuant to the Inspector Act of 1978, as amended in 2002 and Homeland Security Act (PL 107-296). Pursuant to this policy INV SAs are considered law enforcement officers 24-hours a day.

In accordance with the Attorney General's Guidelines (Chapter 2.5), the IG has authorized OIG SAs to carry their officially issued firearm while off-duty. **(Exhibit 5-1)** This decision does not expand a SA's law enforcement authority. Nor does it change the factors that will determine whether a SA will be provided with DOJ legal representation or be subject to personal liability for an incident involving the use of a firearm. **(Exhibit 5-2)** In addition, all laws, regulations and DHS OIG policies governing the use and handling of a firearm while in an official on-duty status shall apply to a SA carrying a firearm while off-duty.

The Lautenberg Amendment, 18 USC 922 (g) (9), prohibits individuals, including federal law enforcement personnel, who have been convicted of misdemeanor crimes or domestic violence from possessing firearms. Any SA who is charged with a crime of domestic violence must immediately notify their SAC. SACs are required to provide notification to the AIGI of the circumstances surrounding the charges.

5.2 GENERAL CONDUCT

SAs are responsible for the safe handling, storage, and use of DHS-OIG issued firearms, non-lethal weapons, and other law enforcement equipment. In addition, SAs are responsible for the safe handling, storage, and disposition of any firearm or other weapon seized or otherwise acquired while engaged in the performance of their official duties.

SAs are prohibited from carrying a firearm while under the influence of alcohol or narcotics.

5.3 APPROVED WEAPONS AND LAW ENFORCEMENT EQUIPMENT

[redacted]

5.4 PERMITS TO CARRY FIREARMS

Nothing in this Handbook shall be construed as interfering with the right of SAs as private citizens to carry a privately owned firearm for personal use. SAs are expected to comply with all applicable Federal, state, and local laws.

SAs will not use their position or credentials to qualify under state or local laws to purchase, license, carry, or use personally owned firearms. Credentials may be shown for identification purposes only.

State, county, and/or local police department permits to carry firearms will not be recognized by the DHS OIG in any way, as authorization to carry personally owned weapons while performing official duties.

5.5 LOSS OR THEFT OF ISSUED FIREARM

SAs shall immediately report the loss or theft of an issued firearm or other weapon to their SAC. SACs must immediately inform the appropriate DAIGI when a firearm or other weapon is missing, stolen, or otherwise unaccounted. The SA will document the loss or theft within 24 hours by submission of a memorandum to the AIGI, through the SAC. The SAC will insure the information is entered into the NCIC.

An inquiry may be conducted under the direction of the AIGI to determine the circumstances of the theft/loss of the firearm or other weapon.

5.6 [redacted]

[redacted]

5.7 USE OF FORCE POLICY

The use of deadly force shall be in accordance with Department of Justice Policy Statement, Use of Deadly Force, dated July 1, 2004 **(Exhibit 5-4).**

5.8 GENERAL USE OF FORCE GUIDELINES

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted].

5.9 REVOCATION OF AUTHORITY TO CARRY A FIREARM

SACs should assess an SA's suitability to carry a firearm. The SAC shall revoke an SA's authority to carry a firearm when it is the SAC's determination that the SA's judgment or ability to handle a firearm is impaired. If the SAC revokes a SA's authority to carry a firearm, the SAC shall notify and document his/her decision to the DAIGI as soon as practical.

Additionally, failure to qualify on the DHS OIG qualification course, involvement in a shooting, or suspension of the SA may result in revocation of the authority to carry a firearm. The SA will be required to surrender their weapon when the authority to carry a firearm is revoked or when directed to do so by the SAC or other competent authority. The SA will be required to re-qualify with their firearm prior to reinstatement should the period of revocation exceed two quarters, or at any time at the discretion of the SAC.

All documentation concerning the revocation and/or reinstatement of authority to carry a firearm should be maintained in the SA's firearms training record for one year.

5.10 TEMPORARY EXEMPTION FROM FIREARMS QUALIFICATION

SACs may temporarily exempt SAs from routine firearm qualification. Reasons for exemption may include extended details outside the DHS OIG and temporary medical conditions. The SA is required to provide medical documentation to their SAC.

SAs who are pregnant are encouraged to discuss possible firearms range hazards, such as lead exposure and gunshot noise, with her physician. The decision whether or not to continue firearm qualification during pregnancy rests with the SA. Regardless of her decision, the SA must provide documentation from her physician supporting her decision to the SAC.

Pregnant SAs who choose to continue qualification must qualify with (but not carry) nonstandard lead-free ammunition. The lead-free ammunition will be provided to the SA.

5.11 AUTHORIZED AMMUNITION

All ammunition must be approved by INV Headquarters as defined in the Training Guidelines Handbook.

Service ammunition (including lead-free ammunition as appropriate) will be used for qualifications. SAs are authorized the issuance of DHS OIG ammunition for off-duty practice.

5.12 FIREARMS INVENTORY, CONTROL AND STORAGE

Inventory

The National Firearms Program Manager maintains a complete inventory of DHS OIG issued firearms.

Each office will also maintain a record of its firearms inventory in EDS. When an SA is transferred to another Field Office or other assignment within the DHS OIG, their issued firearm will be transferred with them.

The National Firearms Program Manager will oversee an annual inventory of all firearms.

[redacted]

Each DHS OIG office must have a suitable firearms handling area equipped with a commercial bullet trap. If it is necessary to load or unload a firearm in the office it must be done in this area using the trap. At all times firearms must be loaded and unloaded in a safe and secure manner.

5.13 AMMUNITION INVENTORY CONTROL AND STORAGE

Inventory

INV Offices will maintain an inventory of DHS OIG ammunition.

Each office will also maintain an inventory of ammunition using the "Ammunition Inventory Log" INV Form-92. **(Exhibit 5-5)** This inventory will also account for the destruction of any outdated ammunition.

Offices will conduct an annual inventory of all DHS OIG ammunition and submit the inventory to the National Firearms Program Manager by the end of each fiscal year. This information will include the amount of ammunition used, the amount of ammunition destroyed, if any, and the amount of ammunition on hand.

Control and Storage

Ammunition will be stored in a secured storage room or in a GSA approved security container and in accordance with State and local ordinances.

Destruction of Outdated Ammunition

THE NATIONAL FIREARMS PROGRAM MANAGER WILL IDENTIFY PROPER DISPOSITION PROCEDURES FOR OUTDATED AMMUNITION.

5.14 SHIPPING FIREARMS AND AMMUNITION

[redacted]

5.15 REPORTING SHOOTING INCIDENTS

SAs must report any shooting incident as soon as practicable to the SAC or designee. The AIGI must be immediately notified of the incident. The AIGI will then notify the IG and Counsel.

The initial notification will be followed within 24 hours by a written report to the AIGI. SAs will retain all of their constitutional rights, including the right to obtain legal counsel and protection from self-incrimination.

If the shooting incident results in personal injury, the initial priority is ensuring appropriate medical attention is obtained. In addition, local law enforcement authorities should be notified.

[CRITICAL INCIDENT POLICY PLACEHOLDER]

This report should include the following facts where applicable:

The time, date, and location where the incident occurred.

The names, contact information, and affiliation of all persons involved in the incident.

The names, contact information, and affiliation of any news media representative(s) present.

The name(s) of any person(s) injured; a description of the injuries; and the name, location, and telephone number of all medical facilities used to treat the injured.

A description and estimate (if possible) of any property damage.

A synopsis of the incident, including the case number of the investigation the SA was working at the time of the shooting incident.

The name(s) of any person(s) arrested and a description of the offenses charged.

The name of the lead investigative agency, including the title and telephone number of the lead investigator(s).

The make and type of any and all weapons used and total number of rounds expended.

A detailed summary of all statements made to any news media representative since the event occurred.

If possible, a detailed summary of statements (including copies, if in writing) made to other law enforcement agencies by witnesses to, or participants in, the incident.

A complete explanation of the involvement (if any) of the United States Attorney's Office/other prosecuting authority, IG Counsel, or any DHS component.

The identity of the DHS OIG supervisor responsible for the initial report of the incident.

5.16 ACCIDENTAL DISCHARGE OF FIREARM

SAs must immediately report any accidental discharge to the SAC or designee. The SAC will notify the AIGI if the accidental discharge results in personal injury or property damage. The initial notification will be followed within 24 hours by a written report to the AIGI. SAs will retain all of their constitutional rights, including the right to obtain legal counsel and protection from self-incrimination. The report should follow the same format as outlined in Section 5.15.

5.17 DEFENSIVE TACTICS AND USING THE [redacted]

[redacted]

[redacted]

5.18 REPORTING INCIDENTS INVOLVING USE OF THE [redacted]

SAs must report any incident involving the use of the [redacted] as an impact weapon, as soon as practicable to the SAC or designee. If the use of the [redacted] results in personal injury or property damage, the AIGI must be immediately notified of the incident. The initial notification will be followed within 24 hours by a written report to the AIGI. SAs will retain all of their constitutional rights, including the right to obtain legal counsel and protection from self-incrimination. The report should follow the same format as outlined in Section 5.15.

5.19 POST-INCIDENT PROCEDURES

SAs involved in a shooting incident are obligated to cooperate with the investigating agency having proper jurisdiction. However, SAs still retain all of their constitutional rights, including the right to obtain legal counsel and protection against self-incrimination. SAs must notify their SAC of the incident as soon as practicable.

Statements will not be solicited by the DHS OIG from any SA involved in, or present during a shooting, until such time as the SA has regained their composure and if the SA asks or a supervisor directs, has been given an opportunity to consult with an attorney or physician.

SAs are reminded that they have the responsibility to render assistance and protection to any person(s) involved in a use-of-force incident.

If an SA has been injured, a designated INV employee will transport members of their immediate family to the appropriate medical facility and remain with them until released by the SAC, DAIGI, or AIGI. DHS OIG personnel should be informed about the ongoing situation but cautioned against discussing it outside INV except for required cooperation with the appropriate law enforcement authorities. No information concerning a shooting or other injury shall be released to anyone, except to appropriate law enforcement authorities outside OIG without the expressed approval of the IG.

DHS OIG policy is not to disclose to the media or otherwise make public the identity of SAs involved in shootings or other less-than-lethal force incidents. All media inquiries must be directed to the CMA. (Chapter 4.14)

Post-trauma-stress counseling and/or intervention, including but not limited to that provided by the Employee Assistance Program (EAP), shall be made available to all SAs involved in shooting incidents. (Chapter 4.17 and 4.18)

Depending on the circumstances of the shooting, participation in such counseling may be mandatory or discretionary. Participation in a post-trauma-stress treatment program will be mandatory if the use-of-force incident resulted in a fatality or serious physical injury to anyone or if the SA requests such assistance. Participation will be discretionary if the use-of-force incident did not result in a fatality or serious physical injury.

If counseling, including that provided by/through EAP, is mandatory, the SA should initiate appropriate contact within 72 hours of the shooting incident unless medically unable to do so. If this is the case, the SAC will initiate the appropriate action.

No SA present during, or involved in, the use-of-force incident should be actively involved in the follow-up investigation.

The SAC may grant administrative leave for SAs involved in any use-of-force incident that result in injury or death.

5.20 POST INCIDENT ADMINISTRATIVE INQUIRY

The INV will conduct an administrative inquiry into any shooting incident, or any other use-of-force resulting in injury or death, regardless of the circumstances. The report of this inquiry is separate and distinct from any report submitted at the time of the incident, or any official investigation conducted by other law enforcement authorities. The SAC of SID, in consultation with the AIGI, will determine the composition of the inquiry team. The leader of the inquiry team will prepare a written report for the AIGI.

CHAPTER 5.0 - EXHIBITS

Exhibit 5-1, Authority to Carry OIG-Issued Firearms Off-Duty

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

August 19, 2004

MEMORANDUM FOR: All Special Agents

FROM: Clark Kent Ervin
Inspector General

SUBJECT: Authority to Carry OIG Firearms Off-Duty

As part of the Homeland Security Act (P.L. 107-296, § 812), Congress provided that Special Agents employed in designated Offices of Inspector General (OIG), including the Department of Homeland Security (DHS) OIG, shall have statutory law enforcement authority. This law directed the Attorney General to promulgate guidelines to implement that authority. On December 8, 2003, the Attorney General issued "Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority." Those guidelines permit Inspectors General to authorize their Special Agents to carry their OIG firearms while off-duty.

After consultation with the Assistant Inspector General for Investigations (AIGI) and the Counsel to the Inspector General, I hereby authorize DHS OIG Special Agents to carry their officially issued OIG firearms while off-duty to meet the operational needs of the OIG and to ensure the safety of OIG Special Agents.

This decision does not expand OIG Special Agents' law enforcement authority nor does it change the factors that will determine whether OIG Special Agents will be provided legal representation by the Department of Justice or be subject to personal liability for an incident involving the use of a firearm. These legal principles are discussed in the attached memorandum from the Counsel to the Inspector General.

While carrying firearms off-duty, OIG agents are subject to the same guidelines and regulations that govern the use and handling of such weapons while on-duty.

Specifically:

- Special Agents are personally responsible for the security of their OIG-issued firearm;
- Special Agents must carry OIG official credentials at all times when firearms are carried;
- Special Agents may not consume or be under the influence of alcoholic beverages when carrying a firearm on or off-duty;
- [redacted]
- Discretion should be exercised when putting on, carrying, and removing firearms to ensure that there is no unnecessary display to the public;
- Unnecessary reference to the fact that Special Agents are carrying a firearm should be avoided;
- [redacted];
- [redacted];
- [redacted];
- Special Agents shall comply with all Department of Justice policies regarding the use of firearms, including the Department of Justice Deadly Force Policy.

If you have any operational questions about these guidelines you should contact the AIGI. Questions on legal authority should be directed to the Counsel to the Inspector General. This memorandum and accompanying attachment will be included in Chapter 5 of the Special Agent Handbook.

Exhibit 5-2, OIG SA Law Enforcement Authority and DOJ Legal Representation Issues

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528

MEMORANDUM FOR: All OIG Special Agents

FROM: Richard N. Reback
General Counsel

SUBJECT: OIG Special Agent Law Enforcement Authority
And Department of Justice Legal
Representation Issues

As part of the Homeland Security Act (P.L. 107-296), Congress provided that Special Agents employed in designated Offices of Inspector General (OIG), including the Department of Homeland Security (DHS) OIG, shall have statutory law enforcement authority. This law also directed the Attorney General to promulgate guidelines to implement that authority. On December 8, 2003, the Attorney General issued "Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority" (Attorney General Guidelines). The Attorney General Guidelines permit Inspectors General to authorize their Special Agents to carry their OIG firearm while off-duty. Pursuant to the Attorney General Guidelines, the DHS OIG Inspector General has authorized DHS OIG Special Agents to carry their official OIG firearm while off-duty.

Although the Inspector General has authorized Special Agents to carry their OIG firearm while off-duty, this decision does not expand Special Agents' law enforcement authority. Nor does it change, in any way, under what circumstances DHS OIG Special Agents may use their official firearm. DHS OIG Special Agents are to continue to use their enforcement authority and their official firearm as they have done in the past, pursuant to DHS OIG training, guidelines, and policy directives as well as the Department of Justice Deadly Force Policy.

This new grant of authority also does not change the factors that will be used to determine

whether Special Agents will be provided legal representation if they are the subject of allegations that arise from the use of a firearm. Special Agents will continue to be required to demonstrate that their actions were carried out in the scope of their employment and their representation is in the interest of the United States.

Following is a brief summary of Special Agents' scope of authority, the types of suits that may be filed in connection with the use of a firearm, and the factors considered in determining whether DOJ will provide legal representation.

I. OIG SPECIAL AGENT LAW ENFORCEMENT AUTHORITY

A. Special Agent Authority Under the Inspector General Act

The Homeland Security Act amended the Inspector General Act to codify OIG law enforcement authority. Prior to the enactment of the Homeland Security Act provisions, the authority of OIG Special Agents at other agencies to carry firearms, make arrests, and execute search warrants was derived from Attorney General orders directing the United States Marshals Service to deputize OIG Special Agents. Under the Inspector General Act, as amended, and the Attorney General Guidelines, DHS OIG Special Agents are now authorized by statute to:

Investigate allegations of criminal wrongdoing or administrative misconduct by employees of the Department of Homeland Security;

Conduct investigations relating to the administration of the programs and operations of the Department of Homeland Security;

Administer to, or take from, any person an oath, affirmation, or affidavit, whenever necessary in the performance of their official duties;

Seek and execute search and arrest warrants;

Arrest without warrant, while engaged in official duties, any person for an offense against the United States committed in the presence of the Special Agent or whom the Special Agent has reasonable grounds to believe has committed or is committing a felony cognizable under the laws of the United States; and

Carry a firearm while on-duty, or off-duty as authorized by the Inspector General.

B. Special Agent Authority Under State Statutes

Office of Inspector General Special Agents cannot enforce state law unless expressly authorized by state statute to do so. A number of states provide some authority for federal law enforcement officers to enforce state law. However, most of those states limit such authority to making arrests for felonies committed in the officer's presence, rendering assistance to local police in an emergency, or providing assistance at the

request of a local police officer or department. If a question arises concerning whether a particular state authorizes federal agents to enforce its laws, contact either the Office of Counsel to the IG or the local USAO for guidance.

As a practical matter, the enforcement of state law by federal law enforcement officers subjects the federal officer to potential liability to which he or she might not otherwise be exposed. For example, federal officers who undertake the enforcement of state law expose themselves to liability for state civil law torts and federal civil rights violations.[1] Although some states provide federal law enforcement officers some immunity from state tort liability when acting pursuant to grants of state law authority, many do not.

The risks of liability for federal law enforcement officers acting under a state law grant of authority are significantly reduced when the officers also are acting within the scope of their federal employment.[2] In those instances, federal law enforcement officers should be entitled to protection under the Federal Tort Claims Act (FTCA).

In summary, as long as federal employees act within the scope of their employment when using their firearm, they will have broad immunity from suit on state law civil damages claims. On the other hand, federal employees who act outside of the scope of their federal employment pursuant to a grant of state law authority expose themselves to liability risks for which their protection is more limited. Therefore, even though some states may expressly authorize federal law enforcement officers to do so, DHS OIG Special Agents should refrain from undertaking state law enforcement efforts or investigating local crimes that have no connection to a DHS OIG matter.

II. SPECIAL AGENT LIABILITY AND REPRESENTATION BY THE DEPARTMENT OF JUSTICE

Federal law enforcement officer liability can arise from violations of state civil tort law, the constitution, and federal statutes that implement constitutional rights. Whether a federal law enforcement officer can be held to be personally liable depends upon the type of violation at issue and whether the officer was acting within the scope of his or her employment.

A. Federal Tort Claims Act

Under the FTCA, 28 U.S.C. §§ 1346(b) and 2672, the United States has waived its sovereign immunity and has agreed to be sued with regard to claims of negligence or wrongful conduct on the part of its employees acting within the scope of their employment. The FTCA is the exclusive remedy for all job-related damage claims against federal employees, except for claims arising under the federal constitution and federal statutes

[1] According to 42 U.S.C. § 1983, the violation of state laws that subjects, or causes to be subjected, any citizen of the United States to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, may expose the officer to be liable to the party injured.

[2] See the discussion of "scope of employment" below.

which themselves authorize suits for damages. If the allegedly negligent employee acted within the scope of his or her employment at the time of the incident out of which the claim arose, the employee should be dismissed as a defendant and "any civil action or proceeding commenced upon such claim shall be deemed [to be] against the United States . . . and the United States shall be substituted as the party defendant." 28 U.S.C. § 2679(d)(1).

Prior to the United States entering a case and being substituted as the defendant, however, the Attorney General must certify that the employee acted within the scope of his or her employment at the time of the incident out of which the claim arose. For purposes of substitution of the United States for the named individual employee, scope of employment is determined under principles of employer liability under the law of the applicable state. Generally, scope of employment under such state law principles is determined by considering: (1) whether the conduct was of a kind the employee is employed to perform; (2) the conduct occurred substantially within the authorized time and space limits of the employment; and (3) the conduct was actuated, at least in part, by a purpose to serve the employer's business.[3]

In 1998, the FTCA was amended to add what is known as "The Good Samaritan Act." 28 U.S.C. § 2671. Pursuant to this amendment, a federal law enforcement officer will be deemed to be acting within the scope of his or her employment for purposes of the FTCA if the officer takes reasonable action, including the use of force, to:

protect an individual in the presence of the officer from a crime of violence;

provide immediate assistance to an individual who has suffered bodily harm or who is threatened with bodily harm; or

prevent the escape of any individual who the officer reasonably believes to have committed in the presence of the officer a crime of violence.

A crime of violence is defined as an offense that has as an element the use, attempted use, or threatened use of physical force against the person or property of another or any offense that is a felony and that by its nature involves a substantial risk that physical force against the person or property of another may be used in the course of committing the offense. 18 U.S.C. § 16.

A review of the legislative history indicates that the Good Samaritan Act was not intended to grant federal law enforcement officers additional authority. Instead, the provision was enacted to provide protection from personal liability for federal law enforcement officers who find themselves in a situation where they must use force to protect their life or safety, or the life or safety of another.

Special Agents should be aware that "in the presence of the officer" is strictly construed,

[3] See Department of Justice, Civil Division, Torts Branch Monograph, "Absolute Immunity for Common Law Torts: The Westfall Act," page 8.

and that Special Agents are not likely to be found to be acting within the scope of their employment if they proceed to the scene of an ongoing crime and intervene with force. In other words, the statute does not authorize federal law enforcement officers to intentionally put themselves in "Good Samaritan" type situations. Accordingly, if it is possible to avoid intervening by calling the local police, DHS OIG Special Agents should do so.

B. Constitutional Violations

When federal employees are sued in their personal capacity for allegations of wrongdoing involving a violation of an individual's constitutional rights, the United States cannot be substituted as the defendant. Therefore, federal employees may be liable in their individual capacities in these types of cases. Because the leading case in this area is Bivens v. Six Unknown Named Agents, 403 U.S. 388 (1971), claims for constitutional violations brought against federal employees in their individual capacity are commonly referred to as Bivens claims. A Special Agent may seek reimbursement for a monetary judgment arising out of a Bivens claim. Reimbursement may be deemed appropriate where employees acted within the scope of their employment, such reimbursement is in the interest of the United States, as determined by the Inspector General or his or her designee, in his or her discretion, and funds are available from the OIG appropriation to pay the judgment.

C. Representation Issues

Whether a federal employee will be able to obtain DOJ representation depends upon two determinations. The first issue is whether the employee was acting within the scope of his employment.[4] In this context the scope of employment is determined by federal, not state law. The second issue is whether DOJ's representation of the employee is in the interest of the United States. 28 C.F.R. § 50.15(a). To determine whether the employee will be represented, the inquiry is generally whether the employee was about the government's business at the time of the occurrence. If the employee's acts were within the scope of his or her employment, there is a general presumption that representation would be in the interest of the government. If the DOJ determines that the employee was acting within the scope of employment and representation is in the interest of the United States but such representation is inappropriate — for example, when there are multiple federal employee defendants with potentially conflicting legal positions — the DOJ can authorize the employee to hire private counsel who will be paid by the government. If the DOJ rejects a request for representation, the individual employee may seek reimbursement for legal expenses after the litigation has concluded.

When DHS OIG employees have been sued, in either their official or personal capacities, the employees should contact the OIG Office of General Counsel (OGC). Because DHS representation is not automatic, employees who desire DOJ representation must request it in

[4] Whether an employee is acting within the scope of his or her employment for purposes of deciding whether DOJ representation will be provided in a Bivens claim is determined by general principles of tort law and may be different from the analysis used in the FTCA case.

writing. DHS OIG employees will be required to provide OGC an affidavit reciting the facts of the incident along with a copy of the summons and complaint or other legal documents. If necessary, OGC will conduct an internal review of the facts and circumstances that resulted in the lawsuit. If OGC concludes that the employee was acting within the scope of his or her employment, OGC will prepare a memorandum recommending that the Civil Division provide legal representation.

Seeking representation under these provisions should not be confused with Emergency, Interim Legal Representation for Federal Law Enforcement Officials in the immediate aftermath of a shooting or other use of force involving serious bodily injury. In those instances, representation is provided on a temporary basis until the DOJ makes a determination regarding representation during the pendency of a lawsuit.

III. CONCLUSION

It is critical to remember that although the Inspector General has authorized Special Agents to carry their OIG-issued firearm while off-duty, this decision does not expand Special Agents' law enforcement authority. Nor does it change, in any way, how DHS OIG Special Agents should utilize their official firearm. DHS OIG Special Agents should continue to use their law enforcement authority and their official firearm as they have done in the past, and abide by all OIG and DOJ Guidelines.

Under the Good Samaritan Act, an OIG Special Agent's off-duty use of force to protect others from a crime of violence occurring in the agent's presence will be deemed to be within the scope of the agent's employment for purposes of the FTCA. However, the Good Samaritan Act amended the definition of scope of employment only under the FTCA. Accordingly, it is less certain that DOJ will provide legal representation to an agent who is sued for a constitutional violation arising from an incident in which he or she engages in the off-duty use of force to protect others.

Some states authorize Special Agents to act as peace officers for the purpose of enforcing state laws. In most instances such authorization is limited to protecting the life of another or assisting local police. An OIG Special Agent who is sued for actions relating to the exercise of state law enforcement authority may not be provided representation by the Department of Justice unless those actions are deemed to be within the scope of the agent's federal employment.

If you have any questions about these legal issues, you should contact the OIG OGC or your Special Agent in Charge.

Exhibit 5-3, TSA 49 CFR 1544.219, Carriage of Accessible Weapons, January 1, 2007

C

Effective: [See Text Amendments]

Code of Federal Regulations Currentness
Title 49. Transportation
Subtitle B. Other Regulations Relating to Transportation
Chapter XII. Transportation Security Administration, Department of Homeland Security (Refs & Annos)
Subchapter C. Civil Aviation Security (Refs & Annos)
"Part 1544. Aircraft Operator Security: Air Carriers and Commercial Operators (Refs & Annos)
"Subpart C. Operations
— **§ 1544.219 Carriage of accessible weapons.**

(a) Flights for which screening is conducted. The provisions of § 1544.201(d), with respect to accessible weapons, do not apply to a law enforcement officer (LEO) aboard a flight for which screening is required if the requirements of this section are met. Paragraph (a) of this section does not apply to a Federal Air Marshal on duty status under § 1544.223.

(1) Unless otherwise authorized by TSA, the armed LEO must meet the following requirements:

(i) Be a Federal law enforcement officer or a full-time municipal, county, or state law enforcement officer who is a direct employee of a government agency.

(ii) Be sworn and commissioned to enforce criminal statutes or immigration statutes.

(iii) Be authorized by the employing agency to have the weapon in connection with assigned duties.

(iv) Has completed the training program "Law Enforcement Officers Flying Armed."

(2) In addition to the requirements of paragraph (a)(1) of this section, the armed LEO must have a need to have the weapon accessible from the time he or she would otherwise check the weapon until the time it would be claimed after deplaning. The need to have the weapon accessible must be determined by the employing agency, department, or service and be based on one of the following:

(i) The provision of protective duty, for instance, assigned to a principal or advance team, or on travel required to be prepared to engage in a protective function.

(ii) The conduct of a hazardous surveillance operation.

(iii) On official travel required to report to another location, armed and prepared for duty.

(iv) Employed as a Federal LEO, whether or not on official travel, and armed in accordance with an agency-wide policy governing that type of travel established by the employing agency by directive or policy statement.

(v) Control of a prisoner, in accordance with § 1544.221, or an armed LEO on a round trip ticket returning from escorting, or traveling to pick up, a prisoner.

Exhibit 5-4, Attorney General's Policy Statement, "Use of Deadly Force," dated July 1, 2004

POLICY STATEMENT USE OF DEADLY FORCE
Approved by the Attorney General July 1, 2004

GENERAL PRINCIPLES

Law enforcement officers and correctional officers of the Department of Justice may use deadly force only when necessary, that is, when the officer has a reasonable belief that the subject of such force poses an imminent danger of death or serious physical injury to the officer or to another person.

A. Deadly force may not be used solely to prevent the escape of a fleeing suspect.

B. Firearms may not be fired solely to disable moving vehicles.

C. If feasible and if to do so would not increase the danger to the officer or others, a verbal warning to submit to the authority of the officer shall be given prior to the use of deadly force.

D. Warning shots are not permitted outside of the prison context.

Officers will be trained in alternative methods and tactics for handling resisting subjects, which must be used when the use of deadly force is not authorized by this policy.

CUSTODIAL SITUATIONS

II. Unless force other than deadly force appears to be sufficient, deadly force may be used to prevent the escape of a prisoner committed to the custody of the Attorney General or the Bureau of Prisons

A. if the prisoner is effecting his or her escape in a manner that poses an imminent danger to the safety of the officer or another person; or

B. if the prisoner is escaping from a secure facility or is escaping while in transit to or from a secure facility.

III. If the subject is in a non-secure facility, deadly force may be used only when the subject poses an imminent danger of death or serious physical injury to the officer or another person.

IV. If the subject is in transit to or from a non-secure facility and is not accompanied by a person who is in transit to or from a secure facility, deadly force may be used only when the subject poses an imminent danger of death or serious physical injury to the officer or to another person.

V. After an escape from a facility or vehicle and its immediate environs has been effected, officers attempting to apprehend the escaped prisoner may use deadly force only when the escaped prisoner poses an imminent danger of death or serious physical injury to the officer or another person.

VI. Deadly force may be used to maintain or restore control of a prison or correctional facility when the officer reasonably believes that the intended subject of the deadly force is participating in a disturbance in a manner that threatens the safety of the officer or another person.

VII. In the prison context, warning shots may be fired within or in the immediate environs of a secure facility if there is no apparent danger to innocent persons: (A) If reasonably necessary to deter or prevent the subject from escaping from a secure facility; or (b) if reasonably necessary to deter or prevent the subject's use of deadly force or force likely to cause serious physical injury.

APPLICATION OF THE POLICY

VIII. This policy is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or equity, against the United States, its departments, agencies, or other entities, its officer or employees, or any other person.

Exhibit 5-5, INV form-92, Ammunition Inventory Log

Office of Inspector General - Investigations
U.S. Department of Homeland Security

Homeland Security

AMMUNITION INVENTORY LOG

FIELD OFFICE: ____________ AMMUNITION TYPE: ____________

Date	Receipts	Issuances	Purpose	Balance	Initials

FORM INV-92

Page ___ of ___

Exhibit 5-6, Defensive Tactics Evaluation Checklist

DEPARTMENT OF HOMELAND SECURITY
OFFICE OF INSPECTOR GENERAL
DEFENSIVE TACTICS TRAINING
PERFORMANCE EVALUATION CHECKLIST

NAME:_____

LOCATION:_____ **DATE:**_____

TASK	P/F
1. [redacted]**:** [redacted]	
2. [redacted]**:** [redacted]	
3. [redacted]**:** [redacted]	
4. [redacted]**:** [redacted]	
5. [redacted]**:** [redacted]	

INV Form-96

COMMENTS:

_____

_____

_____

_____

DHS-OIG DT Instructor Signature: _____

Date: _____

INV Form-96

6.0 TRAINING

6.1 GENERAL

All SA training will be job-related and otherwise consistent with the training policies of the OIG and Office of Personnel Management (OPM). Sources of training used by the OIG include the Federal Law Enforcement Training Center (FLETC) and the Inspector General Criminal Investigator Academy (IGCIA), as well as other public and private vendors.

The Operations and Planning Division (OPD) will coordinate all training. OPD will periodically circulate a list of available training programs.

SAs wishing to enroll in training will obtain authorization from their SAC.

6.2 BASIC TRAINING

All SAs will complete the Criminal Investigator's Training Program (CITP) at the FLETC or an approved equivalent program. Generally, the approved comparable courses of instruction are: The FBI, Basic Special Agent Academy; DEA, Basic Special Agent Academy; US Postal Inspection Service, Basic Inspector Training Program; U.S. Army Military Police School, CID Special Agent Course; U.S. Air Force, Office of Special Investigations, Special Investigators Course.

The Inspector General Investigator Training Program (IGITP) is a follow on course to CITP conducted at the IGCIA.

The Inspector General Transitional Training Program (IGTTP) is a program designed for SAs who have recently transferred to the investigative divisions of the OIG from other investigative agencies. This program is designed to familiarize an SA with the practices and resources that are IG specific.

6.3 SPECIALIZED TRAINING

[redacted]

The Attorney General guidelines **(Exhibit 2-4)** require that OIG SAs complete periodic refresher training in the following areas: trial process, federal criminal and civil legal

updates, interviewing techniques and policy, law of arrest, search and seizure, physical conditioning, firearms, and defensive tactics. For OIG purposes, periodic is defined as being every 3 to 5 years.

In addition to the training required by the AG Guidelines, all OIG employees are mandated to complete annual training as identified in Directive OIG 76-1. This Directive can be accessed through the OIG Intranet (http://intranet).

6.4 MANDATORY TRAINING

There are mandatory annual training modules required for law enforcement related positions. They include Flying While Armed (see Chapter 5.6) and Bloodborne Pathogens.

BLOODBORNE PATHOGENS

The OIG is committed to providing a safe and healthful work environment for our entire staff. In pursuit of this endeavor, the following exposure control plan (ECP) **(Exhibit 6-1)** is provided to eliminate or minimize occupational exposure to bloodborne pathogens in accordance with Occupational Safety and Health Administration (OSHA) Bloodborne Pathogen standard 29 CFR 1910.1030, which prescribes safeguards to protect workers against the health hazards caused by bloodborne pathogens.

The ECP is a key document to assist the OIG in implementing and ensuring compliance with the standard. This ECP includes guidance on:

* Determination of employee exposure

* Implementation of various methods of exposure control, including:
  - Universal precautions
  - Work practice controls
  - Personal protective equipment
  - Housekeeping

* Hepatitis B vaccination

* Incident response and remediation

* Post-exposure evaluation and follow-up

* Communication of hazards to employees and training

* Recordkeeping

* Procedures for evaluating circumstances surrounding an exposure incident

The methods of implementation of these elements of the standard are discussed in the ECP. **(Exhibit 6-1) Exhibits 6-1** and **6-2** are used to comply with the ECP.

6.5 INDIVIDUAL DEVELOPMENT PLAN

Each year, in conjunction with their annual final performance appraisal, SAs will prepare an Individual Development Plan (IDP). **(Exhibit 6-3)** Reference is made to Directive OIG-76-1, which outlines the procedures for the completing the OIG IDP (OIG Form 76-1-1). SAs are reminded that the IDP is a planning document. Requested training may not always be available or approved. The completed IDP will be retained in the Employee Personnel File (EPF).

6.6 ADMINISTRATION OF TRAINING

A training history and record of special law enforcement skills for all SAs is maintained in EDS. The training history will be updated in EDS whenever SAs attend job-related training.

SAs request training by completing a Standard Form (SF)-182 (Request, Authorization, Agreement and Certification of Training) in DHScovery (https://DHScovery@dhs.gov). The completed SF-182 will be routed for approval in DHScovery.

Upon completion of training, the employee and his/her supervisor are responsible for completing the course evaluation section of the SF-182 in DHScovery.

In most cases, agencies and vendors providing training will accept the SF-182 as payment. In cases where the SF-182 is not accepted, the Government-wide Commercial Purchase Card (GwCPC) or other payment methods may be used upon INV approval. An SF-182 is always required, regardless of payment method. For training at FLETC, a Class Registration Form will be completed by the requesting office and submitted to OPD. **(Exhibit 6-4)**

The general travel cards issued to INV personnel cannot be used to pay for training.

SAs should make every effort to attend scheduled training. Cancellations should be made only in emergencies and every effort must be made to obtain a refund from the vendor or re-schedule the training.

6.7 BASIC FIREARMS/USE-OF-FORCE TRAINING

Newly appointed SAs without prior law enforcement experience, shall not be issued firearms or other weapons until they have successfully completed basic firearms and use-of-force training.

Basic firearms/use-of-force training shall consist of that provided during the CITP at FLETC, or comparable training such as the OIG approved Transitional Pistol Training Course contained in the Training Guidelines Handbook.

SAs will receive annual training in use of force and FAA procedures for traveling while armed. (Chapters 2.5 and 5.7) Documentation of this training will be maintained in the administrative firearms file and recorded in EDS.

6.8 FIREARMS QUALIFICATION STANDARDS

SAs are required to qualify quarterly with their issued handgun in accordance with the course of fire provided in the Training Guidelines Handbook. Any SA who fails to achieve a qualifying score during the quarter will not be authorized to carry a firearm until they qualify. SA's will be given a maximum of three range dates per quarter to fire a qualifying score on the OIG approved practical pistol course, or other approved course of fire during quarterly firearms training sessions. SAs may be permitted to fire as many times as necessary to qualify during each of the three range dates. Intervening practice, after the first qualification attempt, may be allowed.

The firearms instructor will report all failures to qualify to the SAC and the National Firearms Program Manager as soon as possible following the close of the scheduled training session. As soon as possible, special and/or remedial training will be provided to assist any shooter unable to qualify.

If duty related responsibilities keep the SA from qualifying, the SAC may excuse an SA from qualifying for that quarter only by completing the appropriate section on the Firearms Certification Form (INV Form 91). The SA must qualify immediately in the following quarter or the SA will not be authorized to carry a firearm until they qualify. For extended periods longer than one quarter, the AIGI is the approving authority.

SAs must provide a memorandum to the SAC explaining any unexcused absences from scheduled firearms qualification training. Unjustified absence(s) from scheduled firearms training may result in disciplinary action.

SAs who have had significant repairs to their issued firearm will re-qualify prior to carrying the weapon.

SAs will also qualify semiannually on a reduced light course of fire, if facilities permit in accordance with the course of fire provided in the Training Guidelines Handbook.

On a semiannual basis, [redacted] provided in the Training Guidelines Handbook.

SAs who have requested approval to carry a non-issued weapon, must qualify on an approved course of fire as a condition of authorization to carry the weapon.

The Firearms Instructor will complete the Firearms Certification (INV Form 91) and make the appropriate entries into EDS.

All courses of fire are determined by the National Firearms Program Manager and are identified in the Training Guidelines Handbook.

6.9 FIREARMS INSTRUCTORS

The National Firearms Program Manager ensures that firearms and use-of-force training are accomplished in accordance with the Attorney General's guidelines. (**Exhibit 2-4**) In addition, each office will designate a qualified Firearms Instructor to coordinate required firearms and use of force training. The Firearms Instructor will administer the office's weapons and use of force programs and issue firearms and ammunition.

Firearms Instructors must successfully complete firearms instructor training at the FLETC or another course approved by the National Firearms Program Manager. Firearms Instructors should be re-certified every five years through in-service training.

Firearms Instructors will maintain an office file of quarterly firearms qualification scores and any applicable certifications attained by the SAs utilizing the "Firearms Certification," INV Form-91. **(Exhibit 6-5)**

The range safety rules and use of force policy will be reviewed as part of the weapons qualification process utilizing INV Form-91.

Any weapon determined by a Firearms Instructor to be unserviceable must be withdrawn from service. The National Firearms Program Manager will determine the most efficient way to have the weapon repaired.

Only a qualified armorer or the firearm manufacturer is authorized to make repairs or modifications to INV firearms. The National Firearms Program Manager must approve these repairs or modifications.

Firearms Instructors may be removed from this position at the discretion of the SAC.

6.10 PHYSICAL TRAINING (PT)

SAs may be authorized to participate in PT activities during the workday up to three hours per week. PT hours cannot accumulate from week to week. SAs will record PT time taken on their Bi-weekly Activity Reports as Training.

SAs wishing to participate must submit a memorandum annually to their SAC requesting authorization to participate in PT on official time (Chapter 4.2).

SAs are only permitted to engage in authorized physical fitness activities as recognized by the U.S. Department of Labor (DOL) for coverage under the Federal Employees

Compensation Act (FECA). These activities include, but are not limited to: calisthenics, aerobic exercise, rowing, bicycling/Lifecycle, Stairmaster, elliptical trainer, spinning, swimming, weight training, walking, jogging, and running.

Competitive contact and dangerous activities of any kind are not approved as part of this program. Such activities historically prohibited by the DOL under FECA would include: racquetball, handball, basketball, football, contact martial arts, boxing, roller-skating, roller-blading, football, skiing, ice-skating, bowling, and golf.

To minimize the risk of injury, agents will not engage in physical fitness during hazardous conditions (e.g., conditions of poor visibility and/or weather extremes).

OIG may reimburse agents for memberships in health or fitness facilities pursuant to the Employee Fitness Subsidy Program.

CHAPTER - 6.0 EXHIBITS

Exhibit 6-1, OIG Exposure Control Plan

U.S. DEPARTMENT OF HOMELAND SECURITY
OFFICE OF INSPECTOR GENERAL
BLOODBORNE PATHOGEN EXPOSURE CONTROL PLAN

The Office of Inspector General (OIG) is committed to providing a safe and healthful work environment for our entire staff. In pursuit of this endeavor, the following exposure control plan (ECP) is provided to eliminate or minimize occupational exposure to bloodborne pathogens in accordance with OSHA standard 29 CFR 1910.1030, "Occupational Exposure to Bloodborne Pathogens."

The ECP is a key document to assist the OIG in implementing and ensuring compliance with the standard, thereby protecting our employees. This ECP includes:

- Determination of employee exposure
- Implementation of various methods of exposure control, including:
  - Universal precautions
  - Work practice controls
  - Personal protective equipment
  - Housekeeping
- Hepatitis B vaccination
- Incident response and remediation
- Post-exposure evaluation and follow-up
- Communication of hazards to employees and training
- Recordkeeping
- Procedures for evaluating circumstances surrounding an exposure incident

The methods of implementation of these elements of the standard are discussed in the subsequent pages of this ECP.

PROGRAM ADMINISTRATION

- The Office of Training is responsible for the implementation of the ECP. The Office of Training will maintain, review, and update the ECP annually, and whenever necessary to include new or modified tasks and procedures.

- Those employees who are determined to have potential occupational exposure to blood or other potentially infectious materials (OPIM) must comply with the procedures and work practices outlined in this ECP.

- Field Offices, RAC Offices, and Sub-Offices will maintain and provide all necessary personal protective equipment (PPE) and will ensure that adequate supplies of the aforementioned equipment are available.

- The Office of Training will be responsible for ensuring that all medical actions required are performed and that appropriate employee health and OSHA records are maintained.

- The Office of Training will be responsible for training, documentation of training, and making the written ECP available to employees, and OSHA.

EMPLOYEE EXPOSURE DETERMINATION

The following is a list of all job classifications within the OIG in which all employees have potential occupational exposure.

JOB TITLE

Special Agents (GS-1811)
Investigators (GS-1810)

METHODS OF IMPLEMENTATION AND CONTROL

Universal Precautions

All employees will utilize universal precautions.

Exposure Control Plan

Employees covered by the bloodborne pathogens standard will review the standards in their annual refresher training in DHScovery. All employees have an opportunity to review this plan at any time by contacting The Office of Training.

The Office of Training is responsible for reviewing and updating the ECP annually or more frequently if necessary to reflect any new or modified tasks and procedures which affect occupational exposure and to reflect new or revised employee positions with occupational exposure.

Personal Protective Equipment (PPE)

- PPE is provided to our employees at no cost to them.

- The types of PPE available to employees are as follows:

- Latex gloves, eye protection.

- PPE is located in all Field Offices, RAC Offices and Sub-Offices.

- All employees using PPE must observe the following precautions:

    - Wash hands immediately or as soon as feasible after removal of gloves or other PPE.
    - Remove PPE after it becomes contaminated.
    - Wear appropriate gloves when it can be reasonably anticipated that there may be hand contact with blood or OPIM, and when handling or touching contaminated items or surfaces; replace gloves if torn, punctured, contaminated, or if their ability to function as a barrier is compromised.
    - Utility gloves may be decontaminated for reuse if their integrity is not compromised; discard utility gloves if they show signs of cracking, peeling, tearing, puncturing, or deterioration.
    - Never wash or decontaminate disposable gloves for reuse.
    - Wear appropriate face and eye protection when splashes, sprays, spatters, or droplets of blood or OPIM pose a hazard to the eyes, nose, or mouth.
    - Remove immediately or as soon as feasible any garment contaminated by blood or OPIM, in such a way as to avoid contact with the outer surface.

The procedure for handling used PPE is as follows:

Field Offices, RAC Offices and Sub-Offices will identify a local vendor certified to handle and remove used PPE.

Laundry

- Contaminated articles will be laundered by a company identified by each Field Office, RAC Office and Sub-Office.

- The following laundering requirements must be met by the vendor:

    - Handle contaminated laundry as little as possible, with minimal agitation.
    - Place wet contaminated laundry in leak-proof, labeled or color-coded containers before transport. Use *red bags or bags marked with biohazard symbol* for this purpose.
    - Wear PPE when handling and/or sorting contaminated laundry

HEPATITIS B VACCINATION

The DHScovery "Bloodborne Pathogen Awareness" Module will provide training to employees on hepatitis B vaccinations, addressing the safety, benefits, efficacy, and methods of administration.

The hepatitis B vaccination series is available at no cost to employees identified in the exposure determination section of this plan. Vaccination is encouraged unless: 1) documentation exists that the employee has previously received the series, 2) antibody testing reveals that the employee is immune, or 3) medical evaluation shows that vaccination is contraindicated.

However, **if an employee chooses to decline vaccination, the employee must sign a declination form.** Employees who decline may request and obtain the vaccination at a later date at no cost. Documentation of refusal of the vaccination is kept with the Office of Training.

Vaccination will be provided by Federal Occupational Health clinics.

POST-EXPOSURE EVALUATION AND FOLLOW-UP

Should an exposure incident occur, contact The Office of Training.

An immediately available confidential medical evaluation and follow-up will be conducted by a Federal Occupational Health Clinic, or a physician chosen by the exposed employee. Following the initial first aid (clean the wound, flush eyes or other mucous membrane, etc.), the following activities will be performed:

- Document the routes of exposure and how the exposure occurred.
- Identify and document the source individual (unless the employer can establish that identification is infeasible or prohibited by state or local law).
- Obtain consent and make arrangements to have the source individual tested as soon as possible to determine HIV, HCV, HBV infectivity; document that the source individual's test results were conveyed to the employee's health care provider.
- If the source individual is already known to be HIV, HCV and/or HBV positive, new testing need not be performed.
- Insure that the exposed employee is provided with the source individual's test results and with information about applicable disclosure laws and regulations concerning the identity and infections status of the source individual (e.g., laws protecting confidentiality).
- After obtaining consent, collect exposed employee's blood as soon as feasible after exposure incident, and test blood for HBV and HIV serological status.
- If the employee does not give consent for HIV serological testing during collection of blood for baseline testing, preserve the baseline blood sample for at

least 90 days; If the exposed employee elects to have the baseline sample tested during this waiting period, perform testing as soon as feasible.

ADMINISTRATION OF POST-EXPOSURE EVALUATION AND FOLLOW-UP

The Office of Training ensures that health care professional(s) responsible for employees' hepatitis B vaccination and post-exposure evaluation and follow-up are given a copy of OSHA's bloodborne pathogens standard.

The Local Manager (SAC or RAC) ensures that the health care professional evaluating an employee after an exposure incident receives the following:

- A description of the employee's job duties relevant to the exposure incident route(s) of exposure.
- Route(s) of exposure.
- Circumstances of exposure.
- If possible, obtain results of the source individual's blood test.
- Relevant employee medical records, including vaccination status.

PROCEDURES FOR EVALUATING THE CIRCUMSTANCES SURROUNDING AN EXPOSURE INCIDENT

The Office of Training will review the circumstances of all exposure incidents to determine:

- Work practices followed.
- Protective equipment or clothing that was used at the time of the exposure incident (gloves, eye protection, etc.)
- Location of the incident.
- Activity being performed when the incident occurred.
- Employee's training.

EMPLOYEE TRAINING

All employees who have potential occupational exposure to bloodborne pathogens must complete the DHScovery Bloodborne Pathogen Awareness Module annually (1811's & 1810's).

The Bloodborne Pathogen Awareness Module includes the topics of epidemiology, symptoms and transmission of bloodborne pathogen diseases. Additionally, the training program covers, at a minimum, the following elements.

- An explanation of methods to recognize tasks and other activities that may involve exposure to blood and OPIM, including what constitutes an exposure incident.

- An explanation of the use and limitations of work practices, and PPE.
- An explanation of the types, uses, location, removal, handling, decontamination, and disposal of PPE.
- An explanation of the basis for PPE selection.
- Information on the hepatitis B vaccine, including information on its efficacy, safety, method of administration, the benefits of being vaccinated, and that the vaccine will be offered free of charge.
- Information on the appropriate actions to take and persons to contact in an emergency involving blood or OPIM.
- An explanation of the procedure to follow if an exposure incident occurs, including the method of reporting the incident and the medical follow-up that will be made available.
- Information on the post-exposure evaluation and follow-up that the employer is required to provide for the employee following an exposure incident.

RECORDKEEPING

Training Records

Training records are completed for each employee upon completion of training. These documents will be kept for at least **three years** in the employee's personal profile within DHScovery.

The training records include:

- The dates of the training sessions.
- The contents or a summary of the training sessions.

Medical Records

Medical records are maintained for each employee with occupational exposure in accordance with 29 CFR 1910.1020, "Access to Employee Exposure and Medical Records."

The Office of Training is responsible for maintenance (collection and proper storage) of the required medical records. These **confidential** records are kept at The Office of Training for at least the **duration of employment plus 30 years.**

Employee medical records are provided upon request of the employee or to anyone having written consent of the employee within 15 working days. Such requests should be sent to the Office of Training.

OSHA Recordkeeping

An exposure incident is evaluated to determine if the case meets OSHA's Recordkeeping Requirement (29 CFR 1904). This determination and the recording activities are done by the Office of Training.

DEPARTMENT OF HOMELAND SECURITY
OFFICE OF INSPECTOR GENERAL
BLOODBORNE PATHOGEN PROGRAM
HEPATITIS B VACCINE DECLINATION (MANDATORY)

I understand that due to my occupational exposure to blood or other potentially infectious materials I may be at risk of acquiring hepatitis B virus (HBV) infection. I have been given the opportunity to be vaccinated with hepatitis B vaccine, at no charge to myself. However, I decline hepatitis B vaccination at this time. I understand that by declining this vaccine, I continue to be at risk of acquiring hepatitis B, a serious disease. If in the future I continue to have occupational exposure to blood or other potentially infectious materials and I want to be vaccinated with hepatitis B vaccine, I can receive the vaccination series at no charge to me.

Signed: _____

Date: _____

Exhibit 6-2, Bloodborne Pathogen Annual Compliance Report

DEPARTMENT OF HOMELAND SECURITY, OFFICE OF INSPECTOR GENERAL

Bloodborne Pathogen Program
Annual Compliance Report

Field Office: _____ **RAC/Sub Office:** _____

Report Completed By: _____

Federal Occupational Health Clinic

Address: _____

Phone: _____

Point of Contact: _____

Date of last contact & confirmation of service availability: _____

All applicable OIG employees have been offered hepatitis B vaccination, Certified by SAC (Signature):

_____

Post-Incident Site Cleaning Vendor

Company Name: _____

Address: _____

Phone (Office & 24 hour emergency): _____

Point of Contact, Title: _____

Date of contact & confirmation of service availability: _____

Post-Incident Laundry Vendor

☐ Same as above

Company Name: _____

Address: _____

Phone (Office & 24 hour emergency): _____

Point of Contact, Title: _____

Date of contact & confirmation of service availability: _____

Personal Protective Equipment

An ample supply of rubber gloves & eye protection is available to all employees with potential exposure to bloodborne pathogens.

Certified (SAC): _____

Exhibit 6-3, OIG Form 76-1-1 OIG Individual Development Plan

OIG Individual Development Plan
FY _____

1. Name	2. Position Title	3. Series/Grade	4. Office of Assignment

5. SHORT-RANGE CAREER GOALS: Specify position title & grade or subject area of where you want to be in 1 to 2 years. State Goals.

6. LONG-RANGE CAREER GOALS: Specify position title & grade or subject area of where you want to be in 3 to 5 years. State Goals.

7. DEVELOPMENT OBJECTIVES: List knowledge, skills and abilities (KSAs) or competencies needed immediately to meet current objectives or to improve performance in present position or identify specific areas you will need in order to achieve the short or long range goals stated above. The Developmental Objectives should be stated in order of priority. *

*PRIORITY: (1) Mission Essential; (2) To increase effectiveness of mission accomplishment; (3) For career development or to increase job efficiency and productivity.

8. SIGNIFICANT PRIOR TRAINING AND DEVELOPMENT (related to the Developmental Objectives of your Short Range Career Goals).

9. Were areas of improvement identified in latest rating?

Yes_____ No_____ N/A_____

10. If no career development is desired or needed at this time, please state specific reason(s).

11. CERTIFICATION: I certify that the training, development, or education identified in this plan constitutes a valid management need for maximum performance of mission requirements and has been developed for the purpose of increasing the employee's performance in his or her current position or to prepare him or her for an identified target assignment.

Employee's Signature	Date	Supervisor's Signature	Date
_____	_____	_____	_____
		_____ (Position)	

OIG Form 76-1-1 (Date: August 2007)

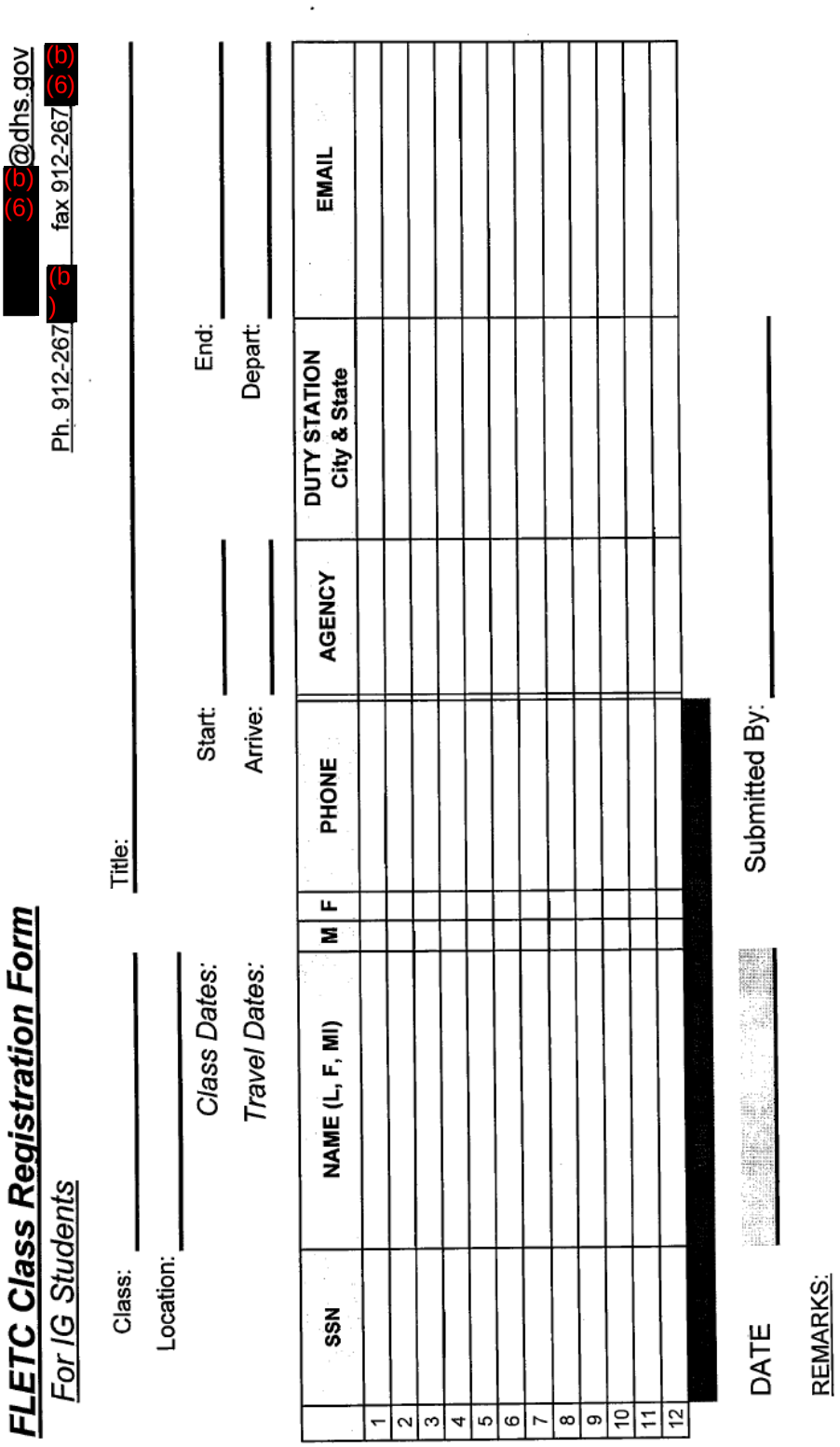
1

OIG Individual Development Plan
FY _____

Name:	
For period:	
Position and Grade:	
Supervisor:	
Office:	
I request a Mentor (yes or no):	**Date:**
Date Mentor assigned (if requested):	**Mentor:**
Career Goals for Training Purposes (from Page 1, #5 or #6):	

Course Title/Subject	*Required Yes/No*	*Date*	*Length*	*Training Provider*	*Estimated Costs Tuition Costs*	*Estimated Costs Travel Per Diem*	*CPEs # or N/A*	*Date Completed*

Exhibit 6-4, FLETC Class Registration Form



FLETC Class Registration Form

For IG Students

Please email to: [redacted]@dhs.gov

Ph. 912-267-[redacted] fax 912-267-[redacted]

Class: _____ Title: _____

Location: _____ Class Dates: Start: _____ End: _____

Travel Dates: Arrive: _____ Depart: _____

	SSN	NAME (L, F, MI)	M	F	PHONE	AGENCY	DUTY STATION City & State	EMAIL
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								

DATE [redacted] Submitted By: _____

REMARKS:

STAND-BY

FLETC Class Registration Form

For IG Students

Please email to:
(b)(6)@dhs.gov
Ph. 912-267(b)(6) fax 912-267(b)(6)

Class: _____ Title: _____

Location: _____

Class Dates: Start: _____ End: _____

Travel Dates: Arrive: _____ Depart: _____

	SSN	NAME (L, F, MI)	M	F	PHONE	AGENCY	DUTY STATION City & State	EMAIL
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								

DATE _____ Submitted By: _____

REMARKS:

Inspector General Criminal Investigator Academy

Class Registration Form

Class: _____ Location: _____

Class Dates: Start: _____ End: _____

Travel Dates: Arrive: _____ Depart: _____

	SSN (Mandatory)	NAME (L, F, MI)	M	F	PHONE	AGENCY	DUTY STATION City & State	EMAIL
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								
21								
22								
23								
24								

DATE _____ Submitted By: _____

REMARKS:

***** At time of registration, please make sure your agency's proper billing documents are on record with [redacted] You can contact her at [redacted]@tigta.treas.gov or 912-267-[redacted]

Exhibit 6-5, INV Form-91, Firearms Certification

Office of Inspector General - Investigations
U.S. Department of Homeland Security

Homeland Security

FIREARMS CERTIFICATION

Name: _____
(Last, First, MI)

Office: _____
(Post of Duty)

Location of Training: _____

Date of Training: _____

Instructor(s): _____

Weapon (*Make, model, & serial no.*): _____

Certification Includes:

Course	Pass(P); Fail (F); or Not Applicable (N/A)	Student's Initials:	Instructor's Initials
OIG Semi-Auto Pistol Course			
Other Course of Fire (explain)			
Safety & Use of Force Policy Course			

Waiver for Firearms Qualification (check one)

Medical: ☐ Travel: ☐ Other: ☐

Explain:

Authorizing Signature (SAC)/Date for Firearms Waiver:

_____

INV FORM-91

FIREARMS CERTIFICATION

Range Safety Rules

1. Firing of weapons will only be permitted with the authorization of a certified firearm instructor.
2. Ear and eye protection will be worn at all times while firing on the range.
3. "Dry firing" will only be allowed at the direction and under the supervision of a firearm instructor.
4. Load and unload weapons only in designated areas and never in a classroom.
5. Follow all commands from a firearm instructor.
6. At all times, the muzzle of a weapon will be pointed in a safe direction. When on the firing line, an upholstered weapon will be pointed down range with the trigger finger off of the trigger and outside of the trigger guard, until firing commands are given by a firearm instructor. No shooter will point a weapon in a direction other than down range unless specifically instructed to do so by a firearm instructor.
7. Do not move from your firing lane unless directed by a firearm instructor. Do not bend over to retrieve magazines, rounds, or other items from the ground, until a firearm instructor has declared the line safe and authorizes the retrieval of items on the ground.
8. If you need assistance, keep your weapon pointed down range, remain in position, raise your non-shooting hand, and wait for assistance from an instructor.
9. On the firing line, questions or comments should be directed to a firearm instructor, not other shooters.
10. A command of "Cease fire or stop firing" issued by a firearm instructor means all shooters will stop immediately and await further instructions.

I have read and agree to abide by the above safety rules.

Signature: _____ Date: _____

INV FORM-91

FIREARMS CERTIFICATION

USE OF FORCE POLICY

Authorized Use of Deadly Force

Deadly force may be employed only as a last resort when the SA has reasonable belief that the subject of such force poses an imminent danger of death or serious bodily injury to the SA or to another person.

Initial Response

It must be made perfectly clear that in some situation the proper initial response might be the application of deadly force.

Verbal Warnings:

If feasible, and if to do so would not increase the danger to the SA or others, a verbal warning to submit to the authority of the officer shall be given prior to the use of deadly force. The protection of life and/or the prevention of serious physical injury are prime concerns when confronting situation in which the use of deadly force may be implemented.

Fleeing Felons

Deadly force may be used to prevent the escape of a fleeing subject if there is probable cause to believe (1) the subject has committed a felony involving the infliction, or threatened infliction, of serious physical injury or death, or (2) the escape of the subject would impose an imminent danger of death or serious physical injury to the SA or another person.

Warning Shots

Warning shots are expressly prohibited

Firing at Moving Vehicles

SAs may fire at the driver or other occupants of a moving vehicle only when the SA has a reasonable belief that the subject(s) pose an imminent danger of death or serious physical injury to the SA or to another person and the public safety benefits of using such force outweigh the risks to the safety of the SA or other persons.

Shooting Dangerous Animals

Deadly force may be directed against dogs or other vicious animals when necessary for self-defense or defense of others.

Use of Force to Intervene in Criminal Activity in Progress.

If, while carrying an OIG approved firearm, a Special Agent observes a situation in which there is an imminent danger of loss of life or serious bodily injury to the SA or another person, the use of deadly force is authorized.

Under the Good Samaritan Act (28 USC 2671), an SA's off duty use of force to protect others from a crime of violence occurring in the SA's presence will be deemed within the scope of the SA's employment for the purposes of the Federal Tort Claims Act (FTCA). An SA who is sued for actions relating to the exercise of state law enforcement authority may not be provided representation by the DOJ, unless those actions are deemed to be with in the scope of the SA's federal employment.

Escapees who are Federal Prisoners: Section B of the Attorney General's Use of Deadly Force Policy Statement, specifically differentiates policy between a Bureau of Prisons escapee and an immigration detainee. Paragraph 2 states that the use of deadly force is not permitted if the subject is in a non-secure facility under the control of the Immigration and Naturalization Service, and (a) has not used or threatened the use of force likely to cause serious physical injury in his or her escape attempt, and (b) has not otherwise manifested an imminent threat of death or serious physical injury to the officer of community.

Signature:_____ Date:_____

INV FORM-91

7.0 PROCESSING ALLEGATIONS

7.1 RECEIPT OF ALLEGATIONS

The OIG has established a Hotline to facilitate and encourage the reporting of instances of waste, fraud and abuse. Management of the hotline is the responsibility of the SAC of ISD.

The Hotline number is: (800) 323-8603
The Hotline Fax number: (202) 254-4297
The Hotline address is: Department of Homeland Security
Office of Inspector General
245 Murray Drive, Building 410, SW
Washington, D.C. 20528

All allegations involving DHS programs, employees, contractors, or operations, however received, will be entered into the Enforcement Data System (EDS) by the Hotline staff.

OIG offices will forward predicating documents for field originated allegations to the Hotline staff at DHSINVCOMPLAINTS@DHS.Gov.

7.2 CLASSIFICATION OF ALLEGATIONS

Allegations will be processed in accordance with the DHS Management Directive 0810.1 and any applicable MOUs. (Chapter 2.7) All allegations will be assigned a reference number in EDS and identified in one of the following ways:

- A complaint that lacks sufficient basis or detail will be administratively closed by ISD.
- A complaint may be referred to one of the DHS components with no reply requested.
- A complaint may be referred to one of the DHS components with a reply requested.
- A complaint that the OIG will investigate.

Complaints that have not been disposed of administratively may be opened as investigation by the ISD staff or referred to the appropriate field office for determination. The office will review the complaint and notify ISD of the disposition. Hotline staff will prepare a response to the initiating DHS component.

DHS components that receive an OIG complaint referral are obligated to notify the OIG should additional unreported criminal misconduct be uncovered during the course of their investigation.

7.3 ALLEGATIONS INVOLVING UNUSUAL CIRCUMSTANCES OR SUBJECTS

Congressional Inquiries: Congressional inquiries will be coordinated through Headquarters at the direction of the AIGI.

DHS OIG Employees: Allegations made against DHS OIG employees will be referred to SID.

Political and Schedule C Appointees: Allegations made against Presidential Appointees (PA), Presidential Appointees with Senate Confirmation (PAS), etc. will be referred to SID.

7.4 REFERRAL OF ALLEGATIONS BY DHS COMPONENTS

In accordance with Management Directive 0810.1 and MOUs with the IG, component agencies are generally required to refer the following categories of misconduct to the IG prior to initiating any independent action (Chapter 2.8).

All allegations of criminal misconduct against a DHS employee.

All allegations of serious, non-criminal misconduct against LEOs.

All allegations of non-criminal misconduct against employees at the GS/GM-15 level or higher, and all political, Schedule C appointees and CIS attorneys.

All allegations of non-criminal misconduct against an employee in the internal affairs division of a DHS entity.

All allegations regarding misuse or improper discharge of a firearm that results in death or personal injury, or otherwise warrants referral to the Civil Rights Criminal Division.

All allegations of fraud committed by contractors, grantees or other individuals or entities receiving DHS funds or otherwise engaged in the operation of DHS programs or operations.

All allegations of visa fraud by DHS employees in the visa issuance process.

Pursuant to an agreement between the OIG and the TSA Office of Inspection, several types of allegations against TSA employees that were routinely referred back to TSA will no longer be referred to the OIG. These allegation types are specifically identified in the agreement and are as follows:

Disorderly/intoxication/traffic/DUI
Failure to Appear (misdemeanor)
Minor theft from divestiture bins/checkpoint *
Computer misuse other than child pornography
Accidental discharge of a firearm not involving injury
OWCP fraud
Domestic violence by non-law enforcement officers
T&A/travel voucher fraud

* Instances of systemic theft or in excess of $2,000 will still be reported as will all allegations against K band and above employees.

In addition, the OIG will investigate allegations against individuals or entities that do not fit into the categories identified above, if the allegations reflect systemic violations, such as abuses of civil rights, civil liberties, or racial and ethnic profiling, serious management problems within the Department, or otherwise represent a serious danger to public health and safety.

7.5 CASE OPENING CRITERIA

The purpose of establishing case opening criteria is to properly align investigative activity with the Agency's strategic goals. [redacted]

[redacted]

7.6 CASE OPENING EXAMPLES

Sample Allegation1: [redacted]

Initiation Decision1: [redacted]

Sample Allegation 2: [redacted]

Initiation Decision 2: [redacted]

Sample Allegation 3: [redacted]

Sample Decision 3: [redacted]

Sample Allegation 4: [redacted]

Sample Decision 4: [redacted]

Sample Allegation 5: [redacted]

Sample Decision 5: [redacted]

7.7 [redacted]

[redacted]

[redacted]

***DHS Employee/Contractor** - *An individual who is appointed, contracted by, or assigned to perform official functions by the Department of Homeland Security.*

For the purpose of this definition, examples include: FTEs, contractors, sub-contractors, COREs, interns, Coast Guard military personnel (active and Reserve) and CG Auxiliaries; individuals assigned to DHS under the Intergovernmental Personnel Act; and employees detailed to DHS from other Federal agencies.

The definition does not include other federal, state, and local officials who are charged with managing DHS funded programs in their respective jurisdictions. For example; the mayor of a city who receives FEMA funds for debris removal is not considered a DHS employee. Similarly, a state Department of Homeland Security employee entrusted with awarding contracts for ambulance services would not be classified as a DHS employee under this definition.

- ***Employee/DHS Contractor Corruption*** –Abuse of public office for private gain. DHS employees and/or contractors who are alleged to have used their official position for personal gain: financial or otherwise. Allegations include:
  - [redacted]

[redacted]

- **Civil Rights/Civil Liberties** – DHS employees or contractors who, while acting under color of their official authority, are alleged to have deprived an individual of any Constitutional right or liberty. Definition includes discrimination and other civil rights violations on basis of race, ethnicity, religion, sex, national origin, sexual orientation, gender identity, family status, or disability. Allegations include:

  - Level 1 Allegations:

[redacted]

- Level 2 Allegations:

[redacted]

- Level 3 Allegations:

[redacted]

- ***Program Fraud / Financial Crimes*** – Alleged activity targeting DHS programs and/or financial systems, or having a nexus to such DHS programs or financial systems. Allegations herein may involve DHS employees and others conspiring to defraud the U.S. Government or governmental entities receiving DHS funds. Allegations include:

  - Level 1 Allegations:

[redacted]

[redacted]

- Level 2 Allegations:

[redacted]

- Level 3 Allegations:

[redacted]

- **General Criminal, Civil, and Administrative Allegations –** Alleged violations of law or regulations with a nexus to DHS programs, employees, or operations not otherwise classified as Corruption, Program Fraud/Financial Crimes or Civil Rights/Civil Liberties which may, or may not, be criminal in nature, or which reflect unfavorably or suspiciously upon the character and integrity of DHS, its employees or operations. Allegations include:

- [redacted]:

[redacted]

- [redacted]

[redacted]

- [redacted]:

[redacted]

l. [redacted]

7.8 CONFLICT OF INTEREST STATUTE REFERRALS

The AIGI is required to notify the Director, Office of Government Ethics (OGE) when any matter involving the alleged violation of Federal conflict of interest statutes is referred to the DOJ. This includes all violations of Title 18 U.S.C., § 203, 205, 207, 208, and 209. The Field Office SAC will notify OGE at the time of referral using OGE Form 202, "Notification of Conflict of Interest Referral." **(Exhibit 7-2).** The Field Office SAC will provide follow up reports to OGE of any indictment, information, or declination of prosecution, as well as any disciplinary or corrective action proposed, initiated, or taken by DHS, using OGE Form 202.

The Field Office SAC will provide copies of transmitted OGE Form 202s to the Deputy AIGI—Field Operations within 24 hours of filing with OGE. Once a final ROI has been issued and OGE has been notified of final action in the matter, the Deputy AIGI will provide a copy of the final OGE Form 202 to the DHS Designated Agency Ethics Official.

The OGE Form 202 should be submitted by email to referrals@oge.gov. If email submission is not feasible, forms may be mailed or transmitted by facsimile as noted below:

U.S. Office of Government Ethics
Attn: Associate Director, Program Review Division
1201 New York Avenue, N.W., Suite 500
Washington, DC 20005-3917

FAX # (202)-482-9238.

Additional information is available at the OGE website www.usoge.gov.

7.9 Whistleblower Retaliation and Reprisals Against Department of Homeland Security Employees

A **Whistleblower** is an employee, former employee, or applicant of the Department of Homeland Security (DHS) who discloses information that the individual reasonably believes evidences a violation of law, rule, or regulation, gross mismanagement, gross waste of funds, abuse of authority, or substantial and specific danger to public health or safety. It does not include a disclosure that is specifically prohibited by law or required by Executive order to be kept secret in the interest of national defense or foreign affairs, unless such information is disclosed to the Office Special Counsel, the Inspector General of an agency, or an employee designated by the head of the agency to receive it. **(Exhibit 7-3)**

Whistleblower Retaliation is the term that describes an adverse personnel action taken against a whistleblower as punishment for a disclosure. In order for retaliation to occur, the manager taking or directing the personnel action must be aware that the employee made the disclosure, and there must be clear and convincing evidence that the disclosure was a contributing factor to the decision to take the personnel action. These cases may also be called a form of reprisal.

Reprisals are those instances when a DHS employee, who has provided information to the OIG, has been threatened with an adverse personnel action or who has been harassed or harmed by any action for having made a complaint or provided information to the OIG.

The OIG has the authority to investigate whistleblower retaliation and reprisal complaints. However, if it is determined that no investigation will be conducted, the OIG will advise employees that they may file a complaint directly with the U.S. Office of Special Counsel (OSC). It is the primary purpose of the OSC to investigate Whistleblower retaliation cases. Only OSC can extend Whistleblower Protection status to an individual under the Whistleblower Protection Act.

7.10 Qui Tam Complaints

The False Claims Act, Title 31, United States Code, Section 3729, allows for a private individual, "whistleblower," with knowledge of past or present fraud against the federal government to bring suit on its behalf. The private person (known as the Relator) must have information that is not public knowledge that the defendant has knowingly submitted or caused the submission of false or fraudulent claims to the United States. Relators may receive between 5 and 10 percent of any award or settlement amount. This provides an incentive for "whistleblowers" to come forward.

Once a Relator brings suit on behalf of the government, the Department of Justice, in conjunction with the U.S. Attorney (USAO) for the district in which the suit is filed, has the option to intervene in the suit. Qui Tam actions are filed under seal, which has to be partially lifted by the court before the government can notify the company or person being sued that a claim has been filed. The identity of the relator may remain sealed after the suit has been dismissed.

These complaints are generally referred to the OIG by the respective USAO and will be investigated in coordination with the USAO.

CHAPTER 7.0 - EXHIBITS

Exhibit 7-1, Case Selection Criteria at a Glance

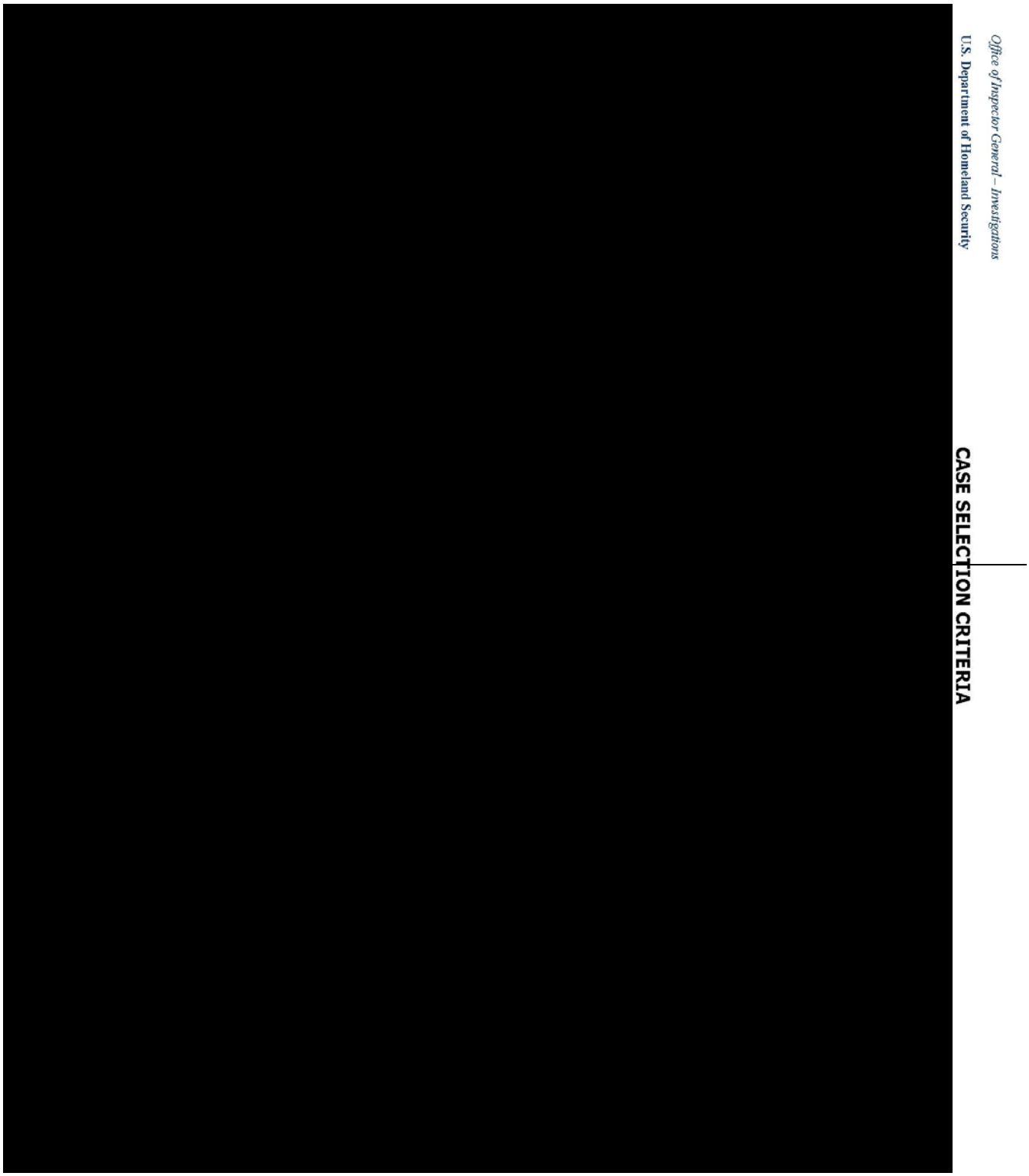


Exhibit 7-2, OGE Form 202, Notification of Conflict of Interest Referral

OGE Use Only

GSA Interagency Report Control No: 0398-OGE-AR

Notification of Conflict of Interest Referral

For use in cases involving possible violations of 18 U.S.C. §§ 203, 205, 207-209 by current or former executive branch employees only; see reverse for summary of statutory/regulatory background. Please return directly to: U.S. Office of Government Ethics, 1201 New York Ave. NW, Suite 500, Washington, DC 20005-3917. Phone: Chief, Program Review Division (202)208-8000, Extension 1115. FAX: (202)208-8038.

Agency Referring the Case	Agency Case or Referral Number	Case Referred to: ☐ DOJ, Public Integrity Section, Criminal Division ☐ U.S. Attorney for (district) _____ ☐ DOJ, other _____
Date of Referral to DOJ	Name of Employee Involved in Case (optional), Agency, and Agency Component Where he/she was Employed.	

PART I ETHICS TRAINING

Is there any evidence the individual received ethics training? ☐ YES ☐ NO ☐ UNCLEAR

PART II STATUTE(S) INVOLVED IN THIS CASE

Please check the appropriate box for the statute(s) involved in this case, then complete the rest of the information for the statute(s).

☐ **18 U.S.C. § 203 (Compensation for Representation Affecting the Government)**
Federal entity before which representation occurred: _____
Compensated representation on behalf of: _____
Were representational services rendered or to be rendered: ☐ by the employee ☐ or by another?

☐ **18 U.S.C. § 205 (Representation Affecting the Government)**
Federal entity before which representation occurred: _____
Representation on behalf of: _____

☐ **18 U.S.C. § 207 (Post-Employment)**
Federal entity before which representation occurred: _____
Representation on behalf of:
Was the communication/representation: ☐ oral? ☐ and/or written?
☐ Former employee termination service before January 1, 1991. Check subsections involved:
☐ 207(a) ☐ 207(b)(i) ☐ 207(b)(ii) ☐ 207(c)
☐ Former employee termination service on or after January 1, 1991. Check subsections involved:
☐ 207(a)(1) ☐ 207(a)(2) ☐ 207(b) ☐ 207(c) ☐ 207(d) ☐ 207(f)
If 207(b) or 207(f) is checked, was behind-the-scenes aid or advice involved? ☐ Yes ☐ No

☐ **18 U.S.C. § 208 (Acts Affecting a Personal Financial Interest)**
Does the case involve the financial interest: ☐ of the employee? ☐ of the employee's spouse?
☐ Minor child? ☐ A firm with which the employee was negotiating for employment?
☐ Other? (specify) _____
Was a waiver sought? ☐ Yes ☐ No Was it granted? ☐ Yes ☐ No
Was the employee required to file a financial disclosure form? ☐ Yes ☐ No If yes, check form involved:
☐ SF 278 ☐ OGE Form 450 ☐ Other (specify) _____
If so, was the basis for the interest disclosed on the financial disclosure form? ☐ Yes ☐ No

☐ **18 U.S.C. § 209 (Supplementation of Salary)**
Type of supplementation (meals, travel, cash, etc.): _____
Value of supplementation: $ _____ Number of supplements: _____

☐ **Additional Statutes Involved in Conflict of Interest Referrals**
Was 18 U.S.C. § 201 (bribery/gratuity) involved? ☐ Yes ☐ No
Was 5 U.S.C. App. (Ethics in Government Act) § 501 (outside earned income) involved? ☐ Yes ☐ No
Was 5 U.S.C. App. (Ethics in Government Act) § 502 (outside employment) involved? ☐ Yes ☐ No
Was 18 U.S.C. § 1001 (false statements) involved? ☐ Yes ☐ No
Was 5 U.S.C. App. (Ethics in Government Act) § 101 et.seq. (Financial disclosure) involved? ☐ Yes ☐ No
Other (list) _____

Agency Contact/Telephone Number	Date

OGE Form 202 (2/02)

Statutory/Regulatory Background

28 U.S.C. § 535 requires every department or agency to report to the Attorney General any information, allegations, or complaints relating to violations of title 18 of the United States Code involving Government employees, including possible violations of 18 U.S.C. § 207 by former Government employees. The Director of the Office of Government Ethics (OGE), in accordance with 5 U.S.C. App. § 402(e)(2), has promulgated regulations at 5 C.F.R. § 2638.603 requiring agencies to concurrently notify the Director when any matter involving a violation of 18 U.S.C. §§ 203, 205, 207, 208, and/or 209 is referred to the Department of Justice pursuant to 28 U.S.C. § 535. Such notification may be accomplished by providing a copy of the referral document or by submitting this optional form, unless such notification would otherwise be prohibited by law. OGE regulations also require that the department or agency subsequently notify the Director of the referral's disposition, including any disciplinary or corrective action taken by the department or agency. 5 C.F.R. § 2638.603(c). Information relating to the disposition of a referral may be communicated to the Director in writing.

PART III ADDITIONAL AGENCY COMMENTS (if any):

—

PART IV DISPOSITION OF REFERRAL (OGE use only):

☐ DOJ declined prosecution.

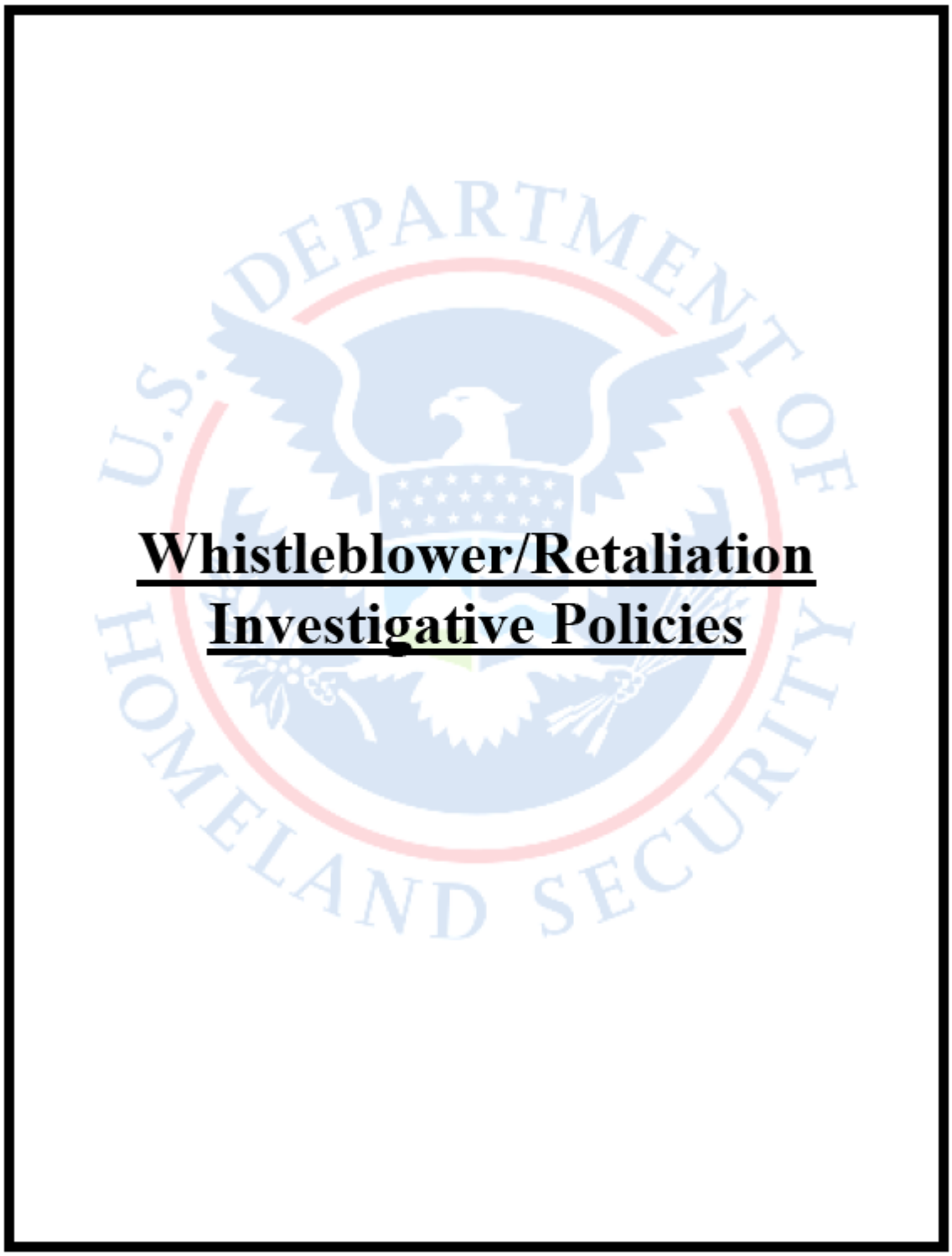
☐ DOJ initiated prosecution.

Resolution:

Agency disciplinary or corrective action, if any:

OGE Form 202 (2/02)

Exhibit 7-3, Whistleblower/Retaliation Investigative Policies



DHS OIG WHISTLEBLOWER POLICY

Table of Contents

Preface

In the course of public service, situations give rise to potential gross fraud or waste, violations of law, or danger to public health or safety. When management fails to address these serious issues, Congress and the public encourage a whistleblower to step forward and receive protection from retaliation. In accordance with that mandate, the U.S. Department of Homeland Security (DHS), Office of Inspector General (OIG) adopted the following *DHS OIG Whistleblower Policy*.

I. Whistleblower

A. Definition

As defined by 5 CFR §1209.4, Whistleblowing is the disclosure of information by an employee, former employee, or applicant that the individual reasonably believes evidences a violation of law, rule, or regulation, gross mismanagement, gross waste of funds, abuse of authority, or substantial and specific danger to public health or safety. It does not include a disclosure that is specifically prohibited by law or required by Executive order to be kept secret in the interest of national defense or foreign affairs, unless such information is disclosed to the Special Counsel, the Inspector General of an agency, or an employee designated by the head of the agency to receive it.

B. Policy and Procedure

The Inspector General Act of 1978, with amendments, §7(a) states that the Inspector General may receive and investigate complaints or information from an employee of the establishment concerning the possible existence of an activity constituting a violation of law, rules, or regulations, or mismanagement, gross waste of funds, abuse of authority or a substantial and specific danger to the public health and safety.

C. Intake

DHS OIG receives complaints by phone, fax, mail or e-mail. The information is memorialized and assigned a record number in our case management database, Enforcement Data System (EDS). Each complaint is reviewed by an experienced DHS OIG investigator who makes whatever consultations or inquiries regarding the matter are necessary for a determination.

D. Legal Review

If the complainant claims to be a whistleblower and the experienced investigator finds a basis for the claim, the investigator will contact the U.S. Office of Special Counsel (OSC). The investigator will provide pertinent details of the claim to OSC and request a determination of whistleblower status.

If the experienced investigator finds no basis for a claim of whistleblowing but the complainant persists, the complainant will be advised to contact the OSC Disclosure Unit directly.

E. Confidentiality

The Inspector General Act of 1978, with amendments, §7(b) states that the Inspector General shall not, after receipt of a complaint or information from an employee, disclose the identity of the employee without the consent of the employee, unless the Inspector General determines such disclosure is unavoidable during the course of the investigation.

DHS OIG must obtain permission from the whistleblower in order to disclose the whistleblower's identity. If the whistleblower cannot be reached to obtain permission or the whistleblower denies permission to disclose, the complaint cannot be referred. Any DHS OIG investigative activity that might disclose the whistleblower's identity is prohibited. If the complaint cannot be referred or investigated based upon a lack of permission to disclose the whistleblower's identity, the complaint must be administratively closed to the file in order to protect the whistleblower's confidentiality.

II. Retaliation

A. Definition

Retaliation is the term that describes an adverse personnel action taken against a whistleblower as punishment for a disclosure. In order for retaliation to occur, the manager taking or directing the personnel action must be aware that the employee made the disclosure, and there must be clear and convincing evidence that the disclosure was a contributing factor to the decision to take the personnel action.

As defined by 5 CFR §1209.4, "personnel action" means, as to individuals and agencies covered by 5 U.S.C. 2302:

(1) An appointment;
(2) A promotion;
(3) An adverse action under chapter 75 of title 5, United States Code or other disciplinary or corrective action;
(4) A detail, transfer, or reassignment;
(5) A reinstatement;
(6) A restoration;
(7) A reemployment;
(8) A performance evaluation under chapter 43 of title 5, United States Code;
(9) A decision concerning pay, benefits, or awards, or concerning education or training if the education or training may reasonably be expected to lead to an appointment, promotion, performance evaluation, or other personnel action;

(10) A decision to order psychiatric testing or examination; or
(11) Any other significant change in duties, responsibilities, or working conditions.

A "contributing factor" means any disclosure that affects an agency's decision to threaten, propose, take, or not take a personnel action with respect to the individual making the disclosure.

"Clear and convincing evidence" is that measure or degree of proof that produces in the mind of the trier of fact a firm belief as to the allegations sought to be established. It is a higher standard than "preponderance of the evidence" as defined in 5 CFR 1201.56(c)(2).

B. Policy and Procedure

The Inspector General Act of 1978, with amendments, §7(c) states that any employee who has authority to take, direct others to take, recommend, or approve any personnel action, shall not, with respect to such authority, take or threaten to take any action against any employee as a reprisal for making a complaint or disclosing information to an Inspector General, unless the complaint was made or the information disclosed with the knowledge that it was false or with willful disregard for its truth or falsity.

C. Intake

DHS OIG receives complaints by phone, fax, mail or e-mail. The information is memorialized and assigned a record number in our case management database, Enforcement Data System (EDS). Each complaint is reviewed by an experienced DHS OIG investigator who makes whatever consultations or inquiries regarding the matter are necessary for a determination.

D. Legal Review

If the complainant claims to be the victim of retaliation and the experienced investigator finds a basis for the claim, or the experienced investigator finds credible evidence of retaliation in an ordinary complaint, the investigator will contact the U.S. Office of Special Counsel. The investigator will provide pertinent details of the complaint to OSC and request a determination of retaliation. Note, if the complainant is a uniformed member of the United States Coast Guard (USCG), then see Section III B of this policy for additional provisions.

If the experienced investigator finds no basis for a claim of retaliation and the complainant persists, the complainant will be advised to contact the OSC Disclosure Unit. Note, if the complainant is a uniformed member of the USCG, then the complainant will be advised to contact the Board for Correction of Military Records of the Coast Guard (BCMR).

III. Associated Organizations and Laws

A. U. S. Office of Special Counsel

The U.S. Office of Special Counsel is an independent federal investigative and prosecutorial agency. Their basic authorities come from the Civil Service Reform Act and the Whistleblower Protection Act. OSC's primary mission is to safeguard the merit system by protecting federal employees and applicants from prohibited personnel practices (PPPs), especially reprisal for whistleblowing. OSC receives, investigates, and prosecutes allegations of PPPs, with an emphasis on protecting federal government whistleblowers. OSC seeks corrective action remedies such as back pay and reinstatement, either by negotiation or from the Merit Systems Protection Board (MSPB), for injuries suffered by whistleblowers and other complainants. OSC is also authorized to file complaints at the MSPB to seek disciplinary action against individuals who commit PPPs. OSC provides a secure channel through its Disclosure Unit for federal workers to disclose information about various workplace improprieties, including a violation of law, rule or regulation, gross mismanagement and waste of funds, abuse of authority, or a substantial danger to public health or safety.

Title 5 U.S.C. §1213 gives OSC the power to compel the agency head to conduct an investigation and submit a written report setting forth the findings within 60 days after the date on which the information was transmitted, or within any longer period of time agreed to in writing by the Special Counsel. For DHS OIG, the agency head is the Secretary of DHS. OSC may request investigative assistance from DHS OIG. DHS OIG may provide limited assistance to OSC that conforms to our legal obligations and investigative resources.

B. Board for Correction of Military Records of the U.S. Coast Guard

The Board for Correction of Military Records (BCMR) of the Coast Guard is a board of civilians within DHS which has authority under Title 10 U.S.C. §1552 to review and correct the personnel records of current and former members of the U.S. Coast Guard and U.S. Coast Guard Reserve. Such records include, but are not limited to, records regarding discharges, reenlistment codes, disciplinary matters, performance evaluations, selection for promotion, advancement, retirement, dates of service, disability ratings, medals, and various bonuses and benefits.

33 CFR §53.9 lists the responsibilities of DHS OIG to uniformed members of the USCG who allege retaliation. It states that DHS OIG shall expeditiously investigate any allegation, if such allegation is submitted, that a personnel action has been taken (or threatened) in reprisal for making or preparing to make a lawful communication to a Member of Congress or an Inspector General concerning a complaint or disclosure of information that the member reasonably believes constitutes evidence of a violation of law or regulation, mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety. No investigation is required

when such allegation is submitted more than 60 days after the Coast Guard member became aware of the personnel action that is the subject of the allegation.

DHS OIG must initiate a separate investigation of the information the Coast Guard member believes evidences wrongdoing if such investigation has not already been initiated. The Inspector General is not required to make such an investigation if the information that the Coast Guard member believes evidences wrongdoing relates to actions that took place during combat.

DHS OIG must complete the investigation of the allegation of reprisal and issue a report not later than 90 days after receipt of the allegation, which shall include a thorough review of the facts and circumstances relevant to the allegation, the relevant documents acquired during the investigation, and summaries of interviews conducted. The Inspector General may forward a recommendation as to the disposition of the complaint.

DHS OIG must submit a copy of the investigation report to the Secretary of Homeland Security and to the Coast Guard member making the allegation not later than 30 days after the completion of the investigation. The copy of the report issued to the Coast Guard member may exclude any information not otherwise available to the Coast Guard member under the Freedom of Information Act (5 U.S.C. §552).

If a determination is made that the report cannot be issued within 90 days of receipt of the allegation, DHS OIG must notify the Secretary and the Coast Guard member making the allegation of the reasons why the report will not be submitted within that time, and state when the report will be submitted.

At the request of the BCMR, DHS OIG must submit a copy of the investigative report to the BCMR. After the final action with respect to an allegation filed under this part, whenever possible, DHS OIG should interview the complainant to determine the views of that person concerning the disposition of the matter.

C. Whistleblower Protection Act of 1989

In 1989 the Whistleblower Protection Act, known as the WPA (P.L. 101-12, 103 Stat. 16), strengthened the protections provided in the Civil Service Reform Act of 1978. This piece of legislation protected federal employees who disclosed information on government misconduct and waste.

When Congress first enacted the WPA, it stated that the intent of the legislation was to: strengthen and improve protection for the rights of Federal employees, to prevent reprisals, and to help eliminate wrongdoing within the Government by — (1) mandating that employees should not suffer adverse consequences as a result of prohibited personnel practices; and (2) establishing ... that while disciplining those who commit prohibited personnel practices may be used as a means by which to help accomplish that goal, the protection of individuals who are the subject of prohibited personnel practices remains the paramount consideration.

The WPA further explained that the Inspector General (IG) of an agency or another employee designated by the head of the agency should receive such disclosures of information which the employee or applicant reasonably believes evidences — (i) a violation of any law, rule, or regulation, or (ii) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.

It is the IG's responsibility to make this information public to their employees. Moreover, 'any disclosure' made to the Special Counsel or to the Inspector General of an agency or another employee designated by the head of the agency to receive such disclosures, which the employee 'reasonably believes' evidences 'a violation of any law, rule, or regulation,' or evidences 'gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety' is also protected. Agency heads are required to inform their employees of these protections.

D. Intelligence Community Whistleblower Protection Act of 1998

Years ago, government employees in the Intelligence Community (IC) did not enjoy the protections of the WPA because of the need to safeguard sensitive or classified information. IC employees had the choice of asking their agency head for permission to bring an allegation to a Congressional Intelligence Committee, or they could decide to bring the allegation to the Committee on their own. Congress found that IC employees usually failed to exercise either option because of the fear of retaliation. To correct this problem, Congress gave IC employees a third option - that of bringing a whistleblower complaint to the Inspector General - with the passage of the Intelligence Community Whistleblower Protection Act of 1998 (ICWPA).

DHS has employees that are considered part of the Intelligence Community. The USCG and CBP have intelligence units, and the DHS Office of Intelligence and Analysis has IC employees. For ease of reference, the U.S. Office of Personnel Management classification for an Intelligence Analyst position is GS-0132.

The ICWPA modified §8H of the Inspector General Act of 1978 to include the new protection. Any other employee of, or contractor to, an executive agency, or element or unit thereof, determined by the President under section 2302(a)(2)(C)(ii) of title 5, United States Code, to have as its principal function the conduct of foreign intelligence or counterintelligence activities, who intends to report to Congress a complaint or information with respect to an urgent concern may report the complaint or information to the appropriate Inspector General (or designee) under this Act [5 USCS Appx. §§ 1 et seq.] or section 17 of the Central Intelligence Agency Act of 1949 [50 USCS § 403q].

If a designee of an Inspector General under this section receives a complaint or information of an employee with respect to an urgent concern, that designee shall report the complaint or information to the Inspector General within 7 calendar days of receipt.

Not later than the end of the 14-calendar day period beginning on the date of receipt of the employee complaint, the Inspector General shall determine whether the complaint or information appears credible. Upon making such a determination, the Inspector General shall transmit to the head of the establishment notice of that determination, together with the complaint or information.

Upon receipt of a transmittal from the Inspector General, the head of the establishment shall, within 7 calendar days of such receipt, forward such transmittal to the intelligence committees, together with any comments the head of the establishment considers appropriate.

If the Inspector General does not find the complaint credible or does not transmit the complaint or information to the head of the establishment in accurate form, the employee (subject to all other applicable laws) may submit the complaint or information to Congress by contacting either or both of the intelligence committees directly.

The employee may contact the intelligence committees directly only if the employee, before making such a contact, furnishes to the head of the establishment, through the Inspector General, a statement of the employee's complaint or information and notice of the employee's intent to contact the intelligence committees directly; and obtains and follows from the head of the establishment, through the Inspector General, direction on how to contact the intelligence committees in accordance with appropriate security practices.

A member or employee of one of the intelligence committees who receives a complaint or information does so in that member or employee's official capacity as a member or employee of that committee. The Inspector General shall notify an employee who reports a complaint or information under this section of each action taken under this section with respect to the complaint or information. Such notice shall be provided not later than 3 days after any such action is taken.

An action taken by the head of an establishment or an Inspector General under the subsections above shall not be subject to judicial review.

In this section, the term "urgent concern" means any of the following:

- A serious or flagrant problem, abuse, violation of law or Executive order, or deficiency relating to the funding, administration, or operations of an intelligence activity involving classified information, but does not include differences of opinions concerning public policy matters.
- A false statement to Congress, or a willful withholding from Congress, on an issue of material fact relating to the funding, administration, or operation of an intelligence activity.
- An action, including a personnel action described in section 2302(a)(2)(A) of title 5, United States Code, constituting reprisal or threat of reprisal prohibited under section 7(c) [5 USCS Appx. § 7(c)] in response to an employee's reporting an urgent concern in accordance with this section.

The term "intelligence committees" means the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate.

E. Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002

The Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (NO FEAR Act) states that Federal agencies be held accountable for violations of antidiscrimination and whistleblower protection laws; to require that each Federal agency post quarterly on its public website, certain statistical data relating to Federal sector Equal Employment Opportunity (EEO) complaints filed with such agency; and for other purposes.

The Department of Homeland Security follows the NO FEAR Act by publishing a link that clarifies the whistleblower protection laws. Individuals also have access to the EEO complaint statistics for each DHS agency. DHS puts forth an annual report to congress outlining the Whistleblower cases so that it is accessible to the public. DHS training offices ensure that employees receive required initial and recertification training in the NO FEAR Act.

F. American Recovery and Reinvestment Act of 2009

In the wake of an economic downturn, Congress passed the American Recovery and Reinvestment Act of 2009 (ARRA) allocating funds and establishing temporary tax incentives designed to help the economy. Included in the bill were unprecedented provisions for accountability and transparency, summarized by ARRA Subtitle and Section below. Interestingly, the law expands DHS OIG responsibility to include whistleblower retaliation against state or local employees or contractors using ARRA funds obtained through DHS.

Subtitle A – Transparency and Oversight Requirements

§ 1514

* Review all complaints from the public regarding investment of funds.
* Complaints that do not become criminal investigations must be relayed immediately to the head of the department or agency concerned.
* "Findings" of the reviews shall be posted on the DHS OIG website and linked to the Recovery Accountability and Transparency Board website. Findings may be redacted pursuant to FOIA and Privacy Act provisions.

§ 1515

* OIG is granted full access to contractor and subcontractor files and records that pertain to the funds used under ARRA.

* OIG is granted full access to interview any contractor and subcontractor employee or officer regarding funds used under ARRA.

Subtitle B – Recovery Accountability and Transparency Board

§ 1521
* Board is established – DHS OIG is one of the members of the Board.

§ 1523
* (a)(2)(C) Board will refer matters to OIG's for investigation.

§ 1527
* (a) OIG's retain full independent authority to decide whether to conduct an investigation or not.
* (b) If the Board requests DHS OIG to conduct or quash an investigation and DHS OIG rejects the request in whole or in part, DHS OIG must prepare a "report" stating the reasons for the decision. The report must be sent to the Board, the head of the applicable agency, and congressional committees of jurisdiction, including both House and Senate Committees on Appropriations.

Subtitle D – Additional Accountability and Transparency Requirements

§ 1553 Whistleblower reprisal complainants

* (b)(1) State/local government employees and contractor/subcontractor whistleblowers who feel subject to reprisal must report the complaint to the OIG.

* OIG may reject the whistleblower reprisal complaint if:
  1) it is determined to be frivolous,
  2) it does not relate to ARRA funds, or
  3) another federal or state judicial or administrative proceeding was previously invoked to resolve the complaint.

* If no exception (1, 2 or 3 above) applies, DHS OIG "shall" investigate the whistleblower reprisal complaint. The DHS OIG final report must be given to:
  1) whistleblower complainant,
  2) employer of the whistleblower complainant,
  3) the head of the appropriate agency, and
  4) the Board.

Whistleblower reprisal complaint deadlines and time limits

* (b)(2) DHS OIG has 180 days from receipt of a whistleblower reprisal complaint to either reject it or submit the final report.

* DHS OIG may extend the 180 day deadline one of two ways:

1) by agreement with the complainant whistleblower, or
2) the IG may decide unilaterally to extend the deadline up to another 180 days. The IG must provide the complainant and the complainant's non-federal employer with a written explanation for the extension.

* DHS OIG must list all ongoing extensions in each Semi-Annual Report to Congress.

* (b)(3)(A) DHS OIG may decide not to conduct or continue a whistleblower reprisal complaint. DHS OIG must provide the complainant and the complainant's non-federal employer with a written explanation of the decision.
* (b)(3)(C) DHS OIG must list all decisions not to conduct or continue an investigation in each Semi-Annual Report to Congress.

Whistleblower complainant access to our investigative files

* (b)(4)(A) The whistleblower complainant will have access to the DHS OIG investigative file under all applicable provisions of the Privacy Act. If the whistleblower complainant files an appeal to an agency head or a court of competent jurisdiction, the DHS OIG file will be considered "Closed" for Privacy Act purposes (the normal "Open Case" exemption will not apply).

* (b)(4)(B) If the whistleblower complainant files suit against the non-federal employer under certain special provisions ((c)(3)), the whistleblower complainant and the non-federal employer will have access to the DHS OIG investigative file under all applicable provisions of the Privacy Act

* (b)(4)(C) List of information the OIG may exclude from disclosure above (Note: list mirrors some of the exceptions listed under the Privacy Act):
    1) information protected by a provision of law, or
    2) any information that would impede an ongoing investigation, but that information must be released as soon as it no longer impedes the investigation. If the IG determines that the information discloses a law enforcement technique, procedure or information that would assist criminals in evading the law or the identity of a confidential source, the information does not have to be disclosed.

Whistleblower complainant confidentiality

* (b)(5) While DHS OIG is conducting an Open whistleblower complaint investigation, DHS OIG may not respond to any inquiry or disclose any information about the complainant except as provided by law.

8.0 CASE AND ADMINISTRATIVE FILE MANAGEMENT

8.1 CASE NUMBERING SYSTEM

The OIG uses an alpha-numeric system to designate cases. Case numbers are automatically generated by EDS upon submission of a complaint documentation form. The case number consists of the following elements:

Field one: Letter designation for Complaints (C), Investigations (I), Referral (R), Management Implication Report (M), and Administratively Closed (Z).

Field two: Two-digit number reflecting the fiscal year e.g. 03.

Field three: Three to seven character acronym to identify the DHS component e.g. TSA, FLETC.

Field four: Three character alpha designation for the DHS OIG investigating office e.g. SFO (San Francisco). (Chapter 2.11)

Field five: Five digit sequential number assigning the identity to the case number.

Field six: One alpha character available if necessary to designate "Special Handling" cases, e.g. "S" (Chapter 7.3).

For example I08 CIS PHL 28871 would designate an investigation opened in 2008 involving CIS employee or programs. The investigation is assigned to the Philadelphia Office and has the sequential numerical designation of 28871.

8.2 CASE FILE ORGANIZATION

Official case files containing original documents will be maintained at the respective office to which the investigation is assigned. The case file and working file should be established immediately upon the opening and assignment of an investigation. Original MOAs will be added to the official case file within ten (10) business days of signature, or in rare circumstances as soon as practicable.

Documents contained in the official case file will be filed chronologically using a six-part file annotated on the outside with the case number. Work will be filed on each side (side one being the inside of the front cover and side six being the inside of the back cover) as follows:

1. Copy of EDS generated complaint form; all records/data searches regarding subject(s), including, photographs, fingerprint cards and FBI Form R-84s.

2. Judicial Documents – Subpoenas and subpoena requests; Court Documents; Copies of Search and Arrest Warrants; Declination Letters; 6(e) letters; Grand Jury material and Consensual monitoring requests.

3. Evidence Inventory Forms; Transcripts of Consensual Monitoring.

4. General Correspondence; Electronic Mail (E-mail) messages; FBI Case Opening Notification Letters; and any Media related material.

5. Case Closing Checklist; Initial Referral Documents; Investigative Plans; Tactical Plans; Expenditure Forms, and case reviews.

6. Index Sheet; Transmittal Memo; ROI; AROI; MIR; Case Report; MOAs with attachments; Collateral Requests; and Agent Notes/Chronology Log.

After the case is closed, the case agent will consolidate their working file into the official case file. All case related E-mail should be printed and retained in the case file. The case agent is responsible for ensuring that the official case file is complete and does not contain duplicate documents and records. Agent notes will be maintained in a manila envelope.

8.3 REQUESTING & REPORTING COLLATERAL INVESTIGATIONS

Requesting

A request for investigative support will be made by a written memorandum or electronic message from the requesting SAC to the receiving office SAC. This request will contain the following information:

The case number and title.
A brief summary of the allegation(s) and relevant issues.
The specific investigative activity requested.
Available background information on individuals relevant to the request, and
Any other factors, including time restrictions.

Reporting

Collateral investigations should be treated as a priority and should be initiated within five days of receipt.

All investigative activity will be documented using an MOA.

Upon completion of the collateral investigative activity, the reporting office will forward a cover memorandum containing a synopsis of the investigative activity and all original documents including agent notes to the requesting office.

EDS Collateral Entries

The reporting office will be responsible for entering the request for a collateral investigation into EDS. Upon completion of the collateral investigation the reporting office will be responsible for closing of the collateral in EDS.

8.4 CASE REVIEWS

A case review is a regularly scheduled evaluation and discussion of the investigative status/progress of all pending cases between a first-line supervisor and the agent to whom such cases are assigned. Such reviews will be conducted quarterly or more frequently at the discretion of the SAC.

Case reviews will be documented on the Case Progress Worksheet (INV Form 6A) and maintained in the case file and uploaded to EDS. **(Exhibit 8-1)**

8.5 CASE CLOSING CHECKLIST

As the final step in every investigation, the assigned SA will review the official case file and complete an INV Form-14, "Case Closing Checklist." **(Exhibit 8-2)**

8.6 INTERVIEW NOTES

During the “discovery” phase of court proceedings, an SA’s notes may be made available to the defense. Therefore, all notes will be maintained and made part of the case file. Interview notes will include the name of interviewee, the date and location of the interview, and who was present.

8.7 INVESTIGATION RELATED EMAILS

Although email is a valuable tool that can make communication faster and more efficient, it may have significant, possibly adverse, consequences if not used thoughtfully. The use of email to communicate substantive case-related information in criminal and parallel criminal/civil cases may trigger the disclosure of this information under the Jencks Act, Federal Rules of Criminal Procedure Rules 16 and 26.2, Brady/Giglio and the Federal Records Act. The inclusion of emails in the case file will be governed by the policy and procedures established by the U.S. Department of Justice. **(Exhibit 8-3)**

There are three general categories within which most case related emails fall:

1. potentially privileged communications
2. substantive communications
3. purely logistical communications

According to the Federal Records Act, 44 USC 3301, and 36 CFR 1234.2, all emails falling within the definition of categories 1 and 2 above must be printed and maintained in the case file.
SA's should consult with the USAO to determine if the emails contain discoverable information.

8.8 EDS CASE DATA ENTRY

Prior to entering a new complaint or investigation, a name check for the subject and complainant must be conducted in EDS.

Complaints

All allegations involving DHS programs, employees, or operations, however received, will be entered into the EDS by the Hotline staff. Complaint information should document the allegation in a clear and concise manner consisting of not more than 500 characters. The complainant's name should be entered in the designated field, but not elsewhere in any narrative.

Investigations

The investigating office is responsible for entering all reportable information (subjects, witnesses, complainants, victims, judicial/civil/administrative action, dispositions) pertaining to investigations into the EDS as soon as possible.

The Comment field can be used to document significant case contacts or developments for part of a permanent case record.

The Narrative field should reflect the initial allegation.

Signed MOAs and ROIs with exhibits will be uploaded into EDS within ten (10) business days of signature, or in rare circumstances as soon as practicable.

Semi Annual Report (SAR) Data

Investigations can be identified for inclusion into the SAR by checking a designated box in EDS. A case summary can then be prepared by the case agent in the designated SAR field. The case agent should ensure that the case summary is prepared in the proper SAR format, so that this information can be "imported" directly into the SAR with few, if any, revisions. Appropriate redactions will be performed by the assigned SAR preparation team.

Transmittal of Reports

INV staff is responsible for entering into EDS the date that reports (ROI, AROI, MIR) were forwarded to a DHS component agency.

8.9 OIG/FBI MUTUAL NOTIFICATION REQUIREMENT

Pursuant to section 4(d) of the Inspector General Act of 1978, as amended, there must be expeditious reporting to the Attorney General (AG) whenever the DHS OIG has reasonable grounds to believe there has been a violation of federal criminal law. (Chapter 2.5)

As the primary investigative arm of DOJ, the FBI has jurisdiction in all matters involving fraud against the federal government, and shares jurisdiction with the OIG in the investigation of fraud against the DHS. In such areas of concurrent jurisdiction, the OIG and the FBI agree to promptly notify each other upon the initiation of any criminal investigation, unless the FBI SAC and the OIG SAC have made other arrangements that preclude the need for notification in certain categories of cases or in certain situations.

Absent exigent circumstances, "promptly" shall be considered to be within 30 calendar days. Notification by the OIG will be in writing and addressed to the FBI in the district in which the investigation is being conducted. Notification shall include, when available, (a) subject name, date of birth, social security number, and (b) any other case identifying information including (i) the date the case was opened or the allegation was received, and (ii) the allegation which predicated the case, INV Form 95, FBI Notification Letter. **(Exhibit 8-4)** For investigations where allegations arise which are beyond the scope of the OIG's jurisdiction, the OIG will immediately notify the appropriate investigative agency. Notification by the FBI shall be in writing and shall be addressed to the appropriate regional office of the Office of Inspector General.

In criminal investigations a federal prosecutor must be consulted at an early stage to ensure that the allegations, if proven, would be prosecuted. Such consultation will also ensure coordination of investigative methods.

8.10 CLAIMS FOR STATISTICAL ACHIEVEMENTS

DHS OIG case agents will only claim credit for achievements in those cases in which DHS OIG had the lead or played an active and substantive role in the investigation associated with the reported achievement. No credit should be taken in any case in which the DHS OIG did not make substantive investigative contributions or the DHS OIG's role could reasonably be construed as that of a mere conduit through which information was passed. The case agent, or lead case agent, in the primary investigative office will claim the statistical credit for the DHS OIG's work on the case. If DHS OIG worked the investigation jointly with another OIG, or another OIG assisted on the investigation, the other OIG should be identified in EDS.

Achievements can be generally classified as; monetary, criminal, civil, administrative, or program savings. Statistics can be claimed and posted to EDS by the effected office upon conclusion of the criminal, civil, and/or administrative action. DHS OIG agents should not claim statistical credit for any achievement or outcome unless they are able to upload

the associated supporting documents, preferably official court documents for criminal and civil matters, into EDS. These uploaded supporting documents will be individually reviewed and audited during the SAR preparation process. If the case agent does not have fully auditable supporting documents, the statistical achievement will not be claimed.

Monetary achievements may result from criminal, civil, and/or administrative actions, and may be claimed on both DHS and non-DHS program related cases.

Criminal, civil and/or administrative action may be imposed against DHS employees as a result of investigations concerning employee misconduct.

Program savings may be claimed only after the DHS has taken administrative action to suspend or terminate improper payments. Program savings will not be claimed in cases that result only in the suspension or termination of DHS employees.

8.11 CIGIE ANNUAL REPORT

Each fiscal year the Council of the Inspectors General on Integrity and Efficiency (CIGIE) prepare an annual report to the President that delineates investigative statistics based upon the following data that is retrieved from EDS:

Successful Criminal Prosecutions - Convictions or pre-trial diversions in federal, local, state or foreign government venues, or under the Uniform Code of Military Justice (UCMJ), any of which result from a case in which an OIG has an active investigative role.

Successful Civil Actions - Civil judgments, or forfeitures in favor of the U.S. government filed in federal, local, state or foreign government venues; or settlements negotiated by a prosecuting authority prior to or following the filing of a formal civil complaint; or judgments, settlements or agreements reached based on the Procurement Fraud Civil Remedies Act (PFCRA), Civil Monetary Penalties (CMP) or other agency specific civil litigation authority; any of which result from a case in which an OIG has an active investigative role.

Personnel Actions - Reprimands, suspensions, demotions, or terminations of federal (including federal contractor/grantee), state, local, and foreign government employees, any of which result from a case in which an OIG has an active investigative role.

Suspensions/Debarments - Agency actions which suspend, restrict or prohibit vendors/contractors, grantees or other non-governmental persons or entities, from doing business with the federal government, any of which result from a case in which an OIG has an active investigative role.

Investigative Recoveries - A) *Criminal case*s - the amount of restitution, criminal fines, or special assessments resulting from a criminal judgment or established through a pre-

trial diversion agreement; B) *Civil cases* - the amount of damages, penalties or forfeitures resulting from judgments issued by any court (federal, local, state, military or foreign government) in favor of the U.S. government; or the amount of funds to be repaid to the U.S. government based on any negotiated settlements by a prosecuting authority; or the amount of any assessments or penalties imposed based on PFCRA, CMP or other agency specific civil litigation authority; C) *Voluntary repayments* - the amount of funds voluntarily repaid based on an OIG investigation before prosecutorial action is taken; any of which result from a case in which an OIG has an active investigative role.

Criminal Indictments/Informations - Criminal indictments or Information filed in a federal, local, state or foreign government court or under the Uniform Code of Military Justice, any of which result from a case in which an OIG has an active investigative role.

8.12 INTERNAL TRANSFER OF OIG INVESTIGATIONS

The SAC of the originating office will forward a memorandum to the SAC of the receiving office outlining the reason for the transfer. The official case file will be sent to the receiving office via a trackable shipper (e.g. FedEx). The Hotline staff must be notified in order to make the appropriate changes in EDS.

8.13 ADMINISTRATIVE FILES

Each field office will establish an administrative file system to store general information relating to policies, procedures, and correspondence to and from the OIG. The administrative file system will follow the "Administrative Files List." **(Exhibit 8-5)**

8.14 SAFEGUARDING GRAND JURY INFORMATION

Agents who are working with grand jury materials are responsible for ensuring their confidentiality. No agent handling grand jury materials may disclose the material or their contents to any third party unless he or she is certain that the disclosure meets the applicable legal standards set forth in Rule 6(e) of the Federal Rules of Criminal Procedure. (Chapter 17.1)

The official case file will be marked on the outside "Contains Grand Jury Material," and the file will be moved to the limited access storage file accessible only to authorized personnel.

8.15 STORAGE OR DISPOSAL OF ADMINISTRATIVE AND INVESTIGATIVE FILES

All investigative case files (open and closed) will be maintained in the SAC field office. Overseas offices such as the San Juan RAC office is exempted from this policy and will maintain investigative case files locally.

Investigative files will be disposed of according to the OIG Records Control Schedule. **(Exhibit 8-6)** The schedule has two categories for investigative case files:

- **Category 1: Temporary** which are retained for 20 years.
- **Category 2: Permanent** which are significant case files that can never be destroyed. The Records Control Schedule establishes the following criteria for determining Permanent cases. These are cases that:

  (1) involve substantive information relating to national security;
  (2) involve allegations made against senior DHS officials;
  (3) attract national media or Congressional attention;
  (4) result in substantive changes in DHS policies or procedures.

The respective SAC will determine the appropriate records retention classification for each investigation when the case is closed by applying the criteria listed above.

When closed investigative case files become inactive and are no longer needed for current OIG business, they will be transferred to the Federal Records Center (FRC) for temporary off-site storage until their eligible disposal (i.e. destruction or transfer to the National Archives for permanent retention). Investigative case files will be transferred according to the procedures provided in **Exhibit 8-7**. **IMPORTANT: Grand Jury material should not be stored at the FRC**. **Disposition of any Grand Jury material should be coordinated with the United States Attorney's Office.**

Administrative files such as time and attendance, travel, and procurement files will be retained according to the time frames established by the General Records Schedule (GRS), which is issued by the National Archives and Records Administration (NARA). The GRS is available on NARA's website at http://www.archives.gov/records-mgmt/ardor/.

Administrative files are usually kept in OIG office space until their eligible destruction date, rather than transferring them to the FRC. This is because the fees for off-site storage of administrative files are not cost effective.

8.16 SAFEGUARDING CLASSIFIED AND SENSITIVE INFORMATION

Classified Information: When unattended, classified materials will be stored in a GSA approved container or a room/area that has been specifically certified and approved for the open storage of classified materials. When classified materials are removed from a storage location, an appropriate cover sheet INV Form 10, "Classified Document Record of Transmittal," **(Exhibit 8-8),** will be affixed to the face of the documents to prevent the casual observation and inadvertent disclosure by an uncleared person or persons without a need-to-know.

When classified materials are transported within the confines of the building, they will have the appropriate cover sheet affixed to the face of the document and inserted into an

unmarked manila folder or envelope so as not to advertise the fact the folder/envelope contains classified materials.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

.

8.17 ALIEN FILES

DHS Citizenship and Immigration Services (CIS) maintains files on all aliens that have applied for benefits. These files are commonly referred to as "A" files. These files generally contain background information to include photographs, fingerprints, personal history information and other documents related to the alien's status. The OIG may obtain "A" files for investigative purposes. SACs are responsible for the proper handling and return of the files to CIS at the conclusion of the investigation, or when they are no longer required.

SACs will designate an 'A' file custodian to coordinate the receipt, storage and return of all 'A' files in the custody of the OIG. The custodian will maintain a log that includes the following information:

- 'A' file number
- Date of receipt
- Name of requestor
- Date of return
- Person to whom the file was returned

Information and documents contained within the 'A' file are potentially evidentiary in nature and should be treated as such.

CHAPTER 8.0 - EXHIBITS

Exhibit 8-1, INV Form 6A, Case Progress Worksheet

Department of Homeland Security
Office of Inspector General
Office of Investigation

Case Progress Worksheet

Date of Review: _____

Supervisor: _____ Case Agent: _____ Case Number: _____

Case Title: _____ Primary Case Category _____

Date Case Initiated: _____ # of Days Opened: _____ Date Range of Review: _____ to _____

DHS Employee Title: _____ DHS Employee Status: _____

TO BE COMPLETED BY THE CASE AGENT

Number of MOAs Approved Since Last Review: _____ Are All Approved Non-GJ MOAs Uploaded into EDS? ○ Yes ○ No

Number of Outstanding MOAs that are pending approval: _____ Outstanding MOA #'s that need uploading _____

Number of Investigative Activity Since Last Review: _____ Is the Investigative Plan Current? ○ Yes ○ NO

Date of Last Investigative Activity: _____

Summary of Current Status/ Investigative Activity to Date:

Anticipated Investigation Milestone(s):

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____

TO BE COMPLETED BY THE REVIEWING SUPERVISOR

Supervisor's Comments and Guidance on Progress and Future Activity:

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____

Supervisor's Signature: _____ Date: _____

DHS OIG FORM 6A Case Review OIG INV V1.2, March 22, 2013

Exhibit 8-2, INV Form 14, Case Closing Checklist

Office of Inspector General - Investigations
U.S. Department of Homeland Security

Homeland Security

CASE CLOSING CHECKLIST

General – ALL CASES

CASE NUMBER: ___I_____

Yes	N/A	
☐	☐	Complaint Document Form
☐	☐	ROI with Exhibits Case Opening Document Transmittal Memo Memorandum of Activity (MOAs)
☐	☐	Agent's Notes/Correspondence/Record Checks/Miscellaneous Reports/Written Statements/Advice of Rights Forms, etc.
☐	☐	FBI Case Notification Letter
☐	☐	Disposition of Evidence/Personal Property
☐	☐	Destruction or Other Disposition of Grand Jury Material
☐	☐	IDMS Indexing Completed
☐	☐	Declination Letter from USAO
☐	☐	Copies of Subpoenas – Other Miscellaneous Court Documents

JUDICIAL CASES ONLY

☐	☐	Copies of Warrants/Indictments
☐	☐	Fingerprints/Photos/Personal History of Offender
☐	☐	FBI Standard Form 84 (Report of Arrest Disposition)
☐	☐	FBI Rap Sheet

OTHER

☐	☐	Disposition of Confidential Informant
☐	☐	Victim/Witness Referrals/Report
☐	☐	Case Review Worksheet

Case Agent Signature and Date: _____

Special Agent in Charge Signature and Date: _____

INV FORM-14

Exhibit 8-3, DOJ Policy on Electronic Communications in Criminal Cases

U.S. Department of Justice

Office of the Deputy Attorney General

The Deputy Attorney General

Washington, D.C. 20530

March 30, 2011

MEMORANDUM FOR THE ASSOCIATE ATTORNEY GENERAL AND
THE ASSISTANT ATTORNEYS GENERAL FOR THE
CRIMINAL DIVISION
NATIONAL SECURITY DIVISION
CIVIL RIGHTS DIVISION
ANTITRUST DIVISION
ENVIRONMENTAL AND NATIONAL RESOURCES DIVISION
TAX DIVISION

DIRECTOR, FEDERAL BUREAU OF INVESTIGATION
ADMINISTRATOR, DRUG ENFORCEMENT ADMINISTRATION
DIRECTOR, UNITED STATES MARSHALS SERVICE
PRINCIPAL DEPUTY DIRECTOR, BUREAU OF ALCOHOL,
TOBACCO, FIREARMS AND EXPLOSIVES
DIRECTOR, BUREAU OF PRISONS

ALL UNITED STATES ATTORNEYS

FROM: James M. Cole
Deputy Attorney General

SUBJECT: Guidance on the Use, Preservation, and Disclosure of Electronic Communications in Federal Criminal Cases

This memorandum supplements the January 4, 2010 Guidance for Prosecutors Regarding Criminal Discovery issued by Deputy Attorney General David W. Ogden (Ogden Memo), particularly section I.B.5, Substantive Case-Related Communications, and is to be read in conjunction therewith.[1] The guidance contained herein is directed to all Department of Justice personnel and to all law enforcement personnel participating as members of a prosecution team.[2]

[1] For guidance concerning cases involving national security information, *see* Acting Deputy Attorney General Gary G. Grindler's September 29, 2010 memorandum, "Policy and Procedures Regarding the Government's Duty to Search for Discoverable Information in the Possession of the Intelligence Community or Military in Criminal Investigations."

[2] "Prosecution team" members include federal, state, and local law enforcement officers and other government officials participating in the investigation and prosecution of the criminal case against the defendant. USAM 9-5.001. The Ogden Memo provides additional guidance where state and local law enforcement has any involvement in a criminal case, stating:

I. Summary

This memorandum provides guidance for prosecution team members on the use and preservation of electronic communications ("e-communications"). The basic principles are simple. Prosecution team members should think about the content of any e-communication before sending it; use appropriate language; think about whether e-communication is appropriate to the circumstances, or whether an alternative form of communication is more appropriate; and determine in advance how to preserve potentially discoverable information.

II. The Relationship Between the Government's Legal Discovery Obligations, Department of Justice Discovery Policies, and This Guidance

The Government's discovery obligations in federal criminal cases are set forth in constitutional case law, particularly *Brady v. Maryland*, 373 U.S. 83 (1963), and *Giglio v. United States*, 405 U.S. 150 (1972); the Jencks Act (18 U.S.C. 3500); Federal Rules of Criminal Procedure 16 and 26.2; and applicable rules of professional conduct.

Specific Department of Justice disclosure policies entitled Disclosure of Exculpatory and Impeachment Information (*Brady* policy) and Potential Impeachment Information Concerning Law Enforcement Witnesses (*Giglio* policy) are set forth in the United States Attorneys' Manual (USAM) at Sections 9-5.001 and 9-5.100.

The purpose of this memorandum is to provide guidance to ensure that the Government meets its legal discovery obligations as applied to electronic communications.[1] As used in this guidance, the term "e-communications" includes emails, text messages, SMS (short message service), instant messages, voice mail, pin-to-pin communications, social networking sites, bulletin boards, blogs, and similar means of electronic communication. This memorandum also provides guidance on how e-communications should and should not be used during the investigation and prosecution of a federal criminal case. A failure to comply with the guidance

---

In such cases, prosecutors should consider (1) whether state or local agents are working on behalf of the prosecutor or are under the prosecutor's control; (2) the extent to which state and federal governments are part of a team, are participating in a joint investigation, or are sharing resources; and (3) whether the prosecutor has ready access to the evidence. Courts will generally evaluate the role of a state or local law enforcement agency on a case-by-case basis. Therefore, prosecutors should make sure they understand the law in their circuit and their office's practice regarding discovery in cases in which a state or local agency participated in the investigation or on a task force that conducted the investigation.

Prosecutors are encouraged to err on the side of inclusiveness when identifying the members of the prosecution team for discovery purposes. Carefully considered efforts to locate discoverable information are more likely to avoid lengthy litigation over *Brady* and *Giglio* issues and avoid surprises at trial.

[1] This memorandum is solely intended to provide guidance to law enforcement personnel in order to attain compliance with the government's criminal discovery obligations with regard to electronic communications. It does not create any right in any person or entity, and it is not enforceable in any criminal or civil case. *United States v. Caceres*, 440 U.S. 741 (1979).

contained in this memorandum may result in delay, expense, and other consequences prejudicial to a prosecution, but it does not necessarily mean that there has been or will be a violation of a disclosure obligation.

III. Guidance for Achieving Full Compliance with the Government's Legal Discovery Obligations Relating to Electronic Communications

A. Benefits and Risks of E-communications

E-communications offer substantial benefits, including speed, sharing, and efficiency.

E-communications also present substantial risks. Because e-communications frequently are prepared and sent quickly and without supervisory review, they may not be as complete or accurate as more formal reports and may reflect a familiar or jovial tone. In court, defense counsel may try to use e-communications containing material inconsistencies, omissions, errors, incomplete statements, or jokes to impeach the credibility of a witness. Additionally, there is a risk that defense counsel will use poorly drafted e-communications between agents, witnesses, and/or prosecutors in court to create the false impression that they contain relevant or contradictory factual information. These risks can be particularly problematic in criminal prosecutions because, depending upon their content, e-communications may be discoverable under federal law.

Thus, prosecution team members should exercise the same care in generating case-related e-communications that they exercise when drafting more formal reports. All prosecution team members need to understand the risks of e-communications, the need to comply with agency rules regarding documentation and record-keeping during an investigation, the importance of careful and professional communication, and the obligation to preserve and produce such communications when appropriate.

B. Categories of E-communications

Case-related e-communications generally fall into four categories:

Substantive communications. "Substantive communications" include:

- factual information about investigative activity;
- factual information obtained during interviews or interactions with witnesses (including victims), potential witnesses, experts, informants, or cooperators;
- factual discussions related to the merits of evidence;

- factual information or opinions relating to the credibility or bias of witnesses, informants and potential witnesses;[4] and
- other factual information that is potentially discoverable under *Brady*, *Giglio*, Rule 16, or Rule 26.2 (Jencks Act).

Substantive communications or the information within them may be discoverable.

Logistical communications. "Logistical communications" include e-communications that contain travel information; identify dates, times and locations of hearings or meetings; transmit reports; etc. Generally, logistical communications are not discoverable.

Privileged or protected communications. "Privileged communications" include attorney-client privileged communications, attorney work product communications, and deliberative process privileged communications.[5] "Protected communications" are those covered by F.R.Crim.P. 16(a)(2).[6] Generally, these communications are not discoverable so long as any discoverable facts contained in them are disclosed in other materials produced in discovery.

---

[4] For example, if a prosecutor or agent opines that an informant will make a "bad" witness because the informant has made prior inconsistent statements, the opinion itself is core work product that need not be disclosed to the defense, but the prior inconsistent statements should be disclosed if the informant testifies at trial. *See generally,* Discovery BlueBook § 6.12.5, *Opinion or Reputation Evidence Regarding Veracity.*

[5] Pursuant to applicable law, a privilege may apply to communications:

a. between prosecutors on matters that require supervisory approval or legal advice, *e.g.*, prosecution memoranda, *Touhy* approval requests, *Giglio* requests, wire tap applications and reviews, and case strategy discussions;

b. between prosecutors or agency counsel and other prosecuting office personnel, agents, or other agency personnel on case-related matters, including but not limited to organization, tasks that need to be accomplished, research, and analysis;

c. between prosecutors and agency counsel or agency personnel (including agents) on legal issues relating to criminal cases, including, but not limited to, *Giglio* and *Touhy* requests; and

d. from the prosecutor or agency counsel to an agent, other agency personnel, or prosecuting office personnel giving legal advice or requesting investigation of certain matters in anticipation of litigation (*e.g.*, "to-do" list).

If warranted, the sender of a privileged e-communication is encouraged to place a "privileged communication" warning on the communication to flag its privileged nature.

[6] *See, generally,* Discovery BlueBook 3.8, *Information Not Subject to Disclosure by the Government – Rule 16(a)(2).*

Mixed Communications. A communication that contains a mix of the categories above may be partially discoverable and may need careful review by a prosecutor or review by a court before a final determination is made as to whether it should be disclosed in discovery.[7]

C. Using E-communications

The following guidance applies at all phases of a criminal case including investigation, trial preparation, trial, and after trial:

1. Prosecution team members should discuss and make sure they understand the e-communications and discovery policies and guidance applicable to their case.

2. Prosecution team members should only write and send e-communications that they would feel comfortable being displayed to the jury in court or in the media.

3. Prosecution team members should be particularly cautious in any e-communications with potential witnesses who are not law enforcement personnel, taking care to avoid substantive e-communications. Of course, any potentially discoverable information should be preserved, regardless of whether the communication is written or oral.

4. Substantive e-communications among prosecution team members should be avoided except when, to meet operational needs, they are the most effective means of communication. Examples include where prosecution team members are in different countries or time zones, or where other operational imperatives require such e-communications. Prosecution team members should consider whether a formal report would be a better way of ensuring accurate communication, clarifying a matter, or preserving potentially discoverable information. Again, potentially discoverable information should be preserved, regardless of whether the communication is written or oral.

5. Prosecution team members may use e-communications for logistical communications, for example, to schedule meetings with witnesses, agents, prosecutors, or other members of the prosecution team, or to transmit a formal report. However, prosecution team members should avoid including any substantive information in such e-communications.

---

[7] For e-communications containing information to be produced in discovery, a prosecutor may make appropriate redactions, summarize the substance of an e-communication in a letter rather than disclosing the e-communication itself, seek a protective order, or take other safeguarding measures.

6. E-communications, like formal reports, should state facts accurately and completely; be professional in tone; and avoid witticism, careless commentary, opinion, or over-familiarity. E-communications should maintain and accurately reflect an arms-length relationship with potential witnesses who are not law enforcement personnel, including victims and informants.

7. Prosecution team members ordinarily should not include information in an e-communication that must be incorporated into a formal agency report, especially with regard to witness interviews or other communications containing a witness's or agent's factual recitations. If for some reason substantive case-related information must be contained in an e-communication, prosecution team members should ensure that the information is accurate and is included in any formal report required by agency policies. Material inconsistencies between an e-communication and a formal report, or omissions, errors, or incomplete statements in e-communications, may be impeachment information and may be used in cross-examination in court proceedings.

8. Prosecution team members should limit the subject matter of any e-communication to a single case at a time to make it easier to segregate e-communications by case.

9. Prosecution team members should inform individuals not on the prosecution team but otherwise involved in the case, including victims, witnesses, and outside experts, that e-communications are a written record that might be disclosed to the defendant and used for impeachment in court like any other written record.

10. Prosecution team members must comply with any applicable policies governing e-communications and should not use personally-owned electronic communication devices, personal email accounts, social networking sites, or similar accounts to transmit or post case-related information.

11. Prosecution team members should not post case-related or sensitive agency information on a non-agency website or social networking site. Information posted on publically accessible websites or social networking sites may be used to impeach the author.

12. Prosecution team members should send e-communications only to those individuals who have a need to know the information contained in the communication.

13. Prosecution team members should employ practices that will preserve any potentially discoverable information contained in e-communications. Preservation of e-communications in certain messaging formats (e.g., text, SMS, instant, PIN, etc.) may present unique challenges.[8] At present, the approaches to preserving potentially discoverable information in e-communications may include: incorporating any potentially discoverable information into a comprehensive report, capturing the message in some format that can be made available to the prosecutor, or preserving the e-communication itself. These approaches may evolve as technology changes and technical capabilities change.

14. The sender should notify recipients of any restrictions on forwarding e-communications that the sender wants observed.

D. Preservation of E-communications

There are three steps to proper handling of e-communications in criminal cases: preservation,[9] review, and disclosure. The number of e-communications preserved and reviewed likely will be greater than the number ultimately produced as discovery.

1. Who is responsible for preserving e-communications?

Each potentially discoverable e-communication should be preserved by each member of the prosecution team who is either (a) the creator/sender/forwarder of the e-communication, or (b) a primary addressee (*i.e.*, in the "To" line). If no member of the prosecution team is a sender or primary addressee of a substantive e-communication (*e.g.*, if an agent is cc'd on an email by a witness to a third party), then each member of the prosecution team who is a secondary addressee (*i.e.*, a "cc" or "bcc" recipient) should preserve the email. Although in some instances this practice will lead to preserving multiple copies of the same e-communication, it will ensure preservation.

2. When should e-communications be preserved?

To ensure that e-communications are properly preserved, prosecution team members should move and/or copy potentially discoverable e-communications, together with any potentially discoverable attachments and threads of related e-communications, from the user's e-

[8] Each component should provide guidance to affected employees on how to preserve the various messaging formats (text, SMS, IM, PIN, etc.), or any other e-communication that may contain potentially discoverable information. Where an e-communication containing potentially discoverable information cannot be preserved electronically or printed, the agency's inability to do so should be documented so that the preservation approach can be explained in court.

[9] This guidance is concerned only with the Government's criminal discovery obligations. It is not intended to address the requirements of the Federal Records Act, 44 U.S.C. §§ 3101 *et seq.*

communication account[10] to a secure permanent or semi-permanent storage location associated with the investigation and prosecution, or print and place them with the criminal case file as soon as possible but not later than 10 days after the e-communication is sent or received. Prosecution team members should ensure that such preservation occurs before the agency computer system automatically deletes the e-communication because of storage limitations or retention policies. Designated network locations that are not subject to automatic deletion may be a secure storage location for potentially discoverable e-communications.

3. Which e-communications should be preserved for later review?

During an investigation it is difficult to know which e-communications may be discoverable if the case is charged. Therefore, members of the prosecution team should err on the side of preservation when deciding which e-communications to preserve for review.

The following e-communications should be preserved for later review and possible disclosure to the defendant:

- Substantive e-communications created or received in the course of an investigation and prosecution.
- All e-communications sent to or received from potential witnesses who are not law enforcement personnel regardless of content.
- E-communications that contain both potentially privileged and unprivileged substantive information.

As discussed below in section II.E.2, agents and their supervisors should work with prosecutors to identify all e-communications that are particularly sensitive and deserve careful consideration before any determination is made to provide them to the defendant as discovery.

4. Which e-communications do not need to be preserved for later review?

Logistical communications between prosecution team members, *e.g.*, scheduling meetings or assigning tasks, generally do not need to be preserved and made available to the prosecutor for review because they are not discoverable unless something in their content suggests they should be disclosed under *Brady*, *Giglio*, Jencks or Rule 16.

[10] With respect to emails, this includes the user's inbox, sent items, and deleted items.

5. How should e-communications be preserved?

When possible, e-communications should be preserved in their native electronic format to enable efficient discovery review. Otherwise, they should be printed and preserved.[11] E-communications that cannot be printed should be preserved in some other fashion, *e.g.*, a narrative report. For email, creation of electronic folders into which pertinent emails can be easily moved is the recommended method for preservation in native format.

6. How do parallel civil or administrative investigations/proceedings affect which e-communications should be preserved in a criminal case?

The best practices for parallel criminal, civil, and administrative proceedings vary from case to case. Be aware that civil proceedings may have different or broader preservation requirements; therefore, the prosecution team should consult with the lawyers handling the parallel proceedings for guidance on preserving e-communications in the early stages of parallel proceedings.

E. Reviewing and Producing Discoverable E-communications to the Defendant

1. Responsibilities of the Prosecutor

It is the prosecutor's responsibility to oversee the gathering, review and production of discovery.[12] In determining what will be disclosed in discovery, the prosecutor should ensure that each e-communication is evaluated, taking into consideration, among other things, what facts are reported, the author, whether the author will be a witness, whether it is inconsistent with other e-communications or formal reports, and whether it reflects bias, contains impeachment information, or contains any information (regardless of credibility or admissibility) that appears inconsistent with any element of the offense or the Government's theory of the case.

If the e-communication contains any particularly sensitive information (as described below), then the prosecutor should consider whether to file a motion for a protective order, seek supervisory approval to delay disclosure (in accordance with USAM § 9-5.001), make appropriate redactions, summarize the substance of an e-communication in a letter rather than disclosing the e-communication itself, or take other safeguarding measures.

---

[11] Agencies may require some e-communications to be printed to paper to comply with the Federal Records Act. Notwithstanding paper copies, preserving e-communications in native electronic format still is appropriate, when feasible, to facilitate electronic review and to preserve metadata that, in rare circumstances, may be discoverable.

[12] When dealing with voluminous e-communications, the prosecution team should discuss and plan for a substantial lead time to gather and review the materials.

2. Responsibilities of the Prosecution Team

It is the responsibility of each member of the prosecution team to make available to the prosecutor all potentially discoverable e-communications so that the prosecutor can review them to determine what should be produced in discovery. The discovery obligation continues throughout the case. *See* Fed.R. Crim. P. 16(c).

Prosecution team members who submit potentially discoverable e-communications to the prosecutor should identify e-communications that deserve especially careful scrutiny by the prosecutor. For example, prosecution team members should identify e-communications the disclosure of which could:

- affect the safety of any person,
- reveal sensitive investigative techniques,
- compromise the integrity of another investigation, or
- reveal national security information.

Homeland Security

Office of Inspector General - Investigations
U.S. Department of Homeland Security

Special Agent in Charge
Federal Bureau of Investigation

Dear

This is to notify you that the Office of Inspector General (OIG), U.S. Department of Homeland Security, San Francisco Office of Investigation has opened a criminal investigation of the following:

Name:
Date of Birth:
Social Security Number:
Location:
OIG Case Number:
Date Opened/Received:

This investigation concerns allegations of violation of 18 USC

This notification is being made in accordance with a Memorandum of Understanding entered into between the Department of Justice, the FBI, and the Department of Homeland Security OIG.
No Further action is required on your part.

THIS INFORMATION IS CONSIDERED SENSITIVE AND ANY DISSEMINATION WILL NOT BE MADE WITHOUT THE PRIOR AUTHORITY OF THIS OFFICE.

Should you need any additional information, please feel free to contact Special Agent

Sincerely,

Special Agent in Charge
U.S. Department of Homeland Security
Office of Inspector General

INV FORM-95

Exhibit 8-5, Administrative Files List.

ADMINISTRATIVE FILE MANAGEMENT

1000 AUTHORITY AND ORGANIZATION - General

1100 Organizational Structure
1200 Policy and Procedure
1300 External Relations – Liaison
1400 Memoranda of Understanding

2000 PERSONNEL MANAGEMENT - General

2100 Employee Conduct
2200 Awards
2300 Outside Activities/Employment
2400 Equal Employment Opportunities
2500 Law Enforcement Availability Pay (LEAP)
2600 Liability Insurance
2700 Time and Attendance - General
2710 Bi-weekly Activity Reports
2720 Alternate Work Schedules
2800 Health and Safety – General
2810 Annual Physical Contract/Information
2820 Blood Borne Pathogens
2830 Job Related Injuries
2900 FTE

3000 TRAINING - General

3100 FLETC
3200 IGCIA
3300 Outside Training Vendors
3400 Training Projections
3500 Conferences

4000 FIREARMS - General

4100 Deputation
4200 Qualification Standards
4300 Accidental Discharge
4400 Ammunition
4500 Firearms Instructors
4600 Quarterly Requalification - General
4610 Range Information

4620 Scores

5000 INVESTIGATIONS - General

5100 INV Memos
5200 Interception of Communications
5300 Victim Witness Assistance Program
5400 Forensic Requests
5410 Polygraph
5420 Computer Forensics
5430 Other Forensics
5500 Information Databases
5510 NCIC
5520 TECS
5530 Other
5600 Annual Evidence Verification
5700 Confidential Funds - General
5710 Confidential Expenditures

6000 GENERAL LEGAL MATTERS

6100 FOIA Requests
6200 Privacy Act Requests
6300 Giglio/Henthorn
6400 Declination Letters

7000 ADMINISTRATIVE MANAGEMENT

7100 Budget
7200 Space Management
7210 Lease
7220 Contractors
7230 Office Security
7240 Parking
7250 COOP Plan & Emergency Management
7300 Shipping
7310 FedEx
7320 USPS
7400 Information Technology
7500 Records Management
7600 Commuter Subsidies
7700 Office Inventory and Official Property
7710 Reporting Lost, Stolen, or Damaged Official Property
7720 Equipment
7730 Service Contracts
7800 Government Purchase Card

7810 Supplies
7900 Travel
7910 Travel Allocations
7920 Travel Vouchers

8000 GENERAL CORRESPONDENCE

8100 Internal Correspondence
8110 INV
8120 Field Offices
8130 Other DHS OIG
8200 External Correspondence
8210 DHS Components
8220 Other Government (non Law Enforcement)
8230 Other Law Enforcement
8240 FBI Notification Letter
8250 USAO
8300 Congressional Correspondence
8310 Congressional Hearings
8400 PCIE/ECIE
8500 Commendation Letters
8600 Press Release
8700 Chron Files

9000 VEHICLES GENERAL

9100 Fleet Folders (Individual file for each vehicle)
9200 Vehicle Accidents / Damage

Exhibit 8-6, Records Control Schedule

Background

The attached records control schedule authorizes the retention of investigative case files and the Enforcement Data System. This background section explains key records management concepts needed to understand and apply the attached schedule's disposition instructions.

Q1: What is the difference between Temporary versus Permanent Records?

A1. Temporary records are eligible for destruction after a specified time period. Whereas, Permanent records are considered so historically significant that they can never be destroyed. Agencies must transfer their Permanent records to the National Archives and Records Administration, which will then assume permanent physical and legal ownership of the files. The disposition instructions for OIG investigative case files are divided into two categories:

- **Item 1: Temporary** which are retained for 20 years.
- **Item 2: Permanent** which are significant case files that meet certain criteria and can never be destroyed.

The attached schedule lists the criteria for identifying those files that warrant permanent preservation. **The Headquarters Inspection Division will decide whether the case file is Temporary versus Permanent by applying the schedule's criteria. This decision will be made when the case is closed.**

Q2. When does the retention period start for OIG investigative case files?

A2. The retention period **ALWAYS begins on the last day of the fiscal year in which the investigation is closed** (i.e., 9/30/20XX). This is true regardless of when during the fiscal year the investigation was closed.

Q3. What does the term "cut off" mean and how are file cutoffs used to calculate the disposal date for an investigative case file?

A3. To cut off files means to make a logical break or stopping point in the collection of **closed** records. For investigative case files, the file cutoff date will always be the last day of the fiscal year in which the case was closed. The following example shows how the file cutoff determines when an investigative case file is eligible for disposal:

Example of Temporary Case File Closed in FY 2005

- The case was closed on 10/15/2004. The closed file's cutoff date is 9/30/2005.
  The 20-year retention BEGINS on 9/30/2005.
- The case file will be destroyed in October **2025** (i.e., 9/30/2005 plus 20 years).

U.S. Department of Homeland Security
Office of Inspector General

INVESTIGATIVE CASE FILES AND ENFORCEMENT DATA SYSTEM

THIS SCHEDULE COVERS RECORDS MAINTAINED BY THE OFFICE OF INSPECTOR GENERAL (OIG), OFFICE OF INVESTIGATIONS. THE RECORD SYSTEM CONSISTS OF PAPER INVESTIGATIVE CASE FILES AND THE ENFORCEMENT DATA SYSTEM (EDS). UNLESS OTHERWISE NOTED, ALL DISPOSITION INSTRUCTIONS ARE MEDIA NEUTRAL. THEY APPLY REGARDLESS OF THE MEDIA OR FORMAT OF THE RECORDS.

Investigative Case Files. Case files developed during investigations of known or alleged fraud and abuse, and irregularities and violations of laws and regulations. The case files relate to Department of Homeland Security (DHS) personnel and programs and operations administered or financed by DHS, including contractors and others having a relationship with DHS. This includes investigative reports and related documents, such as correspondence, notes, attachments and working papers. For disposition instructions, see Items 1-2 below.

Description of Records	Authorized Disposition	Disposal Authority
1. All Investigative Case Files **EXCEPT for unusually significant cases covered in Item 2 below.**	**TEMPORARY.** Cut off at end of the fiscal year in which the investigation is closed. Transfer to the Federal Records Center for temporary off-site storage as volume warrants. Destroy 20 years after completion of the investigation and all actions based thereon.	N1-563-07-05, Item 1

2. Significant Investigative Case Files that: (1) involve substantive information relating to national security; (2) involve allegations made against senior DHS officials; (3) attract national media or Congressional attention; or (4) result in substantive changes in DHS policies or procedures.	**PERMANENT.** Cut off at the end of the fiscal year in which the investigation is closed. Transfer to the National Archives and Records Administration for permanent retention 20 years after completion of the investigation and all actions based thereon. **Continued on the Next Page**	N1-563-07-05, Item 2

Enforcement Data System (EDS). The EDS supports the OIG Office of Investigations in its mission to conduct and supervise investigations of alleged violations of criminal, civil or administrative laws and regulations relating to DHS employees, contractors and other individuals and entities associated with DHS. The database is used to process complaints and to manage information provided during investigations. The system allows the OIG to index investigative case information; manage case inventory; track complaint status, disposition and results; and prepare various management and statistical reports. The EDS also captures investigative property records and special agent training records for Office of Investigation employees.

Dispositions instructions for EDS source documents, data entries, and outputs are covered under Items 3-7 below.

Description of Records	Authorized Disposition	Disposal Authority
EDS inputs/source documents. Includes the Complaint Data Entry Form and related documentation.	**TEMPORARY**. After the data has been entered/scanned and verified, file the Complaint Data Entry Form in the appropriate investigative case file and retain according to the disposition instructions in Items 1 and 2.	N1-563-07-05, Item 3
EDS data for Investigative Cases **EXCEPT FOR Significant Investigative Cases described in Item 2).**	**TEMPORARY.** Delete 20 years after completion of the investigation and all actions based thereon, or when no longer needed for operational purposes, whichever is later.	N1-563-07-05, Item 4

EDS data for Significant Investigative Cases described in Item 2.	**PERMANENT.** Transfer physical custody to the National Archives 5 years after completion of the investigation and all actions based thereon. Transfer legal custody to National Archives 20 years after completion of the investigation and all actions based thereon.	N1-563-07-05, Item 5
EDS data for government property records and other investigator-related information.	**TEMPORARY**. Delete when superseded or when no longer needed for operational purposes.	N1-563-07-05, Item 6
EDS outputs, such as management tracking and other ad hoc reports. These reports include printed or on-line displays containing lists or summary statistical information concerning investigative caseload, accomplishments, etc.	**TEMPORARY.** Destroy when no longer needed for business purposes or place in appropriate file and apply approved disposition for that item.	N1-563-07-05, Item 7

Exhibit 8-7, Transferring Closed Investigative Case Files to the FRC

These procedures explain how to transfer closed investigative records that are no longer needed for current OIG business to the Federal Records Center (FRC) for temporary off-site storage. The National Archives and Records Administration maintains a network of regional FRCs that store inactive records until they are eligible for final disposition (i.e., destruction or permanent transfer to the National Archives). Topics covered in these procedures include:

- Applying the disposition instructions in the OIG's Records Control Schedule.
- Organizing your files for transfer.
- Completing the Standard Form (SF) 135, Records Transmittal and Receipt.
- Packing the files and labeling the boxes.
- Sending your shipment to the FRC.

Use this guidance in conjunction with any specific direction issued by the Assistant Inspector General for Investigations or your Special Agent in Charge (SAC).

If you have any questions, please contact (b) (6), the OIG's Records Officer, by phone at (202) 254-(b) or email at (b) (6) @dhs.gov.

Before You Start

A. **Become familiar with the disposition instructions in the Office of Investigation's Records Control Schedule shown in Exhibit 8-5.** You will need to apply the Record Control Schedule's disposition instructions to determine which records are eligible for storage and to compute the disposal dates. The Schedule has two categories for investigative files:

- **Item 1: Temporary files** that are retained for 20 years.
- **Item 2: Permanent files** that are historically significant and can never be destroyed.

The INV Inspections Division will determine the appropriate records retention classification for each investigation when the case is closed. See the Getting Started section of these procedures for further discussion.

B. **Order standard record boxes through the General Services Administration (GSA) by calling 1-800-525-8027 or ordering online at www.gsaadvantage.gov**. Order the item called Special-Use Box, NSN # 8115-00-117-8249, measuring 14¾ x 12 x 9 ½. **IMPORTANT: Make sure you order boxes with the stock number ending in 8249. These are the only boxes that fit the FRC's shelves.**

You will also need a black felt-tip marker and clear packing tape. Clear tape can be ordered from GSA using Item NSN 7510-00-073-6094.

Getting Started

Step 1: Identify and Separate the Files

Temporary records are transferred to the FRC separately from permanent records. Therefore, an important first step is to separate any permanent files from the collection of files to be transferred. You will also need to sort your files by the fiscal year in which they were closed since this determines when the case file is eligible for disposal. Complete the following actions to identify and separate your files:

- Look at the Enforcement Data System (EDS) to see if the closed case has been designated as Temporary or Permanent. **IMPORTANT: The INV Inspections Division will determine the appropriate records retention classification for each investigation when the case is closed, and will enter the corresponding designation in EDS. If you are not certain about which category a closed case belongs under, consult with the Inspections Division.**

- Separate the files into two groups: (1) temporary files and (2) permanent files.

- Then sort each of these two groups by the **fiscal year in which the investigation was closed**. For example, files closed during FY 2004-2007 will be sorted as follows:

    1. Files closed in FY 2004.
    2. Files closed in FY 2005.
    3. Files closed in FY 2006.
    4. Files closed in FY 2007.

    IMPORTANT: Do not mix temporary and permanent files in the same group.

- Ensure that the files are complete with all supporting material and any final documents included.

- Ensure that the files are complete with all supporting material and any final documents included.

- **Remove any Grand Jury material since these documents cannot be stored at the FRC.** Coordinate the disposition of any Grand Jury material with the U.S. Attorney's Office.

Step 2: Organize the Files

- Remove duplicate materials, irrelevant notes, and any other "non-record" documents. If you have multiple identical copies of a document, use the original (or clearest copy if no original exists) and dispose of the remaining copies. **If documents are not exact duplicates, ensure that a copy of each variation is kept in the official file.**

- Separate paper and non-paper records (e.g., tape recordings, videotapes, computer diskettes, CDs, or microfilm). **Non-paper records must be transferred separately from paper records.**

- Separate classified and unclassified material. **To the extent possible, do not include classified and unclassified files in the same box.** [redacted].

- Place the records in accordion or manila folders. **The FRC will not accept loose papers, 3-ring binders, or hanging files.**

- Label each folder with a title identifying the contents. Use a meaningful file name that will aid any future retrieval of the folder without confusion.

Step 3: Pack the Records

Records are transferred to the FRC in groups or collections called "accessions." An accession consists of one or more boxes that contain the same type of records (i.e., temporary versus permanent files) and the same disposal date. **Each fiscal year grouping of closed files represents a separate accession or transfer because they will have different disposal dates.** Pack your records as follows:

- Box each group of files by their fiscal year closing date. For example:

  FY 2004 files in boxes 1-5.
  FY 2005 files in boxes 1-12.
  FY 2006 files in boxes 1-20.
  FY 2007 files in boxes 1-8.

  (Note: for the example above, you would have four different accessions.)

- **All files in a box should have the same fiscal year closing date. To the extent possible, avoid mixing files with different or multiple fiscal year closing dates.**

Step 3: Pack the Records (Continued)

- Pack the file folders in an upright position and use the same order as they were arranged in the office's files. Place **letter-size folders** in the boxes so that they are ordered from front to back. Place **legal-size folders** in the boxes so that they are ordered from left to right.

- Do not place non-paper records such as videotapes or CDs in the same box with paper records.

- Do not over pack or crowd files into the boxes.

- Do not mark the boxes at this time. Wait until the FRC assigns an accession number and returns the approved records transfer form to you (as further discussed in Step 6).

Step 4: Prepare Box Inventory Lists

Prepare an inventory list identifying the contents of each box (see the sample shown in Attachment 1). This helps you and the FRC to know what folders are in each box. **Create a separate inventory list for each fiscal year grouping of closed files** (e.g., one inventory list for files closed in FY 2005, another list for files closed in FY 2006, and a third list for files closed in FY 2007). You can determine the format of your list provided it has the following information:

- Name and telephone number of the person who prepared the inventory list.

- Disposal Authority.
  - For temporary files, use **N1-563-07-05, Item 1**.
  - For permanent files, use **N1-563-07-05, Item 2**.

- The box number and folder titles.

- Remarks indicating if a particular box contains:
  - Non-paper records, such as tape recordings, videotapes, computer diskettes, CDs, etc.
  - Classified material (i.e., Confidential, Secret, or Top Secret).

Step 5: Prepare and Submit the SF-135, Records Transmittal and Receipt Form

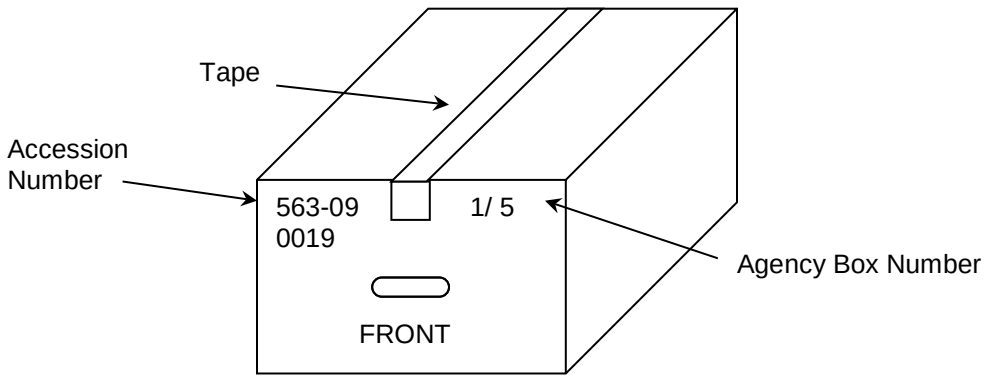
The SF-135 contains important information about your transfer that enables the FRC to properly store and service your records. Attachment 2 provides a sample SF-135 and instructions for completing the form. Blank forms are posted on the OIG Intranet at [redacted]

A separate SF-135 is required for each fiscal year grouping of closed files. This is because the disposal date for each group is different. For example, case files closed in FY 2004 will have separate SF-135 than those closed in FY 2005.

Your completed SF-135 must be approved by both the OIG Records Officer and the FRC BEFORE shipping the records. To get approval, first email the SF-135 and inventory list to (b) (6) at (b) (6) @dhs.gov. After (b) (6) reviews your information, she will advise you to submit the SF-135 and inventory list to the FRC for formal approval. The FRC will assign an accession number and return the approved SF-135 to you within 10 working days, authorizing shipment of the boxes.

Step 6: Number and Label the Boxes

- Once you receive the approved SF-135, you will have 90 days to ship your boxes. After 90 days, your accession number will be cancelled.
- Label your boxes with a wide black felt marker as follows:
  - Write the accession number in the upper left hand corner.
  - Write the box number in the upper right hand corner. Begin with box #1 and include the total number of boxes in the accession (e.g. 1/10, 2/10, 3/10, etc). See the sample below.
  - Lettering should be approximately 1" high.



Step 6: Number and Label the Boxes (continued)

- Place a copy of the approved SF-135 and inventory list in box #1 of each accession.
- Seal the boxes. Do not tape over the accession number or box number. Do not place mailing or shipping labels on the end of the box with the accession number.

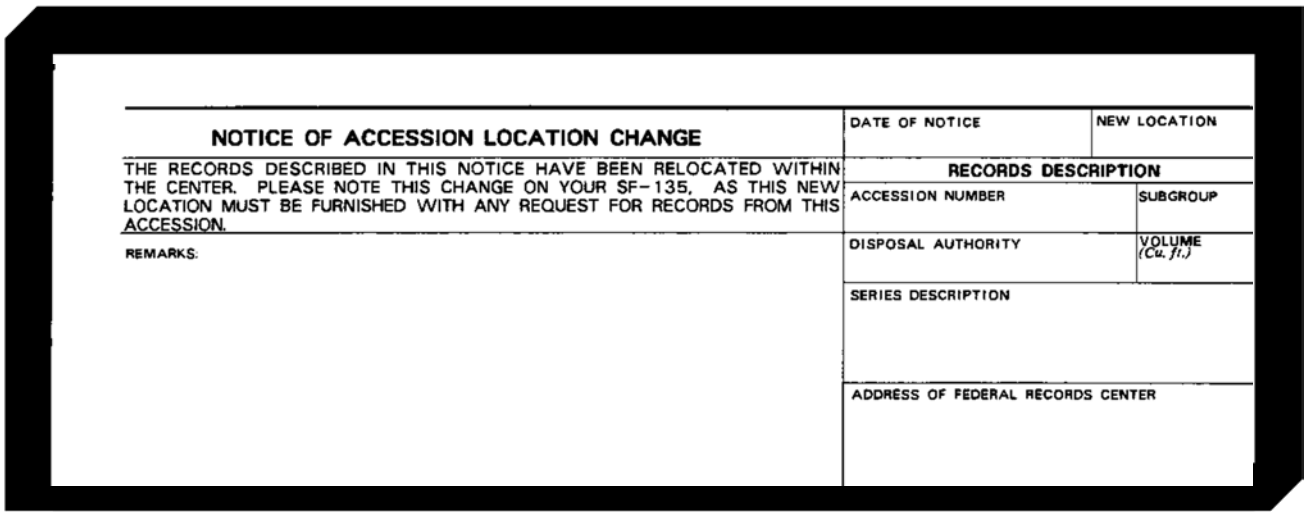
Step 7: Ship the Records

You may send your files by FedEx or U.S. Parcel Service. Large shipments (e.g., more than 20 boxes) must be stacked in a certain order. The FRCs differ slightly regarding the preferred stacking order for large shipments. Please contact the transfer office at your local FRC to obtain further instructions. FRC phone numbers and e-mail addresses are available FRC Director's home page at http://www.archives.gov/frc/directors.html

Step 8: Maintain Good Records in Your Office

After your records arrive at the FRC, you will receive a final receipt copy of the SF-135. File the final copy for your reference and attach the inventory list. The SF-135 and inventory list may be destroyed 6 years after the related case files are destroyed or after the files are transferred to the National Archives for permanent preservation.

Occasionally, the FRC will need to relocate your records after assigning a storage location. If so, the FRC will send you the Notice of Accession Location form shown below. You will need to update your file copy of the SF-135 to reflect the new location.



NOTICE OF ACCESSION LOCATION CHANGE

THE RECORDS DESCRIBED IN THIS NOTICE HAVE BEEN RELOCATED WITHIN THE CENTER. PLEASE NOTE THIS CHANGE ON YOUR SF-135, AS THIS NEW LOCATION MUST BE FURNISHED WITH ANY REQUEST FOR RECORDS FROM THIS ACCESSION.

REMARKS:

DATE OF NOTICE | NEW LOCATION

RECORDS DESCRIPTION

ACCESSION NUMBER | SUBGROUP

DISPOSAL AUTHORITY | VOLUME (Cu. ft.)

SERIES DESCRIPTION

ADDRESS OF FEDERAL RECORDS CENTER

Attachment 1: Sample Box Inventory List

Department of Homeland Security
Office of Inspector General
Houston Field Office of Investigations
(b) (6) [redacted]

Prepared By: (b) (6) [redacted] Date: February 3, 2009

INVENTORY OF OIG INVESTIGATIVE FILES CLOSED IN FY 2005

Disposal Authority: N1-563-07-05, Item ___ **(NOTE: For Temporary Files, enter Item 1. For Permanent Files, enter Item 2.)**

Box No.	Box Contents	Remarks
1 of 4	I-Case # _____ I-Case #_____ I-Case #_____	Contains Videotapes
2 of 4	I-Case # _____ I-Case #_____ I-Case #_____ I-Case # _____	
3 of 4	I-Case # _____ I-Case # _____ I-Case #_____	Contains Classified Information at the Secret level.
4 of 4	I-Case # _____ I-Case #_____ I-Case #_____ I-Case # _____	

Important: Prepare a separate inventory list for each fiscal year grouping of closed files (e.g., cases closed in FY 06 would be listed separately from the FY 05 files shown above.

Attachment 2: Sample SF-135, Records Transmittal and Receipt Form

A sample SF-135 is shown below. Detailed instructions for completing the form are attached.

RECORDS TRANSMITTAL AND RECEIPT — Complete and send original and one copy of this form to the appropriate Federal Records Center for approval prior to shipment of records. See specific instructions on reverse. PAGE 1 OF [ ] PAGES

1 TO (Complete the address for the records center serving your area as shown in 36 CFR 1228.150.)

Ft. Worth Federal Records Center
P.O Box 6216
Forth Worth, Texas 76115

5 FROM (Enter the name and complete mailing address of the office retiring the records. The signed receipt of this form will be sent to this address.)

[redacted]
DHS Office of Inspector General
Houston Field Office of Investigations
[redacted]

2	AGENCY TRANSFER AUTHOR-IZATION	TRANSFERRING AGENCY OFFICIAL *(signature and title)* Joe Black, Special Agent In Charge; DHS-OIG, Houston Field Office of Investigations	DATE
3	AGENCY CONTACT	TRANSFERRING AGENCY LIAISON OFFICIAL *(Name, office and telephone No)* Mary Smith, Investigative Specialist (713) 406-4600 DHS-OIG Houston Field Office of Investigations mary.smith@dhs.gov	
4	RECORDS CENTER RECEIPT	RECORDS RECEIVED BY *(Signature and Title)* **LEAVE BLANK**	DATE

6 **RECORDS DATA**

ACCESSION NUMBER			VOLUME *(cu. ft.)*	AGENCY BOX NUMBERS	SERIES DESCRIPTION *(with inclusive dates of records)*	RESTRIC-TION	DISPOSAL AUTHORITY *(schedule and item number)*	DISPOSAL DATE	COMPLETED BY RECORDS CENTER			
RG	FY	NUMBER							LOCATION	SHELF PLAN	CONT. TYPE	AUTO. DISP.
(a)	*(b)*	*(c)*	*(d)*	*(e)*	*(f)*	*(g)*	*(h)*	*(i)*	*(j)*	*(k)*	*(l)*	*(m)*
563	09	**LEAVE BLANK**	6	1-6	Investigative Case Files closed in FY 2005. CUTOFF: 9/30/06 **Records Subject to Privacy Act**		N1-563-07-05, Item 1	10/2026				

NSN 7540-00-634-4093 135-107 Standard Form 135 (Rev. 7-85) Facs
Prescribed by NARA
36 CFR 1228.152

Instructions for Completing the SF-135

Obtain a blank copy of the SF-135 at [redacted]. Then fill out the form as follows:

- **Item 1 FRC Address:** Enter the name and address of the regional FRC servicing your area. To find the address of your particular FRC, go to [redacted]
- **Item 2 Agency Transfer Authorization:** Enter your SAC's name and title, and your office's name. The SAC should sign and date this block.
- **Item 3 Agency Contact:** Enter your name, office, phone number, and email address.
- **Item 4 Records Center Receipt:** Leave blank. The FRC will complete this.
- **Item 5 "From" Block:** Enter your name and your office's mailing address.
- **Item 6 Accession Number:** Items 6(a) thru 6(c) comprise the accession number. Complete these items as follows:
- **Item 6(a) RG:** Enter 563 which is the Record Group (RG) number assigned to DHS.
- **Item 6(b) FY:** Enter the last two digits of the current fiscal year in which you are completing the form.
- **Item 6(c) Number:** Leave blank. The FRC will assign a sequential number.
- **Item 6(d) Volume:** Enter the total number of boxes in the accession.
- **Item 6(e) Agency Box Numbers:** Enter the inclusive range of box numbers (e.g., 1-30).
- **Item 6(f) Series Description:** Indicate the fiscal year in which the files were closed and the file cutoff date, which is **ALWAYS the last day** of the fiscal year in which the case was closed (i.e., 9/30/XX). **Also include a bolded statement indicating that the records are subject to the Privacy Act.** A sample entry for Item 6(f) is shown below.

> Investigative Case Files closed in FY 2005. FILE CUTOFF: 9/30/06.
>
> **Records subject to Privacy Act.**

- **Item 6(g) Restriction:** Leave blank. The FRC will complete this item.
- **Item 6(h) Disposal Authority:**
  - For temporary files, cite **N1-563-07-05, Item 1**.
  - For permanent files, cite **N1-563-07-05, Item 2**.

- **Item 6(i) Disposal Date:** Compute the disposal date using the file cutoff date. The file cutoff will ALWAYS be the last day of the fiscal year in which the case was closed (i.e., 9/30/XX). This is true regardless of when the case closed during the fiscal year. Examples for calculating disposal dates are shown below.

  Example #1: Temporary Case File Closed During FY 2007

  - The case was closed on 11/17/2006.
  - The file cutoff date is 9/30/2007 (i.e., the last day of FY 2007). **The 20-year retention for temporary files BEGINS on 9/30/2007.**
  - The disposal date will be October 2027 **(i.e., 9/30/2007 plus 20 years). For purposes of the SF-135's Item 6(i), enter 2027/OCT.**

  Example #2: Permanent Case File Closed During FY 2007

  - The case file was closed on 6/25/2007.
  - The file cutoff date is 9/30/2007 (i.e., the last day of FY 2007).
  - The permanent file will be transferred to the National Archives for permanent ownership 20 years after the file cutoff date (i.e., 9/30/2007 plus 20 years).
  - For purposes of the Item 6(i), enter **2027/P**. Note: Permanent files are transferred to the National Archives on an annual basis so you do not need to specify a month. Also, the letter "P" signifies that the file is permanent.

- **Items 6(j)-(m):** Leave these items blank. The FRC will complete them.

Exhibit 8-8, INV Form 10, Classified Document Record of Transmittal

Office of Inspector General - Investigations
U.S. Department of Homeland Security

Homeland Security

CLASSIFIED DOCUMENT
RECORD OF TRANSMITTAL

(The inclusion of classified information should be avoided)

Prepare in accordance with 31 CFR, Part 2

TRANSMITTAL DATE

SECTION A – ADDRESSEE AND SENDER *(Type or Print in Ink)*	
TO:	FROM:

SECTION B – DOCUMENT DESCRIPTION *(Type or Print in Ink)*				
CLASSIFICATION	DATE OF DOCUMENT	Description – (Identify items such as report, letter, memo, etc. Unclassified subject or short title. Copy number and number of attachments.)	ORIGINATOR	# OF COPIES

SECTION C – ACKNOWLEDGEMENT OF RECEIPT		
NAME *(Type or Print)*	SIGNATURE	DATE

SECTION D – RECORD OF INTERNAL TRANSMITTAL				
ADDRESSEE	COPY NO.	NAME OF RECIPIENT *(Type or Print in Ink)*	SIGNATURE	DATE
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				

INV FORM-10

9.0 INVESTIGATIVE INTERVIEWS AND STATEMENTS

9.1 INTERVIEWS AND TESTIMONIAL EVIDENCE DEFINED

An interview may be defined as the systematic questioning of an individual to determine if they have knowledge relevant to an investigation.

Evidence that is communicative in nature is called testimonial evidence; i.e., it reveals knowledge. Testimonial evidence can be in the form of oral statements, written statements, non-verbal responses, or by conduct.

9.2 INTERVIEW GUIDELINES

SA safety should be the primary concern when choosing a location to interview subjects and witnesses. For safety and evidentiary considerations, two SAs (or other law enforcement personnel) should be present to conduct an interview whenever practicable. SAs should interview subjects and witnesses in an area free from potential weapons. At the start of the interview, the SAs should consider asking the subject or witness if they are armed and if necessary, complete a pat-down search of them.

SAs should conduct background checks before interviewing subjects whenever practicable.

SAs should seek to establish a rapport with the interviewee and be watchful for telltale indications of deception such as “body language.”

Agents are reminded that employees represented by the National Treasury Employees Union (NTEU) are entitled to special processing as outlined in Article 22 of a Federal Labor Relations Authority (FLRA) decision. Although Article 22 of the agreement does not apply to DHS OIG, ICE and CBP are obligated to follow its terms. This needs to be considered when working a joint investigation with ICE OPR or CBP IA when planning to interview NTEU employees.

Interview Preparation

SAs should determine the investigative issues and elements of proof required to sustain any charges or adverse actions. SAs should determine how witnesses relate to the investigation and what information they can provide. SAs should consider preparing questions in advance. Arrange and mark all documents that will be presented for authentication or identification.

Conduct of the Interview

At the start of the interview, the SAs should fully identify themselves and clearly state the subject matter of the interview. The SA will advise the person of their rights if appropriate.

SAs should obtain the interviewee's full identifying data, work/residence/associates, telephone numbers and, when relevant, complete a "Personal History Information," INV Form 13, **(Exhibit 9-1)**.

SAs should allow the person interviewed to present information in its entirety if relevant to the case. SAs should formulate questions in a logical manner and ask them in understandable terms.

The interview should be confined to matters within the scope of an official inquiry or investigation.

Two SAs will be present when the interviewee is the subject of the investigation or a critical witness; when the interviewee is of the opposite sex or a minor, or when the interview is to be conducted in a location where safety may be of concern.

When two SAs conduct an interview, the case agent should thoroughly brief the participating agent on the investigation prior to the interview, so both can participate in the questioning. It is recommended that one of the agents be designated to take notes.

Follow-up questions on all leads developed during an interview should be pursued. The SA should never assume that a re-interview or follow-up contact of the individual is possible.

Non-Disclosure Warnings

The SA conducting the interview has the option of providing a disclosure warning to the interviewee and any union representative present. These warnings advise the interviewee not to discuss the nature of the interview with any other person(s) except private legal counsel or union representatives. **(Exhibits 9-2, 9-2A and 9-2B)**

9.3 ELECTRONIC RECORDING OF INTERVIEWS

A. Policy Overview

1. There is a presumption that statements made by persons in DHS OIG custody will be recorded following arrest and prior to initial appearance when the arrestee is in a place of detention with suitable recording equipment. Further guidance on conducting custodial recorded interviews and what constitutes detention is outlined below. Recording of non-custodial interviews is optional and guidance is also outlined below.

2. For the purposes of this section, a "recorded interview" occurs when a DHS OIG Special Agent, after providing his/her official identity to a party with whom the DHS OIG Special Agent is communicating, records the party's statements. A recorded interview may be overt or covert, and may occur in a non-custodial or custodial setting.

Note: For the purpose of this interview policy, the terms "interview" and "interrogation" are interchangeable.

3. All approvals, procedures and legal guidance applicable to interviews in general, e.g., voluntariness, compliance with Miranda and the Fifth and Sixth Amendments, and contact with represented persons, shall continue to apply to the electronic recording of interviews.

4. Special Agents must use suitable recording equipment as issued and approved by OIG management. OIG issued cell phones or other personally owned equipment shall not be used for recordings. Additionally, "dual-use" equipment, such as tablets or laptop computers or any other devices that are not primarily electronic recording devices are not permitted for use.

B. Overtly Recorded Non-Custodial Interviews

1. Special Agents have the option to conduct an overtly recorded non-custodial interview. An overtly recorded interview occurs when a Special Agent, identified as such, advises the interviewee that the interview is or will be recorded, or the interviewee is otherwise clearly aware that the interview is in fact being recorded (e.g., a visible operating recording device is placed in front of the interviewee).

2. The Special Agent must provide notification to his/her supervisor as soon as feasible, but no later than 5 business days after completion of an overtly recorded noncustodial interview. The notification should be in the form of the interview summary captured in a Memorandum of Activity (MOA).

3. Additionally, prior to conducting the interview, the interviewing employee should consider the factors listed below to ensure the overtly recorded interview is operationally prudent and consistent with investigative or intelligence gathering objectives:

   a. Whether the purpose of the interview is to gather evidence for prosecution or intelligence for analysis or both;

   b. If prosecution is anticipated, the type and seriousness of the crime, including, in particular, whether the crime requires *mens rea*, or a mental element, such as knowledge or intent to defraud, proof of which would be considerably aided by the interviewee's admissions in his/her own words;

   c. Whether the interviewee's own words and appearance (in video recordings) would help rebut any doubt about the meaning, context or voluntariness of his/her statement or confession raised by his/her age, mental state, educational level, or understanding of the English language; or is otherwise expected to be an issue at trial, such as to rebut an insanity defense; or may be of value to behavioral analysts;

d. If interviewers anticipate that the interviewee might be untruthful during an interview, whether a recording of the false statement would enhance the likelihood of charging and convicting the person for making a false statement;

e. The sufficiency of other available evidence to prove the charge beyond a reasonable doubt;

f. The preference of the USAO and the Federal District Court regarding recorded interviews or confessions;

g. Local laws and practice particularly in task force investigations where state prosecution is possible;

h. Whether interviews with other witnesses or subjects in the same or related investigations have been electronically recorded; and

i. The potential to enlist the witness or subject's cooperation and the value of using his/her own words to elicit his/her cooperation.

C. Overtly Recorded Non-Custodial Interviews: Documentation and Handling

1. After completing the recorded interview, the Special Agent must generate an MOA documenting the fact that the interview took place. The MOA must state the official identity of the interviewing agent(s), the purpose of the interview, the identity of the individual recorded and the details of the recording session (e.g., date, time, start and stop periods, and reasons for stopping). The MOA should also list identifying information of other relevant individuals, organizations, companies or other entities mentioned for the purpose of indexing to allow for future word search capabilities. The agent should also include a summary of the recording if doing so will aid in the management of the investigation and/or provide a document for intelligence sharing and analysis. Transcription of the recording is optional. The following caveat must be added to the MOA:

   "The below is an interview summary. It is not intended to be a verbatim account and does not memorialize all statements made during the interview. Communications by the parties in the interview room were electronically recorded. The recording captures the actual words spoken."

2. At the conclusion of recording the statement, the Special Agent will:

   a. For video recorded interviews:

      If the video recording device used for the interview records onto an insertable memory/data card, the original video-recorded interview will be removed from the video camera uploaded from the memory card to a secure OIG computer as soon as practicable after the interview. If the video recording device used

records on media other than an insertable memory/data card contained in the camera (e.g., an internal system recording video on an external hard drive or server), the agent recording the interview should take steps to download the recording onto a DVD or other appropriate external memory device and then a secure OIG computer as soon as practicable. The memory/data card or the DVD containing the original video recorded interview will then be initialed and dated by the Special Agent who recorded the interview and placed in a suitable container that should be labeled with the case number, the interviewee's full name, the date of the interview, the location of the interview, and the names of the Special Agent(s) conducting the interview. The container with the original recording will then be secured as evidence. No Special Agent shall alter, change, modify, or conceal any portion of any recorded interview.

The copy of the interview remaining on the OIG computer will be the working copy that the Special Agent can view and use for investigative purposes, and it will also be used to make additional copies to provide to prosecutors or transcription service providers.

b. For audio recorded interviews:

The original audio recorded interview will be uploaded to a secure OIG computer and then will be immediately burned onto a CD, DVD or appropriate external memory device. This CD or DVD will be initialed and dated by the agent who recorded the interview and placed in a suitable container, which will be labeled with the case number, the interviewee's full name, the date of the interview, the location of the interview, and the names of the Special Agent(s) conducting the interview. The container with the original recording will then be secured as evidence. No Special Agent shall alter, change, modify, or conceal any portion of any recorded interview.

The copy of the interview remaining on the OIG computer will be the working copy that the Special Agent can listen to and use for investigative purposes, and it will also be used to make additional copies to provide to prosecutors or transcription service providers.

3. Recordings made under this policy will be maintained according to current retention standards applicable to OIG official case files.

4. Any handwritten notes taken during the recorded interview must be retained as original note material.

[redacted]

[redacted]

[redacted]

[redacted]

F. Custodial Recorded Interviews (Warrant/Probable Cause): General Provisions

1. There is a presumption that statements made by persons in OIG custody will be recorded following arrest and prior to initial appearance when the arrestee is in a place of detention with suitable recording equipment. All statements made during a custodial interview of persons arrested by a DHS OIG Special Agent for federal crimes[1], prior to initial appearance and while in a place of detention with suitable recording equipment, must be electronically recorded (with very limited exceptions as listed below). A place of detention includes a DHS OIG field office, RAC office or Sub-Office, and an established or controlled task force location. A place of detention also includes non-DHS OIG locations such as state, local, or tribal law enforcement facilities, offices, correctional or detention facilities, jails, police or sheriff's stations, holding cells, or other structures used for detention purposes with suitable recording equipment. The custodial recorded interview may be overt or covert. If feasible, prior to the arrest, the employee should discuss with his/her chain of command and the prosecutor the presumption of recording and whether or not it applies in the case at hand. No supervisory approval is necessary to record a post-arrest custodial interview. No INV Form-71A **(Exhibit 9-3)** is necessary for a post-arrest custodial interview.

2. The recording may be audio only, but video may also be used. The recording must commence the moment the subject enters the interview room and continue for the duration of the interview. The recording should include an advice and waiver of Miranda rights, as well as a question and answer segment designed to demonstrate that the subject's statements are voluntary and not the product of coercion.

3. The recording equipment should be turned on prior to the arrestee being placed in the interview room and should only be turned off after the interview is completed and the subject has left the room. All discussions in the interview room, including any pre-interview discussions, even if they occur before the reading of the Miranda advisement, must be included in the recording. Should the need arise for either the arrestee or agent to leave the interview room, recording devices can continue to operate without interruption. If the recording is temporarily stopped, the reason for stopping the recording and the duration should be documented.

4. If the arrestee wants to speak privately with his attorney in the interview room, the recording equipment must be turned off. We cannot record, or attempt to record, any communication intended to be private that occur between the attorney and an arrestee.
5. Pursuant to 18 USC §3501, the following factors bear on voluntariness and should be considered:

[1] This policy does not apply to a person arrested for a state or local crime during a joint or task force investigation.

a. The time elapsing between arrest and arraignment of the defendant making the statement, if it was made after arrest and before arraignment;;

b. whether such defendant knew the nature of the offense with which he was charged or of which he was suspected at the time of making the confession;

c. whether or not such defendant was advised or knew that he was not required to make any statement and that any such statement could be used against him;

d. whether or not such defendant had been advised prior to questioning of his right to the assistance of counsel; and

e. whether or not such defendant was without the assistance of counsel when questioned and when giving such confession.

6. Special Agents must use suitable recording equipment as issued and approved by OIG management. OIG issued cell phones or other personally owned equipment shall not be used for recordings. Additionally, "dual-use" equipment, such as tablets or laptop computers or any other devices that are not primarily electronic recording devices are not permitted for use.

7. Custodial interviews that do not occur in a place of detention are excluded from the mandatory recording policy. When practicable, however, the decision whether or not to record such interviews may be the subject of consultation between the agent and the prosecutor, to determine when recording may be appropriate. Recording is not required when a person is waiting for transportation, or is en route, to a place of detention. If a Special Agent deems it prudent or necessary to record a post-arrest custodial interview while en route to a place of detention, no supervisory approval is needed. In such situations, agents must use recording equipment as otherwise permitted under these provisions.

8. The presumption, however, does not apply when the interviewee is outside the United States. The presumption of recording does not apply to interviews conducted abroad, or to interviews on U.S. warships or U.S. military installations in overseas locations, U.S. Embassies abroad or on other U.S. government property physically outside the United States. Though the presumption of recording does not apply outside the United States, the decision whether to record an interview outside the United States should be the subject of consultation between the agent and the prosecutor to determine when recording may be appropriate.

G. Overtly Recorded Custodial Interviews

DHS OIG Special Agents may conduct an overtly recorded custodial interview. An overtly recorded custodial interview occurs when an OIG Special Agent, identified as such, advises the interviewee that the interview is being or will be recorded, or the interviewee is otherwise clearly aware that the interview is in fact being recorded (e.g.,

visible operating recording device is placed in front of the interviewee). No supervisory approval is necessary to record a post-arrest custodial interview. No INV Form 71A **(Exhibit 9-3)** is necessary for an overtly recorded custodial interview.

H. Overtly Recorded Custodial Interview: Documentation and Handling

1. After completing the recorded interview, the agent must generate an MOA documenting the fact that the interview took place. The MOA must state the official identity of the interviewing agent(s), the purpose of the interview, the identity of the individual recorded and the details of the recording session (e.g., date, time, start and stop periods, and reasons for stopping) and list identifying information or other relevant individuals, organizations, companies or other entities mentioned for the purpose of indexing to allow for future word search capabilities. The Special Agent should also include a summary of the recording if doing so will aid them in the management of the investigation and/or provide a document for intelligence sharing and analysis. The following caveat must be added to the MOA:

   "The below is an interview summary. It is not intended to be a verbatim account and does not memorialize all statements made during the interview. Communications by the parties in the interview room were electronically recorded. The recording captures the actual words spoken."

2. The OIG will provide electronic copies for distribution pre-indictment. Post-indictment, the USAO will pay for transcripts of recordings as necessary.

3. Any handwritten notes taken during the recorded interview must be retained as original note material.

4. Upon completion of the interview, the recording must be handled as set forth in paragraphs C 2 a and b, above.

[redacted]

[redacted]

K. Exceptions to Recording of Post-Arrest Custodial Interviews

1. Unless conducted pursuant to prior written approval, the interviewing Special Agent must document in an email to the SAC, as soon as feasible, but no later than 5 business days after the completion of the interview, the exercise of an exception to the mandated requirement to record a custodial post-arrest interview. The email must be captioned, "Exception to Mandatory Recording of Post-Arrest Custodial Interview," and must specifically address the reason(s) why the interview was not recorded (e.g. one of the enumerated exceptions below). Upon SAC approval, the interviewing Special Agent must also complete an MOA, for the case file, documenting the exception. A copy of the MOA documenting the basis for utilizing an exception to the mandatory recording of post-arrest custodial recorded interview policy must be made available to the AUSA by the "office of origin" field office overseeing the investigation.

a. Refusal of subject to be recorded during the interview: If the subject is advised that the interview will be recorded and he/she indicates that he/she is willing to provide a statement but wishes not to be recorded, then the recording need not take place. Once recording has started, the interviewing employee may cease the recording of the interviewee if the interviewee asks not to be recorded. No supervisory approval is needed to cease recording when an interviewee asks not to be recorded. The interviewee's request to cease the recording should be captured on the recording and the request also documented in the corresponding summary MOA.

b. Public Safety Exception: If the questioning is reasonably prompted by an immediate concern for the safety of the public or the arresting agent under *New York v. Quarles* then recording is not mandatory.

c. National Security Exception: National security investigations implicate unique concerns with respect to the need to protect classified information and sources and methods, among other things. However, the mere fact that an interview may involve classified information or classified sources and methods is NOT, on its own, sufficient to implicate the national security exception. In all custodial post-arrest recorded interviews in national security investigations, agents are to ensure the proper classification and marking, as appropriate and in accordance with the appropriate DHS Security Classification Guide or other US Intelligence Community (USIC) classification authorities, of all documentation or media capturing the content of the interview, including but not limited to, interviewer notes, video recording files, audio recording files, written transcripts, physical and/or electronic images, and original and derivative written reports. That an interview is recorded as opposed to documented in an MOA does not affect the OIG's responsibility to protect properly classified information from disclosure.

To invoke the national security exception, prior SAC and AIGI approval is required. Notice must also be provided to the Assistant United States Attorney(s) assigned to the case. The MOA documenting the basis for applying the national security exception should also document the date and method (e.g., email or telephone call, etc.) by which the AUSA was informed of the decision to not record a post-arrest, custodial interview, and the position of the USAO.

In national security investigations, once a recording has begun, and the interviewing employee seeks to cease the mandatory recording of a post-arrest, custodial interview, the interviewing employee's decision to cease recording must have prior SAC and AIGI approval, and all of the following criteria must be met:

(1). the subject waives Miranda rights,
(2). the subject agrees to cooperate with the Government,
(3). the subject waives the right to a speedy presentment, and

(4). it becomes operationally necessary to relocate the subject to a location other than a place of detention defined in paragraph F above. In such a circumstance, the interview may still be recorded as a matter of discretion pursuant to this subchapter 9.3. The decision to relocate the subject, as well as the subject's consent to the relocation, should be captured on the recording.

Alternatively, once recording has started, the interviewing Special Agent may cease the recording of the interviewee if the interviewee asks not to be recorded. No supervisory approval is needed to cease recording when an interviewee asks not to be recorded. The interviewee's request to cease the recording should be captured on the recording and the request also documented in the corresponding summary MOA.

The following factors may assist in determining whether to invoke the national security exception to not record a post-arrest, custodial interview:

(1). The interview is likely to expose or discuss information which is classified higher than SECRET, or is compartmented, a Special Access Program, or other highly sensitive USIC collection or program;
(2). The interview is likely to expose information related to sensitive human sources, such as Recruitment-In-Place, a Double Agent Operation, or a jointly operated source;
(3). The interview is likely to utilize or expose USIC or foreign government information and the USIC partner or foreign government objects to the recording;
(4). The interview necessitates participation by a USIC partner whose identity must be protected;
(5). If the subject is arrested overseas and the law enforcement interview of the subject has commenced before the subject's arrival in the United States; or
(6). The interview is likely to result in information about foreign government penetrations of the U.S. Government or discuss information about a Sensitive Investigative Matter (SIM).

This is not meant to be an exhaustive list and other considerations may counsel in favor of applying the national security exception. Conversely, the inclusion of one or more of the above factors does not guarantee exclusion from the recordings policy in a national security investigation. As such, any application of the national security exception must articulate with specificity the likely harm associated with recording a post-arrest, custodial interview in a particular investigation.

d. Recording is not reasonably practicable: In the event that the circumstances of the arrest does not allow for the recording of the interview such as law enforcement safety, equipment malfunction, an unexpected need to move the interview from the detention center (i.e., medical facility), or a need for large-

scale take downs with multiple interviews in a limited timeframe exceeding the number of recording facilities.

e. "Residual" Exception: The SAC and the United States Attorney, or their designees, agree that a significant and articulable law enforcement (e.g., avoiding disclosure of a sensitive law enforcement technique) purpose requires not recording the interview. Some considerations may include the potential safety and welfare of a confidential human source. This exception is to be used judiciously and very infrequently.

L. Preamble to Recorded Interviews

1. When recording statements, the Special Agent will start the recording with a preamble that provides the date, time, identification of the participants, and the reading (or re-reading, if previously read) of the interviewee's Fifth Amendment rights, followed by the interviewee's acknowledgement and waiver of these rights.
2. In instances where the recording is conducted covertly, the preamble will be recorded outside the presence of the interviewee and as contemporaneously with the start of the interview as is practical. However, the covert recording should also address the interviewee's Fifth Amendment rights in the same manner described above for overt recordings.

9.4 INTERVIEWING MINORS

Under federal law, a "minor" is defined as a person who has not attained his or her 18th birthday.

Two SAs should be present when interviewing minors. Although there is no federal legal requirement to have a parent, guardian, or custodian present during a juvenile interview, strong consideration must be given to having such persons present.

SAs interviewing minors should use "understandable language" and take into consideration the age and educational level of the minor being interviewed.

The federal government generally defers prosecution of minors to the State. SAs are encouraged to consult with local prosecutors and the AUSA regarding matters involving minors.

9.5 USE OF INTERPRETERS

If the individual to be interviewed cannot converse in English, or if the SA is not qualified to use the principal language of the person to be interviewed, a reliable interpreter will participate in the interview. Whenever possible, the interpreter should not have any personal association with the matter in question.

In certain instances, an audio recording of the interview may be advisable. Reference Section 9.3, Electronic Recording of Interviews, for instruction on conducting recorded interviews. This

recording can subsequently be used to facilitate an independent translation of the contact, which can be utilized to corroborate/validate the text of the interview.

9.6 DOCUMENTING INTERVIEWS

An MOA INV Form 09 will be used to document interviews as outlined in Chapter 12.4.

9.7 WRITTEN STATEMENTS

Generally, written statements or affidavits will be obtained whenever possible from the subject of the investigation. Statements should also be requested from material witnesses in matters that are likely to have a significant impact on the outcome of the investigation.

The subject's statement puts admissions or denials made during the course of an interview in the subject's own words, under the subject's own signature. A statement of a witness provides a personal account that can be used to refresh recollections and dissuade a witness from later changing their testimony.

The statement should be taken near the conclusion of the interview and should mirror the oral admissions or denials that were made during the interview.

The preferred statement format is the narrative form. The interrogatory form (question and answer type) may be used at the discretion of the interviewing agent in certain circumstances such as when the content of the interview is highly technical. Questionnaires will generally not be provided to subjects and/or witnesses to complete on their own.

When necessary, the interviewing agent may assist in the preparation of the statement to ensure that all pertinent areas covered in the interview are fully documented and extraneous matters avoided. SAs should generally not write statements for interviewees unless the interviewee is unable to complete the statement for themselves. If the SA prepares the statement, the SA should pay particular attention to avoid words and phrases that the interviewee would not understand or use.

The individual must be given the opportunity to read and make corrections to the statement prior to signing. The interviewee should initial and date the beginning and end of each page of the statement. Any corrections should be initialed and dated by the interviewee. A line should be drawn through all blank areas of the statement and initialed by the interviewee.

If appropriate, when a subject has been advised of their rights, the preamble will include: "I have been advised of my rights per Miranda/Garrity, which I have waived prior to making this statement."

If a DHS employee, who is not a subject, agrees to furnish a statement only after being informed of the DHS MD requiring full employee cooperation in an official investigation, strike the words "*free and voluntary"* on the INV Form 28 **(Exhibit 9-4)**. If the employee insists, insert a sentence to the effect: *"This statement is being furnished to comply with the Inspector General's*

Act and the Department of Homeland Security regulations requiring me to cooperate in an official investigation."

An MOA will be drafted for each statement obtained during the course of an investigation. The statement will be appended as an attachment to the MOA. The MOA should contain a summary of the information that was provided, but should not repeat verbatim the information in the statement. The MOA should also include any other information that was not included in the statement.

If critical information was left out of the statement, a second statement should be obtained. The supplemental statement must always make reference to the original statement. Do not destroy the original statement or return it to the interviewee.

Statements will be documented using INV Form 28, "Sworn Statement" **(Exhibit 9-4).**
A Spanish version of the "Sworn Statement" INV Form 28S is available **(Exhibit 9-5)**.

9.8 EXCULPATORY AND FALSE EXCULPATORY STATEMENTS

When subjects deny their involvement or culpability in an offense, agents will make every attempt to obtain written statements including these denials. The purpose of obtaining these statements is to restrict the subject from altering their account of the facts. A false statement may become a prosecutorial tool for impeaching the credibility of a defendant or witness at trial.

False or exculpatory statements and evidence must be brought to the attention of the prosecutor or other presiding official in the course of any civil, administrative, or criminal proceeding.

9.9 OATH OR AFFIRMATION

5 U.S.C. Appendix 3, Section 6 (a) (5) gives SAs explicit authority to administer oaths and affirmations. General authority is given in 5 U.S.C. § 303. SAs will administer the oath or affirmation in a formal manner and have the interviewee raise their right hand. Then ask one of the following:

> OATH: *"Do you swear that the statement you have given is the truth, the whole truth, and nothing but the truth, so help you God?"*
>
> AFFIRMATION: *"Do you affirm, under penalty of perjury, that the statement you have given is the truth, the whole truth, and nothing but the truth?"*

If a person refuses to sign a statement but admits that the contents are true and accurate, make a notation at the end of the statement that the statement was read to or by the interviewee, who acknowledged the contents to be true and accurate, but refused to sign the document. The notation should then be signed by the interviewing SAs. Such refusal and the surrounding circumstances should be documented on an accompanying MOA.

If the interviewee or their representative requests a copy of the statement, it should be provided only after the statement has been completed, signed and properly witnessed.

Other circumstances such as deafness or physical impairments may require the agent to take extra measures (e.g. interpreter, sign language expert, etc.) to assure the person acknowledges the correctness of the statement.

CHAPTER 9.0 - EXHIBITS

Exhibit 9-1, INV Form 13, Personal History Information

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

PERSONAL HISTORY INFORMATION

Case Number:_____

Personal

Subject Name:				Armed & Dangerous:		
Alias/Nickname:				Alias/Nickname:		
Sex:	Race:	Eyes:	Hair:	Height: (FT;IN)		Weight:
DOB:		Est. Age:		POB:		
Scars:				Tattoos:		
Physical Deformity:				Speech/Accent:		
SSN:				Drivers License (State/No.):		
FBI No:				State/Local Police No.:		
State/Local Police No.:				State/Local Police No.:		
Military Service Branch:				Duty Dates:	Discharge Type:	
Military Service No.:				Misc. No.:		
INS Alien No.:				Passport No.:		
Education:						

Residence & Vehicle

Primary Address:		
Secondary Address:		
Primary Telephone:	Secondary Telephone:	
Vehicle:	Tag No.:	State:
Vehicle:	Tag No.:	State:

Employment & Financial

Occupation(s):	Skills:
Employer Name:	Telephone:
Address:	
Supervisor's Name:	Duties Performed:
Employer Name:	Telephone:
Address:	
Supervisor's Name:	Duties Performed:
Bank or Credit Card Name:	Account No.:
Bank or Credit Card Name:	Account No.:
Bank or Credit Card Name:	Account No.:

INV FORM-13 Rev. April 2015

PERSONAL HISTORY INFORMATION

Relatives and/or Associates

Relationship	Name	Address	Telephone

Additional Information: _____

_____

_____

_____

Handwriting Date: _____ Photograph Date: _____ Fingerprints Date: _____

Date of NCIC/State Wanted Check: _____ Results: _____

_____

_____

Special Agent (*Signature*): _____ Date: _____

Exhibit 9-2, INV Form 17, Disclosure Warning for Bargaining Unit Employees

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Disclosure Warning for Bargaining Unit Employees

"WARNING NOT TO DISCLOSE INVESTIGATIVE INFORMATION"

You are being interviewed as part of a continuing, official investigation by the U.S. Department of Homeland Security, Office of Inspector General. As this investigation involves a sensitive matter, you are instructed not to discuss the nature or substance of this interview, or the existence of this investigation with any other person(s), except private legal counsel, or your union representative, if you have one.

Failure to comply with this directive could subject you to disciplinary and/or criminal action for interfering with or impeding an official investigation.

This advisement was made prior to the interview of _____ (employee's name) on _____(month, day, year) at _____(time, a.m./p.m.).

I have read and understand this warning.

_____(signature) Date:_____
Employee

_____(print name)

_____ (signature) Date:_____
Special Agent
Department of Homeland Security
Office of Inspector General

_____(print name) Date:_____

_____ (signature)
Witness

Disclosure Warning for Bargaining Unit Employees
INV Form-17 (6/13)

Exhibit 9-2A, INV Form 18, Disclosure Warning for Non-Bargaining Unit Employees

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Disclosure Warning for Non-Bargaining Unit Employees

"WARNING NOT TO DISCLOSE INVESTIGATIVE INFORMATION"

You are being interviewed as part of a continuing, official investigation by the U.S. Department of Homeland Security, Office of Inspector General. As this investigation involves a sensitive matter, you are instructed not to discuss the nature of this interview with any other person(s), except private legal counsel.

Failure to comply with this directive could subject you to disciplinary and/or criminal action for interfering with or impeding an official investigation.

I, _____, have read and understand the above warning.
(Print Name)

_____(signature) Date:_____
Employee

_____ (print name) Date:_____
Special Agent

_____ (signature)
Special Agent
Department of Homeland Security
Office of Inspector General

_____ (print name) Date:_____

_____ (signature)
Witness

Disclosure Warning for Non-Bargaining Unit Employees
INV Form-18 (6/13)

Exhibit 9-2B, INV Form 19, Disclosure Warning for Union Representative

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

Department of Homeland Security Office of Inspector General

Verbal Disclosure Warning for Union Representative

"WARNING TO NOT DISCLOSE INVESTIGATIVE INFORMATION"

You are acting as a Union Representative in connection with an interview of an Agency employee as part of a continuing, official investigation being conducted by the U.S. Department of Homeland Security, Office of Inspector General.

As this investigation is sensitive in nature, you are instructed not to discuss the nature of this interview with any other person(s), except the person being interviewed and with other union officials who are not parties of this investigation, and only as may be required to perform your representational duties.

A party to the investigation is an individual who has been identified as either a witness or the subject of the investigation.

Failure to comply with this directive could subject you to disciplinary and/or criminal action for interfering or impeding an official investigation.

This advisement was made to _____(name of union representative), prior to the interview of _____(name of employee), which was conducted on _____(month, day, year) at _____(time, a.m./p.m.).

_____ (signature) Date:_____
Union Representative

_____(print name) Date:_____

_____ (signature)
Special Agent
Department of Homeland Security
Office of Inspector General

_____ (print name) Date:_____

_____ (signature)
Witness

Exhibit 9-3, INV Form 71A, Report Regarding Covert Recording of Non-Custodial Interview in a State Requiring Consent by More Than One Party

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

REPORT REGARDING COVERT RECORDING OF NON-CUSTODIAL INTERVIEW IN A STATE REQUIRING CONSENT BY MORE THAN ONE PARTY

TO: Special Agent in Charge

FROM:

SUBJECT: **Request for Approval to Covertly Record a Non-Custodial Interview in a State Requiring Consent by More Than One Party**

Case Number:_____

Title:_____

Case Agent:_____

Authorization Official:(SAC) _____ (Date) _____

OIG Counsel Approval By: _____ (Date) _____
Requests for Counsel review should be addressed to the Counsel to the IG (b) (6) @oig.dhs.gov) with a copy to OC's Administrative Officer (b) (6) @oig.dhs.gov)

Location of Interview: _____

_____

Name(s) of Individual(s) Recorded:

_____

_____

Investigative Benefits Derived:

INV FORM-71A

Exhibit 9-4, INV Form 28, Sworn Statement – Handwritten

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

SWORN STATEMENT

Date/Time: _____ Location: _____

County of: _____ State of: _____

I, _____, hereby make the following sworn statement to _____, who has identified himself/herself to me as a Special Agent with the U.S. Department of Homeland Security, Office of Inspector General. No promises or threats have been made to me.

SWORN STATEMENT

INV FORM-28 September 2011 Page _____ of _____ Initials:_____

SWORN STATEMENT

STATEMENT OF: _____

I have read this statement of _____ pages. It is true, accurate, and complete to the best of my knowledge and belief. I have been given an opportunity to make any corrections, additions, or deletions.

_____
(Signature)

Subscribed and sworn (or affirmed) to before me this _____ day of
_____ (Month), _____ (Year), at _____ (City), _____ (State).

_____
Special Agent
U.S. Department of Homeland Security
Office of Inspector General
Office of Investigations

_____
(Witness's Signature)

INV FORM-28 April 2015 Page _____ of _____

Exhibit 9-5, INV FORM-28S, Sworn Statement Spanish –Handwritten

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

DECLARACIÓN JURADA

Fecha / Hora: _____ Localización: _____

Condado: _____ Estado: _____

Yo, _____ , le hago la siguiente declaración jurada a _____ , quien se a identificado como un(a) Agente Especial con el Departamento de Seguridad Nacional, Oficina del Inspector General. No me han hecho promesas ni amenazas.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

INV FORM-28S September 2011 Página _____ de _____ Iniciales: _____

DECLARACIÓN JURADA

INV FORM-28S September 2011 Página _____ de _____ Iniciales: _____

DECLARACIÓN JURADA

Declaración de _____

Yo he leído esta declaración que consiste de _____ páginas. Contiene la verdad, es precisa y completa a mi mejor saber y entender. Me han dado la oportunidad de hacerle rectificaciones, adiciones y deleciones.

_____
(Firma del declarante)

Jurada y firmada delante mi este _____ día de _____ del _____, en

_____, _____.

_____
Agente Especial
Departamento De Seguridad Nacional
Oficina del Inspector General
Oficina de Investigaciones

_____
(Firma de Testigo)

INV FORM-288 September 2011 Página_____ de _____

10.0 SUBJECT INTERVIEWS

The instructions specified in sections 10.1 through 10.8 may not apply to CBP employees represented by the National Treasury Employees Union (NTEU). See section 10.9 for special procedures for CBP members of the NTEU.

10.1 SUBJECT INTERVIEWS

All employee subjects, in non-custodial settings, will initially be provided with a Garrity warning, as specified on the "Federal Employee Warning Form" INV Form 27 **(Exhibit 10-3)**. If the subject refuses to be interviewed after having been advised of his/her rights under Garrity, and there is no foreseeable criminal exposure (as determined by the SAC or ASAC of the investigating office) or declination from the Department of Justice has been obtained, the interviewing agent may give a Kalkines Warning. Kalkines warnings will be given using INV Form 26 (revised 6/13), "Advice of Rights (Kalkines)."

The subject interview will be documented on an MOA. (Chapter 12.4) Generally, written statements or affidavits will be requested from the subject of the investigation. (Chapter 9.7) The MOA detailing the interview of a subject will indicate what form of rights advisement was provided and what affirmative verbal or written waiver was given.

10.2 DHS EMPLOYEES

DHS employees are generally required to assist investigators in the performance of their official duties. The employee can be compelled to cooperate under the Inspector General Act, 5 U.S.C.A. App. 3, as amended. Cooperation is also required under the DHS Management Directive # 0810.1 and the Secretary's April 8, 2008, memorandum on cooperation with the OIG. **(Exhibit 2-11)**

Section 5 of the directive and the Secretary's memorandum state, in part, that DHS employees and management will:

- Cooperate fully by disclosing complete and accurate information pertaining to matters under OIG review.
- In response to a specific OIG inquiry, inform OIG personnel of any areas or activities they believe require special attention.
- Not conceal information or obstruct audits, inspections, investigations, or other inquiries being conducted by the OIG.

- Be subject to criminal prosecution and disciplinary action, up to and including removal, for knowingly and willfully furnishing false or misleading information to OIG officials.

- Be subject to disciplinary action for refusing to provide information or answer questions posed by OIG officials if questioned on a matter that may lead only to an administrative action (as distinct from a criminal prosecution).

- Honor OIG requests for interviews with program officials in a timely manner.

- Respect employees' rights to speak directly and confidentially with the OIG in accordance with legal requirements.

- Refrain from inappropriate activity that might inhibit or chill an employee or contractor's communication or cooperation with the OIG.

The effect of these authorities is that a DHS employee who has no foreseeable criminal exposure or has received immunity from prosecution can be compelled to cooperate with OIG. When compelling a subject to cooperate a Kalkines warning will be given and documented using INV Form 26, Advice of Rights (Kalkines).

If a DHS employee with no foreseeable criminal exposure refuses to cooperate in an official investigation, the SA will advise the employee of the standards of conduct requirement as noted above. If the employee still refuses to cooperate, the immediate supervisor of the employee should be requested to order the employee to cooperate. If these measures do not result in the cooperation of the employee, the matter should be reported to the SAC who may contact higher officials at the employing agency/bureau.

Generally, a DHS employee who has foreseeable criminal exposure will not be compelled under the Standards of Conduct to cooperate in an investigation. Any compelled statement obtained would not be admissible in a criminal proceeding against the employee.

When an interview develops into a situation in which the employee may have foreseeable criminal exposure, the SA should stop the interview and issue a Miranda or Garrity warning before continuing with questioning.

The DHS component, not the OIG, takes administrative action against employees. SAs should not suggest that the OIG will discipline or recommend discipline of the affected employee. The OIG merely reports investigative findings including failure to cooperate.

10.3 CUSTODIAL VS. NON-CUSTODIAL DEFINED

A custodial interview is primarily one in which the subject believes that their movement has been restricted. Examples of custodial interviews include voluntary or non-voluntary post arrest interviews, interviews within jail or other confinement facilities, or interviews in any other environment where subjects are likely to reasonably believe that they have been arrested or are not free to leave the premises.

A non-custodial interview is one conducted in a non-coercive environment in which the subject understands that they are not under arrest and are free to terminate the interview and leave the place of interview at any time.

10.4 CUSTODIAL SITUATIONS (MIRANDA WARNINGS)

The United States Supreme Court held in Miranda v. Arizona, 384 U.S. 436 (1966), that the prosecution may not use statements stemming from "custodial interrogation" of a subject unless, prior to questioning, the subject was informed of the following:

- The right to remain silent.
- That anything they say can be used against them in a court or other proceeding.
- The right to consult an attorney for advice before making any statement or answering any questions and have the attorney present during questioning.
- The right to have an attorney appointed by the U.S. Magistrate or the Court to represent them if they cannot afford or otherwise attain one.
- The right to stop the questioning at any time.

SAs should be familiar with what might be considered custodial interrogations and should take measures to assure that evidence obtained under such circumstances is not excluded (i.e., give the warning or make it absolutely clear to the subject that they are not in custody).

In determining whether an individual is "in custody" for purposes of Miranda, a "reasonable person" test is used (i.e., how a reasonable person in the subject's position would have understood the situation). For example:

> Courts have held that the questioning of a subject in a government vehicle constitutes "custodial interrogation."
>
> Questioning of a subject being detained by another law enforcement agency at the scene of a raid should be treated as a "custodial interrogation."

Under Howes v. Fields, 132 S. Ct. 1181 (2012) a person already imprisoned is not necessarily entitled to a Miranda warning if interviewed by law enforcement on a different crime. SAs should consult with a prosecutor prior to interviewing detained subjects without giving Miranda warnings.

An "Advice of Rights (Miranda)" form, INV Form 25 **(Exhibit 10-1),** will be completed by the subject(s) to certify that they read, understood, and waived their rights. The Spanish version of Miranda is also available, INV Form 25S **(Exhibit 10-2)**.

10.5 CUSTODIAL SITUATIONS FOR FOREIGN NATIONALS

When foreign nationals are arrested or detained, they must be advised of the right to have their consular officials notified pursuant to the 1963 Vienna Convention on Consular Relations (VCCR). Detained foreign nationals will be provided with a Consular Notification Form (INV Form 99 or INV Form 100: Exhibits 10-8 and 10-9) commensurate with the obligation to contact the country of citizenship.

If the foreign national is a citizen of one of the below listed countries, it is mandatory that the SA notify, by telephone or fax, the nearest consular official immediately, and in any event within four days of the arrest or detention, regardless of the foreign national's wishes. Additional information can be obtained by calling the State Department Operations Center at 202-647-1512 or Email: consnot@state.gov.

Albania
Algeria
Antigua and Barbuda
Armenia
Azerbaijan
Bahamas
Barbados
Belarus
Belize
Brunei
Bulgaria
China (including Macao and Hong Kong)[1]
Costa Rica
Cyprus
Czech Republic
Dominica
Fiji
Gambia
Georgia
Ghana
Grenada
Guyana
Hungary
Jamaica
Kazakhstan
Kiribati
Kuwait
Kyrgyzstan
Malaysia
Malta
Mauritius
Moldova
Mongolia
Nigeria
Philippines
Poland
Romania
Russia
Saint Kitts and Nevis
Saint Lucia
Saint Vincent and the Grenadines
Seychelles
Sierra Leone
Singapore
Slovakia
Tajikistan
Tanzania
Tonga
Trinidad and Tobago
Tunisia
Turkmenistan
Tuvalu
Ukraine
United Kingdom
Uzbekistan
Zambia
Zimbabwe

Foreign nationals who are from countries subject to mandatory notification will be explained the following (INV Form 99 or INV Form 100):

> Because of your nationality, we are required to notify your country's consular officers here in the United States that you have been arrested or detained. We will do this as soon as possible. In addition, you may communicate with your consular officers. You are not required to accept their assistance, but your consular officers may be able to help you obtain legal representation, and may contact your family and visit you in detention, among other things.

All detained foreign nationals, except those from mandatory notification countries, will be explained the following (INV Form 99 or INV Form 100):

> As a non-U.S. citizen who is being arrested or detained, you may request that we notify your country's consular officers here in the United States of your situation. You may also communicate with your consular officers. A consular officer may be able to help you obtain legal representation, and may contact your family and visit you in detention, among other things. If you want us to notify your consular officers, you can request this notification now, or at any time in the future.

10.6 GARRITY AND KALKINES WARNINGS

A public employee who is being questioned in any proceeding about a matter that could result in a criminal prosecution of him or her may not be subject to disciplinary action solely for invoking the Fifth Amendment privilege and refusing to answer questions or to sign a waiver of immunity.

Any statement given by a public employee based upon a threat of dismissal from their job, if the employee fails to provide such statement, will be inadmissible against the employee in a subsequent criminal proceeding.

The instructions specified below may not apply to CBP employees represented by the National Treasury Employees Union (NTEU). See section 10.9 for special procedures for CBP members of the NTEU.

Garrity

All employee subjects will initially be provided with a Garrity warning, as specified on the "Federal Employee Warning Form" INV Form 27 **(Exhibit 10-3)**. The Garrity warning provides the traditional Miranda safeguards (without offering to appoint an attorney), and also explains that the employee may not be discharged from employment for exercising their Fifth Amendment right to silence.

If the subject exercises his/her right against self-incrimination, or requests an attorney, the interview must be terminated.

Kalkines

The Kalkines warning is a means of requiring an employee to make a statement concerning their knowledge or involvement in a matter under investigation. Under Kalkines, the employee is afforded immunity from prosecution for a specified offense and any statement made by the employee may not be used as against them in a criminal proceeding.

In doing so, the OIG asserts its right to require the employee to explain their knowledge or involvement or face disciplinary action. In addition, the statement itself may be used in an administrative action against the employee, and the employee can still be prosecuted for providing a false statement.

Before Kalkines warnings are issued, the SAC or ASAC of the investigating office must determine that the subject has no foreseeable criminal exposure in the matter being discussed at interview or obtain a declination from a prosecutor.

The SA will give the “Kalkines” warnings to the employee prior to questioning using INV Form 26 (revised 05/08), "Advice of Rights (Kalkines).” A space on the form is provided in which the SAs must describe in detail the alleged criminal activity that has been declined for prosecution. **(Exhibit 10-4)**

SAs are reminded that if an interview where Kalkines has been given develops into a situation in which the employee may have foreseeable criminal exposure, the SA should stop the interview and issue a Miranda or Garrity warning before continuing with questioning.

10.7 WARNING AND ADVISEMENT TABLE

It is beyond the scope of this manual to list and explain every circumstance and condition under which the advisement of rights comes into play. However, the following general guidelines will apply.

Situation	Minimum Requirement
Subject is in custody or under arrest and is a non-employee.	Miranda rights required. (INV Form 25)
Subject is in custody or under arrest and is an employee.	Miranda rights required. (INV Form 25)
Subject is not in custody and is not a DHS employee.	No warning required.
Subject is in custody on a matter other than what you are investigating, is an employee, and has foreseeable criminal exposure in your investigation	Garrity warning (INV Form 25) required. Miranda rights (INV Form 27) required unless SAs receive authorization from a prosecutor. Howes v. Fields, 132 S. Ct. 1181 (2012)
Subject is not in custody but is a DHS employee and has foreseeable criminal exposure.	Garrity warning is required. (INV Form 27)
Subject is a DHS employee and the SAC or ASAC of the investigating office has determined no foreseeable criminal exposure in the matter being discussed exists.	Garrity warnings are given, but if the subject refuses to be interviewed then interviewing agent can compel cooperation using a Kalkines warning.(INV Form 26)
Subject is a CBP employee, not in custody, who is represented by the NTEU	Follow the requirements specified in section 10.9

10.8 EMPLOYEE'S RIGHT TO REPRESENTATION

The instructions specified below may not apply to CBP employees represented by the National Treasury Employees Union (NTEU). See section 10.9 for special procedures for CBP members of the NTEU.

Attorney Representation

An employee under investigation for a criminal or administrative matter is allowed to have an attorney before answering any questions. In an administrative matter, an attorney is present only as an observer to the interview and may not participate in the interview directly.

Union Representation - Weingarten

5 U.S.C. § 7114(a) (2) (B) provides federal employees in a collective bargaining unit the right to have a union representative with them when they are questioned by agency personnel in certain circumstances. This right is a codification on the holding in NLRB v. J. Weingarten, Inc., 420 U.S. 251 (1975).

On June 17, 1999, the Supreme Court decided in NASA v. FLRA, 119 S.Ct. 1979, 1999 U.S. LEXIS 4190, that OIG investigators are representatives of the agency for purposes

of the statutory Weingarten right and 5 U.S.C. § 7114(a)(2)(B) applies to an interview conducted by the OIG SA.

The policy of INV is that all interviews conducted by SAs are pursuant to the Inspector General Act and are subject to the Weingarten statute at 5 U.S.C. § 7114(a)(B), which allows employees to have a union representative with them when they are questioned and reasonably believe that the questioning may lead to disciplinary action. This is regardless of whether the interviews are conducted for criminal or administrative purposes. Generally, union representatives should be allowed to be present in interviews of employees conducted by SAs.

All OIG interviews of DHS bargaining unit employees (except TSA) are subject to the requirement to provide Weingarten rights when requested and if disciplinary action could result from investigative findings. The requirement applies to both criminal and administrative cases. In such instances, the SA must either allow a union representative to be present, terminate the interview, or provide the employee the choice of being interviewed without union representation. Prior to the commencement of the interview, SAs will complete INV Form 15, Union Representative Advisory. **(Exhibit 10-5)**

Currently, there is no requirement for OIG SAs to affirmatively advise the employee before the start of the interview of the right to request union representation. Only one employee representative will be permitted in the interview. 5 U.S.C. § 7114(a) (3) requires agencies to annually advise all employees of this right. OIG SAs should liberally interpret the concept of an employee request.

While employees can request a particular representative, no undue delay is required in order to have a particular representative become available. When the union representative is a witness or subject of an inquiry, consultation with IG Counsel is necessary in order to evaluate all the circumstances of the case to determine how the prevailing law will apply.

The union representative is entitled to confer with the employee, and to ask the SA clarifying questions. However, the representative is not in charge of the interview and may not answer for the employee. Interference or efforts to answer for the employee will not be tolerated. The case law clearly establishes the SA's right to hear the employee's own account regarding the matters at issue.

Union representatives who exceed their appropriate role should be asked to desist. Refusal will justify the termination of the union representative's participation in the interview and the employee will be advised of their right to continue the interview without the representative or, forego the interview until another union representative is available. In such cases, the circumstances should be documented and an acknowledgement obtained from the employee of his receipt and understanding of these options on INV Form 16, Union Advisory to Employee, **(Exhibit 10-6)**.

10.9 SPECIAL PROCEDURES FOR CBP MEMBERS OF THE NTEU (CBP/NTEU EMPLOYEES)

The Federal Labor Relations Authority (FLRA) ruled that terms of a collective bargaining agreement negotiated between CBP and the NTEU apply to OIG investigations. Article 22 of the agreement, "Investigations" requires DHS OIG to follow different procedures and use different forms for CBP/NTEU employees.

Article 22 only applies to CBP employees who are members of NTEU. It does *not* apply to:

- Border Patrol employees assigned to Border Patrol Sectors (members of the National Border Patrol Council, an AFGE union); or
- Employees of the Office of Chief Counsel (DHS OGC employees).
- TSA employees.

When the OIG knows in advance that we will interview a CBP/NTEU employee, agents will provide reasonable advance notice to the applicable NTEU Chapter of:

a) when and where the interview will take place;
b) whether it will be audio or video taped; and
c) the general subject matter of the interview.

[redacted]

If the OIG wishes to interview a CBP/NTEU employee who is the subject of an investigation, the employee must be provided with the "General Notice" form, Appendix A-1 of Article 22 (Exhibit 10-10, INV Form 107), informing the employee about the general nature of the matter, i.e. whether criminal or administrative, or both. For any CBP/NTEU employee who may be subject to discipline as a result of our investigation, administer Article 22's "Weingarten Rights" form, Appendix A-2 (Exhibit 10-10, INV Form 108).

If the interviewee is not a subject, provide the "Third Party Witness Interview Notification" form, Appendix A-3 (Exhibit 10-10, INV Form 106). In circumstances in which it is appropriate to administer Miranda, Garrity, or Kalkines (Article 22 uses the term "Beckwith" instead of "Garrity") warnings, for CBP/NTEU employees use the forms in Exhibit 10-10: "Appendix A-4, Miranda Rights" (INV Form 109); Appendix A-5, "Beckwith Rights" (INV Form 110); and Appendix A-6, "Kalkines Rights" (INV Form 111).

Unlike interviews of bargaining unit employees in unions other than CBP employee members of NTEU, there are no non-disclosure forms for union employees or representatives. Instead, OIG agents may **read** the narratives included in Exhibit 10-11 (INV Form 112) which contain non-disclosure warnings to CBP/NTEU employees and their representatives.

10.10 MILITARY SUBJECTS

Military witnesses and subjects should be advised of their rights in accordance with Article 31, Uniform Code of Military Justice (UCMJ). Agents should be sensitive to the voluntariness of situations where a United States Coast Guard (USCG) civilian or military employee is instructed by a military officer/supervisor to submit to an interview by an OIG SA. This scenario raises the question of the voluntariness of the witness since their submission to an interview may be construed as doing so under the orders of the military.

After identification and introduction of subject matter, give advice of rights under Miranda Tempia (Tempia applies the Miranda rules to military personnel), and in accordance with Article 31, UCMJ 10 USC 831(b). INV Form 11, Miranda-Tempia Military **(Exhibit 10-7)**.

10.11 WAIVER OF DISCIPLINARY ACTION

A situation could arise where the affected DHS agency/bureau would be willing to waive disciplinary action against an employee in exchange for a statement from that employee. If the employee has foreseeable criminal exposure and the DOJ is not willing to forgo prosecution, the terms of any such agreement between the employee and the agency should be reduced to writing and should contain the following written disclaimer:

> "Nothing contained herein shall be deemed or construed to affect criminal liability or to limit the responsibility of the Department of Justice to prosecute violation of federal criminal laws. This agreement does not constitute a grant of immunity from criminal prosecution, and its acceptance by (employee's name) shall constitute a knowing and personal waiver of rights under the Fifth Amendment to the United States Constitution."

The employee being interviewed must sign the agreement containing the disclaimer.

In the event that the employee's statement contains evidence reflecting that a criminal violation of federal law has been committed, or in the event that other evidence is developed reflecting such a criminal violation, the signed statement containing the disclaimer shall be forwarded to DOJ when the matter is referred for prosecution.

CHAPTER 10.0 - EXHIBITS

Exhibit 10-1, INV Form 25, Advice of Rights (Miranda)

Office of Inspector General - Investigations
U.S. Department of Homeland Security

Homeland Security

ADVICE OF RIGHTS (MIRANDA)

You have the right to remain silent.

Anything you say can be used against you in a court or other proceeding.

You have the right to consult an attorney for advice before making any statement or answering any questions, and you may have him/her present with you during questioning.

You may have an attorney appointed by the U.S. Magistrate or the court to represent you if you cannot afford or otherwise obtain one.

If you decide to answer questions now, with or without an attorney, you still have the right to stop the questioning at any time.

However, you may waive the right to advice of counsel and your right to remain silent and answer questions or make a statement without consulting an attorney if you so desire.

Do you understand your rights? _____

Do you waive your rights? _____

(Date/Time)	(Location)	(Printed Name)	(Signature)

(Witness' Printed Name)	(Witness' Printed Name)
(Witness' Signature)	(Witness' Signature)
(Date/Time)	(Date/Time)

INV FORM-25

Exhibit 10-2, INV Form 25S, Advice of Rights (Miranda/Spanish)

Oficina del Inspector General – Investigations
Departamento de Seguridad De La Patria

Homeland Security

NOTIFICACION DE LOS DERECHOS "MIRANDA"

NOTIFICACION DE LOS DERECHOS "MIRANDA"
EN LOS CASOS DE CUSTODIOS QUE NO SEAN
EMPLEADOS DEL DEPARTAMENTO

Advertencias y garantías de los custodios

SUS DERECHOS

Antes de que le hagamos cualquier pregunta o de que Usted haga cualquier declaración, debe conocer sus derechos:

- Usted tiene el derecho al silencio y a negarse a responder a las preguntas que se le hagan en cualquier momento.
- Lo que diga o haga puede utilizarse contra Usted en un tribunal o en cualquier otro procedimiento judicial.
- Usted tiene el derecho a consultar con un abogado antes de responder a cualquier pregunta y de estar acompañado de un abogado en cualquier interrogatorio que se le haga ahora o en el futuro.
- Si no puede pagar a un abogado, se le facilitara uno gratuitamente.
- Si decide responder ahora a las preguntas, tiene el derecho a negarse a responder en cualquier momento que lo desee.

He leído esta declaración y entiendo cuáles son mis derechos. Estoy dispuesto a hacer una declaración y a responder a las preguntas. Comprendo y sé lo que estoy haciendo. No me han hecho ninguna promesa ni amenaza, ni nadie me ha hecho presión ni coacción de ninguna forma.

(Fecha/Hora)	(Numero de la causa)	(Nombre escrito)	(Firma del Sujeto)

(Nombre escrito del Testigo)	(Nombre escrito del Testigo)
(Firma del Testigo)	(Firma del Testigo)
(Fecha/Hora)	(Fecha/Hora)

INV FORM-25S

Exhibit 10-3, INV Form 27, Federal Employee Warning Form (Garrity)

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

FEDERAL EMPLOYEE WARNING FORM

This interview is voluntary.

You have the right to remain silent if your answers may incriminate you.

Anything you say may be used against you as evidence both in an administrative proceeding or any future criminal proceeding.

Although you would normally be expected to answer questions regarding your official duties, in this instance you are not required to do so. Your refusal to answer solely on the grounds that your answers may tend to incriminate you, will not subject you to disciplinary action.

I have read the aforementioned and agree to the terms mentioned therein.

_____ (Date/Time)	_____ (Location)
_____ (Printed Name)	_____ (Signature)

_____ (Witness' Printed Name)	_____ (Witness' Printed Name)
_____ (Witness' Signature)	_____ (Witness' Signature)
_____ (Date/Time)	_____ (Date/Time)

Advice of Rights (Beckwith/Garrity)

INV FORM-27 (06/13)

Exhibit 10-4, INV Form 26, Advice of Rights (Kalkines)

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

ADVICE OF RIGHTS (KALKINES)

You are going to be asked a number of specific questions concerning the performance of your official duties as it relates to:

_____

_____

Under the provisions of the Inspector General Act, 5 U.S.C.A. App. 3, as amended, you are required to cooperate fully by disclosing complete and accurate information pertaining to matters under OIG review.

You may be subject to disciplinary action, to include termination, for refusing to provide information or answer questions posed by OIG officials if questioned on a matter that may lead only to an administrative action (as distinct from a criminal prosecution).

You are advised that the answers you provide pertaining to the matter presently under investigation, or any information or evidence which is gained by reason of your answers, cannot and will not be used against you in a criminal proceeding, except that you may be subject to criminal prosecution for any false statements made during this interview.

I have read the aforementioned and agree to the terms mentioned therein.

_____ (Date/Time)	_____ (Location)
_____ (Printed Name)	_____ (Signature)
_____ (Witness' Printed Name)	_____ (Witness' Printed Name)
_____ (Witness' Signature)	_____ (Witness' Signature)
_____ (Date/Time)	_____ (Date/Time)

Advice of Rights (Kalkines)
INV FORM-26 (revised 06/13)

Exhibit 10-5, INV Form 15, Union Representative Advisory

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

UNION REPRESENTATIVE ADVISORY

_____ has requested that you participate as a union representative in an interview being conducted by the U.S. Department of Homeland Security, Office of Inspector General (DHS-OIG). The interview is part of an official investigation being undertaken pursuant to DHS-OIG's authority under the Inspector General Act, as amended, 5 U.S.C.A. App. 3, and the Homeland Security Act of 2002, as amended.

The DHS-OIG is conducting this interview in order to obtain the employee's account of the matters under investigation. The DHS-OIG understands that you are entitled to assist the employee during the course of the interview. In order to facilitate your representation of the employee, you will be afforded a reasonable opportunity to confer with the employee during the course of the interview.

The DHS-OIG expects that you will refrain from any action that would interfere with the DHS-OIG's legitimate interest in achieving the objective of the investigation or would compromise its integrity. The DHS-OIG is interested in obtaining the employee's own account of the matters under investigation. Accordingly, please do not attempt to answer questions on behalf of the employee, dictate the employee's answers to questions asked, or otherwise to take charge of this proceeding. In order to maintain the integrity of this investigation, the DHS-OIG requests that you not reveal to anyone other than another union official assigned to assist you in representing _____in this matter the purpose, any part of the substance of the interview, or the existence of this investigation.

We expect that any disagreement regarding the conduct of this interview or your role as union representative will be resolved amicably during the course of this proceeding. However, in order to avoid an adversarial confrontation and to achieve the objectives of the investigation, the DHS-OIG reserves the right to terminate your participation in the interview and afford the employee the choice of either continuing without your participation or foregoing the interview until another union representative is available.

I, _____ appeared at an official DHS-OIG investigative interview as a union representative and was provided a copy of this Advisory.

_____ _____
Union Representative Date

_____ _____
Special Agent Date
DHS-OIG

Union Representative Advisory
INV FORM-15 (6/13)

Exhibit 10-6, INV Form 16, Union Advisory to Employee

Office of Inspector General - Investigations
U.S. Department of Homeland Security

Homeland Security

UNION ADVISORY TO EMPLOYEE

During an interview undertaken as part of an official Department of Homeland Security, Office of Inspector General (DHS-OIG) investigation, the individual serving as your union representative has been advised that he or she has engaged in activity that has interfered with the DHS-OIG's legitimate interest in achieving the objective of the investigation. In order to avoid an adversarial confrontation and to achieve the objectives of the investigation, you are being afforded the choice of (1) continuing this interview without the participation of your union representative or (2) discontinuing the interview, at this time until another union representative is available.

ACKNOWLEDGMENT

Having read this advisory, I choose to:

_____ continue with the DHS-OIG interview without the participation of a union representative.

_____ forego the opportunity to be interviewed at this time until another union representative is available.

_____ _____
Employee's Signature Date

INV FORM-16

Exhibit 10-7, INV Form 11, Miranda-Tempia Warning, Military Acknowledgment of Rights

Office of Inspector General - Investigations
U.S. Department of Homeland Security

Homeland Security

MIRANDA/TEMPIA WARNINGS

MILITARY ACKNOWLEDGMENT OF RIGHTS

Location: _____

I, _____, have been advised by Special Agent _____ that I am suspected of committing the following offense(s): _____

I UNDERSTAND THAT:

1. I have the right to remain silent. I do not have to make any statement or answer any questions.
2. Before I decide whether or not I want to make a statement or answer any questions, I may consult with a lawyer.
3. If I decide to consult with a lawyer, the interviewer will stop this interview. I may consult with a military lawyer without cost to me if the government intends to continue questioning me. I may also consult with a civilian lawyer at my own expense.
4. If I decide to make a statement, anything I say may be used as evidence against me in any court martial, non-judicial proceeding, administrative proceeding, or civilian court.
5. If the questioning continues, I may stop it at any time by refusing to make further statements or by requesting to consult with a lawyer.
6. I have the right to have a lawyer present during any further questioning.

I HAVE CAREFULLY read the above and I understand what my rights are. Any questions that I have asked concerning my rights have been answered to my complete satisfaction.

_____	_____
Employee's Printed Name	Witness' Printed Name
_____	_____
Employee's Signature	Witness' Signature
_____	_____
Date and Time	Date and Time

INV FORM-11

Exhibit 10-8, INV Form 99, Consular Notification (English)

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

CONSULAR NOTIFICATION (English)

Statement 1: For All Foreign Nationals Except Those from "Mandatory Notification" Countries

As a non-U.S. citizen who is being arrested or detained, you may request that we notify your country's consular officers here in the United States of your situation. You may also communicate with your consular officers. A consular officer may be able to help you obtain legal representation, and may contact your family and visit you in detention, among other things. If you want us to notify your consular officers, you can request this notification now, or at any time in the future.

Do you want us to notify your consular officers at this time? Yes/No _____

Name: _____ (Printed Name) Signature: _____

Date: _____ Witness: _____

Statement 2: For Foreign Nationals from "Mandatory Notification" Countries

Because of your nationality, we are required to notify your country's consular officers here in the United States that you have been arrested or detained. We will do this as soon as possible. In addition, you may communicate with your consular officers. You are not required to accept their assistance, but your consular officers may be able to help you obtain legal representation, and may contact your family and visit you in detention, among other things.

Please sign to show that you have received this information.

Name: _____ (Printed Name) Signature: _____

Date: _____ Witness: _____

Consular Notification (English)
INV FORM-99 (6/13)

Exhibit 10-9, INV Form 100, Consular Notification (Spanish)

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

CONSULAR NOTIFICATION (Spanish)

Statement 1: For All Foreign Nationals Except Those from "Mandatory Notification" Countries

Por no ser ciudadano de los Estados Unidos, y estar arrestado o detenido, usted puede pedirnos que notifiquemos de su situación a los funcionarios consulares de su país en los Estados Unidos. También puede comunicarse con los funcionarios consulares de su país. Entre otras cosas, un funcionario consular de su país puede ayudarle a conseguir asesoramiento legal, y también puede ponerse en contacto con su familia y visitarle en el lugar de detención. Si usted desea que notifiquemos a los funcionarios consulares de su país, puede solicitarlo ahora o en cualquier oportunidad en el futuro.

¿Desea que notifiquemos ahora a los funcionarios consulares de su país? _____ Si (Yes) _____ No (No)

Nombre: _____ (Printed Name) Firma: _____ (Signature)

Fecha: _____ (Date) Testigo: _____ (Witness)

Statement 2: For Foreign Nationals from "Mandatory Notification" Countries

Debido a su nacionalidad, estamos obligados a notificar a los funcionarios consulares de su país en los Estados Unidos que usted h sido arrestado o detenido. Haremos esta notificación lo más pronto posible. Además, usted puede comunicarse con los funcionarios consulares de su país. Usted no está obligado a aceptar su ayuda, pero esos funcionarios pueden ayudarle, entre otras cosas, a conseguir asesoramiento legal, y también pueden ponerse en contacto con su familia y visitarle en el lugar de detención.

Sírvase firmar para indicar que ha recibido esta información.

Nombre: _____ (Printed Name) Firma: _____ (Signature)

Fecha: _____ (Date) Testigo: _____ (Witness)

Consular Notification (Spanish)
INV FORM-100 (6/13)

Exhibit 10-10, NTEU Advisements: General Notice, INV Form 107

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

GENERAL NOTICE

Article 22 Federal Labor Relations Authority agreement CBP and NTEU

Appendix A-1

I am investigating the alleged _____ (theft, misuse, loss, etc.). You,

_____, are the subject of the investigation concerning this matter.
(Employee Name)

One of the following must be checked.

___ The general nature of this matter is criminal.

___ The general nature of this matter is administrative.

One of the following must be checked.

___ This interview is related to possible criminal misconduct by you.

___ This interview is not related to possible criminal misconduct by you.

_____ _____
Employee's initials Date

General Notice - NTEU
INV FORM-107 (6/13)

Exhibit 10-10, NTEU Advisements: Weingarten Rights, INV Form 108

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

WEINGARTEN RIGHTS

Article 22 Federal Labor Relations Authority agreement CBP and NTEU

Appendix A-2

EMPLOYEE NOTIFICATION REGARDING UNION REPRESENTATION

Pursuant to 5 USC §7114(a)(2)(B) you have the right to be represented during the interview about to take place by a person designated by the exclusively recognized labor organization for the unit in which you work, if,

(a) you reasonably believe that the results of this interview may result in disciplinary action against you; and

(b) you request representation.

I acknowledge receipt of the aforementioned notification of my right to representation.

_____ _____
Signature of Employee Date

Weingarten Rights - NTEU
INV FORM-108 (6/13)

Exhibit 10-10, NTEU Advisements: Third Party Notification, INV Form 106

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

THIRD PARTY WITNESS INTERVIEW NOTIFICATION

Article 22 Federal Labor Relations Authority agreement CBP and NTEU

Appendix A-3

You are not currently the subject of this investigation. However, you may be held responsible for any false statements you make or for any violation of the CBP Code of Conduct that you admit. Therefore, if at any time during the interview you reasonably believe that you may be subjected to discipline as a result of your statements, you may request representation by the exclusively recognized labor organization for the unit in which you work.

I acknowledge receipt of the aforementioned notification of my rights.

_____ _____
Signature of Employee Date

Third Party Notification - NTEU
INV FORM-106 (6/13)

Exhibit 10-10, NTEU Advisements: Miranda Rights, INV Form 109

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

MIRANDA RIGHTS

Article 22 Federal Labor Relations Authority agreement CBP and NTEU

Appendix A-4

WAIVER OF RIGHT TO REMAIN SILENT AND OF RIGHT TO ADVICE OF COUNSEL

STATEMENT OF RIGHTS

- Before we ask you any questions, it is my duty to advise you of your rights.
- You have the right to remain silent.
- Anything you say can be used against you in court, or other proceedings.
- You have the right to consult an attorney before making any statement or answering any question, and you may have him present with you during questioning.
- You may have an attorney appointed by the U.S. Magistrate or the court to represent you if you cannot afford or otherwise obtain one.
- If you decide to answer questions now with or without a lawyer, you still have the right to stop the questioning at any time, or to stop the questioning for the purpose of consulting a lawyer.

However, you may waive the right to advice of counsel and your right to remain silent, and you may answer questions or make a statement without consulting a lawyer if you so desire.

WAIVER

I have had the above statements of my rights read and explained to me and fully understanding these rights I waive them freely and voluntarily, without threat or intimidation and without any promise of reward or immunity. I was taken into custody at _____ (time), on _____ (date), and have signed this document at _____ (time), on _____ (date).

_____
(name)

WITNESSES:

_____ _____
(name) (name)

Miranda Rights - NTEU
INV FORM-109 (6/13)

Exhibit 10-10, NTEU Advisements: Beckwith Rights, INV Form 110

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

BECKWITH RIGHTS

Article 22 Federal Labor Relations Authority agreement CBP and NTEU

Appendix A-5

You have the right to remain silent if your answers may tend to incriminate you.

Anything you say may be used as evidence later in an administrative proceeding or any future criminal proceeding involving you.

If you refuse to answer the questions posed to you on the grounds that the answers may tend to incriminate you, you cannot be discharged solely for remaining silent. However, your silence can be considered in an administrative proceeding for its evidentiary value that is warranted by the facts surrounding your case.

I have been given the above warning at the beginning of the interview held on _____.

_____ _____
Signature of Employee Date

Beckwith Rights - NTEU
INV FORM-110 (6/13)

Exhibit 10-10, NTEU Advisements: Kalkines Rights, INV Form 111

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

KALKINES RIGHTS

Article 22 Federal Labor Relations Authority agreement CBP and NTEU

Appendix A-6

Statement of Rights and Obligations

Before we ask you any questions, it is my obligation to inform you of the following:

You are here to be asked questions pertaining to your employment with CBP and the duties that you perform for CBP. You have the option to remain silent, although you may be subject to removal from your employment by the Service if you fail to answer material and relevant questions relating to the performance of your duties as an employee. You are further advised that the answers you may give to the questions propounded to you at this interview, or any information or evidence which is gained by reason of your answers, may not be used against you in a criminal proceeding except that you may be subject to a criminal prosecution for any false answer that you may give.

****

Receipt by Employee

I have been given the above Statement of Rights and Obligations at the beginning of the interview held on _____.

_____ _____
Signature of Employee Date

Kalkines Rights - NTEU
INV FORM-111 (6/13)

Exhibit 10-11, NTEU Non-Disclosure Statements, INV Form 112

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

NON-DISCLOSURE

Article 22 Federal Labor Relations Authority agreement CBP and NTEU

Narrative for CBP/NTEU employees—*not* for hard copy distribution:

If union representation is allowable and the employee opts for representation, Agents may ***read*** the following to the union employee at the interview. Do not provide this language in written form.

> You are being interviewed as part of a continuing, official investigation by the U.S. Department of Homeland Security, Office of Inspector General. As this investigation involves a sensitive matter, you are instructed not to discuss the nature or substance of this interview, or the existence of this investigation with any other person or persons, except private legal counsel, your union representative, or another union official assigned to assist your representative in this matter. Failure to comply with this directive could subject you to disciplinary and/or criminal action for interfering with or impeding an official investigation.

Narrative for CBP/NTEU union representatives—(*not* for hard copy distribution):

If union representation is appropriate and is requested, Agents may ***read*** any or all of the following four paragraphs to the union representative. Do not put provide this language in written form. The third paragraph contains non-disclosure language.

> A DHS employee has requested that you participate as a union representative in an interview being conducted by the U.S. Department of Homeland Security, Office of Inspector General (DHS-OIG). The interview is part of an official investigation being undertaken pursuant to DHS-OIG's authority under the Inspector General Act, as amended, 5 U.S.C.A. App. 3, and the Homeland Security Act of 2002, as amended.
>
> The DHS-OIG is conducting this interview in order to obtain the employee's account of the matters under investigation. The DHS-OIG understands that you are entitled to assist the employee during the course of the interview. In order to facilitate your representation of the employee, you will be afforded a reasonable opportunity to confer with the employee during the course of the interview.
>
> The DHS-OIG expects that you will refrain from any action that would interfere with the DHS-OIG's legitimate interest in achieving the objective of the investigation or would compromise its integrity. The DHS-OIG is interested in obtaining the employee's own account of the matters under investigation. Accordingly, please do not attempt to answer questions on behalf of the employee, dictate the employee's answers to questions asked, or otherwise to take charge of this proceeding. In order to maintain the integrity of this investigation, the DHS-OIG requests that you not reveal to anyone other than another union official assigned to assist you in representing the employee in this matter the purpose or any part of the substance of the interview, or the existence of this investigation.

Non-Disclosure - NTEU
INV FORM-112 (6/13)

Exhibit 10-11, NTEU Non-Disclosure Statements, INV Form 112 page 2

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

We expect that any disagreement regarding the conduct of this interview or your role as union representative will be resolved amicably during the course of this proceeding. However, in order to avoid an adversarial confrontation and to achieve the objectives of the investigation, the DHS-OIG reserves the right to terminate your participation in the interview and afford the employee the choice of either continuing without your participation or foregoing the interview until another union representative is available.

Non-Disclosure - NTEU
INV FORM-112 (6/13)

(b) (7)(D) [redacted]

[redacted]

(b) (7)(D) [redacted]

F. (b) (7)(D)

(b) (7)(D)

(b) (7)(D)

sphere of activities or high significance to DHS OIG's national objectives, even if the

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D) [redacted]

F. *Use by DHS OIG Only*: (b) (7)(D) [redacted]

(b) (7)(D) [redacted]

1. (b) (7)(D) [redacted]

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

6.

(b) (7)(D)

1. (b) (7)(D) [redacted]

(b) (7)(D) [redacted]

(b) (7)(D) [redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

(b) (7) (D)

(b) (7)(D)

[redacted]

(b) (7) (D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

[redacted]

(b) (7) (D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

G. (b) (7)(D)

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

(b) (7)(D) [redacted]

(b) (7)(D) [redacted]

(b) (7)(D) [redacted]

(b) (7)(D) [redacted]

(b) (7)(D) [redacted]

(b) (7)(D) [redacted]

(b) (7)(D) [redacted]

(b) (7)(D) [redacted]

(b) (7)(D) [redacted]

(b) (7)(D) [redacted]

(b) (7)(D) [redacted]

(b) (7)(D) [redacted]

(b) (7)(D) [redacted]

(b) (7)(D) [redacted]

(b) (7)(D)	
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

(b) (7)(D) [redacted]

(b) (7)(D) [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

(b) (7)(D)

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

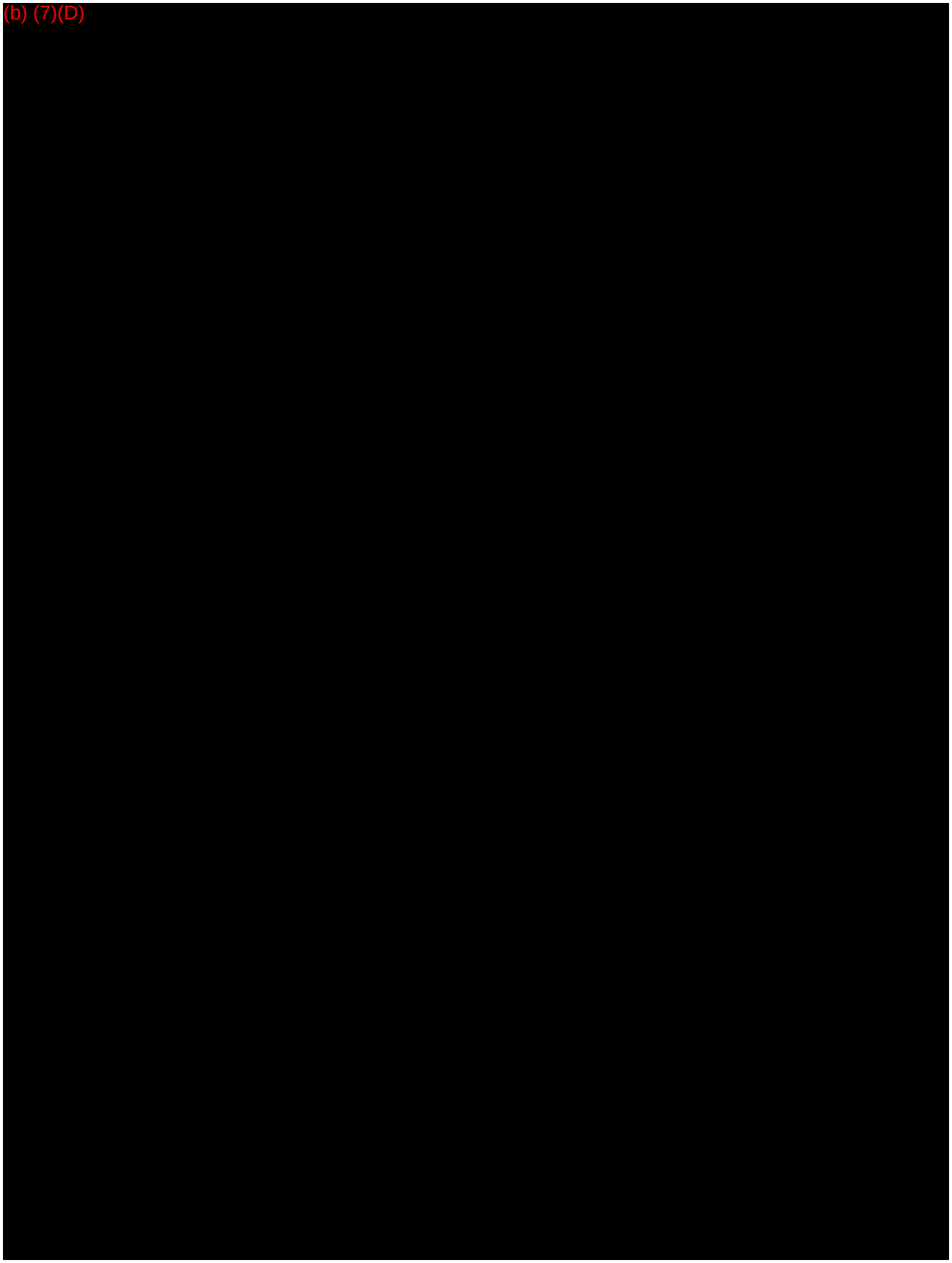
[redacted] (b) (7)(D)

(b) (7)(D)

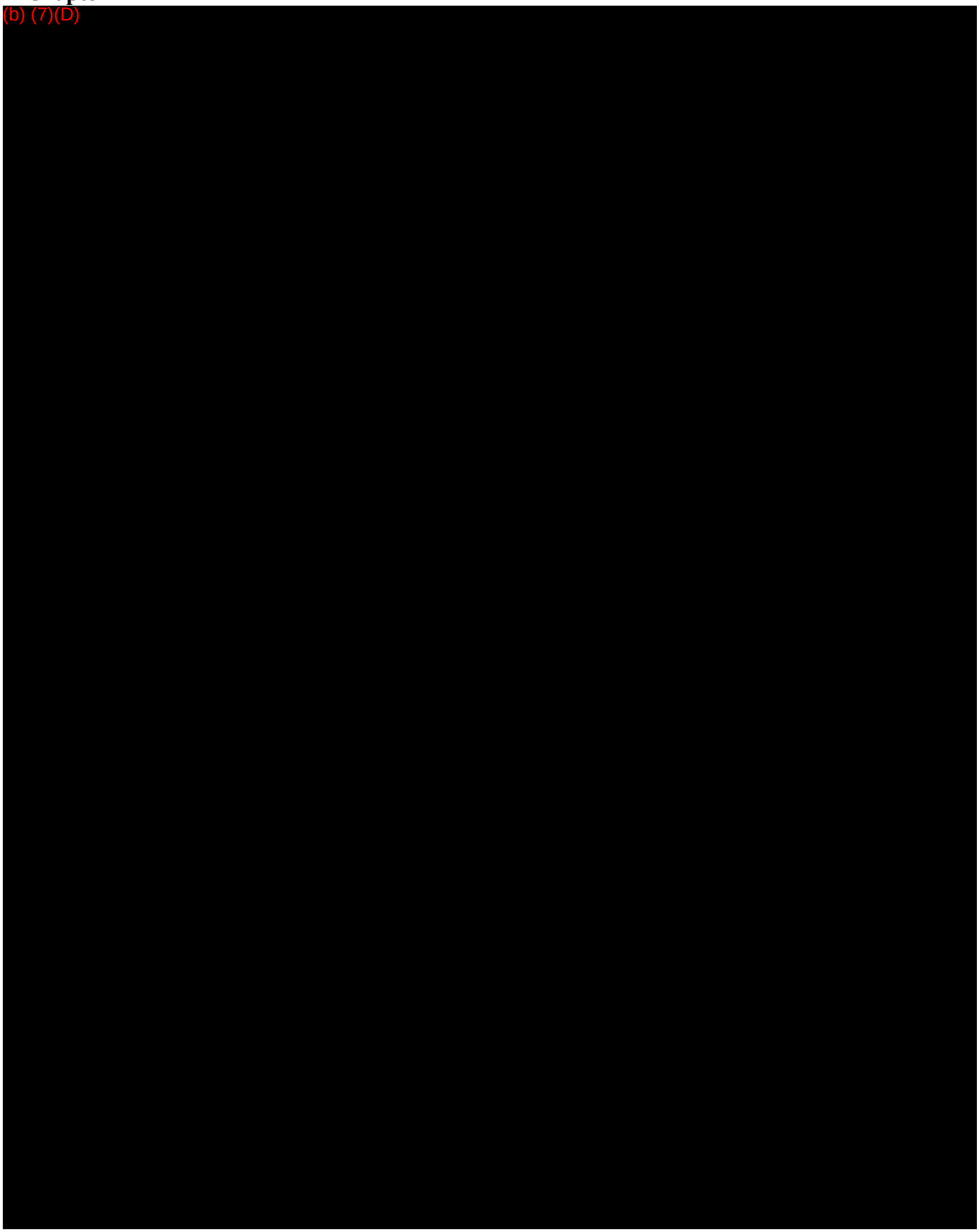
[redacted]

(b) (7)(D)

(b) (7)(D)



(b) (7)(D)



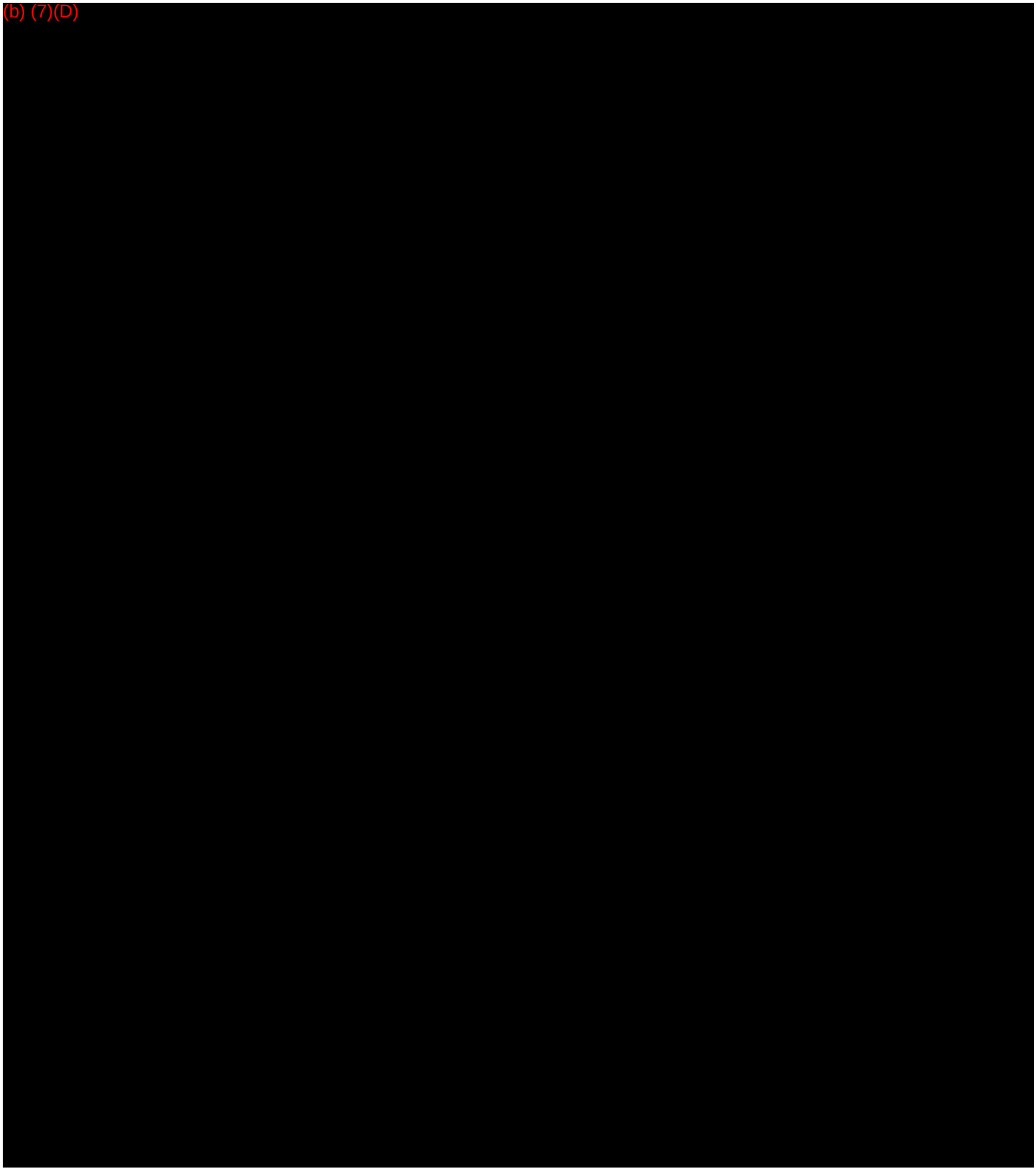
(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

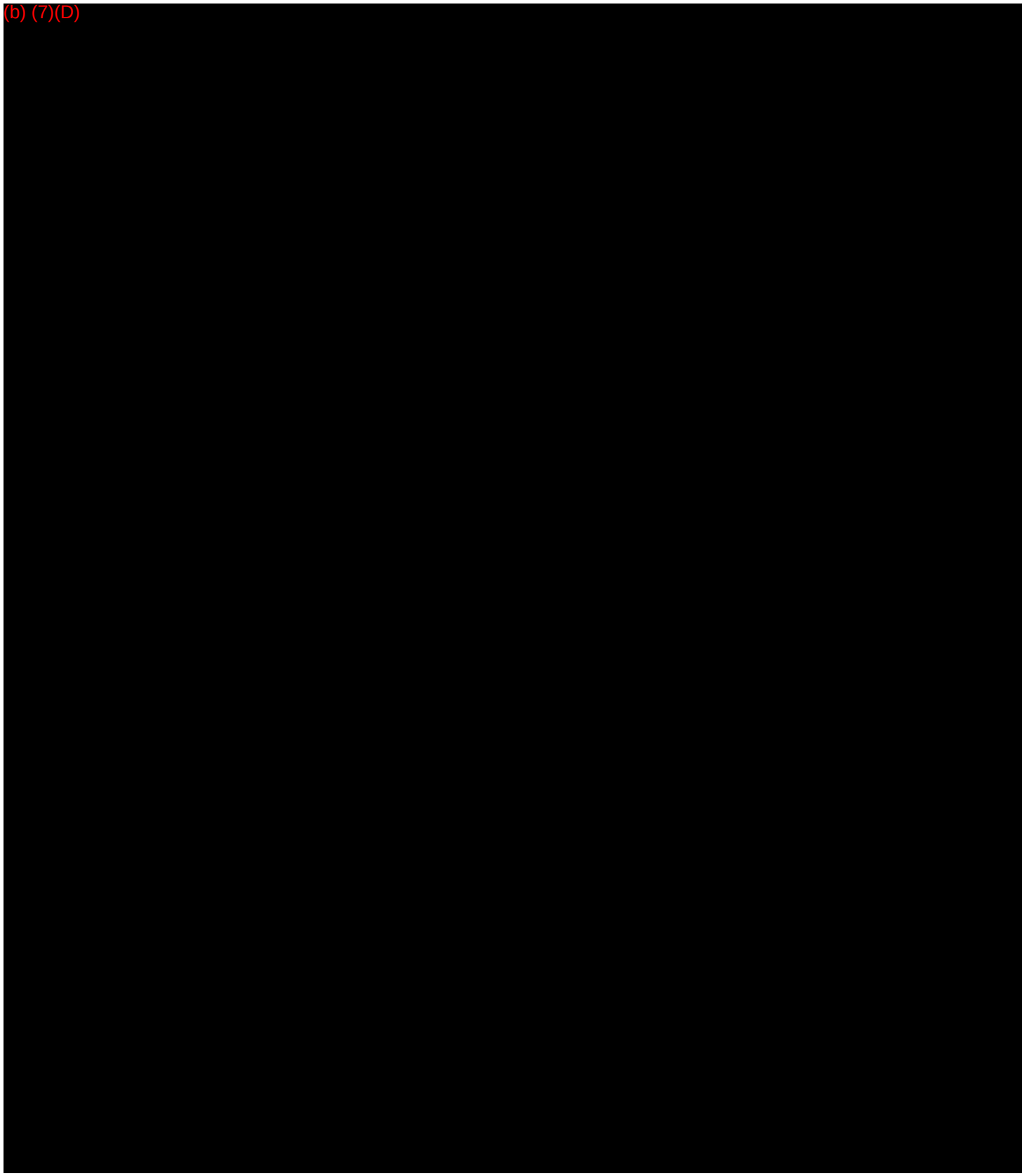
(b) (7)(D)



(b) (7)(D)

[redacted]

(b) (7)(D)

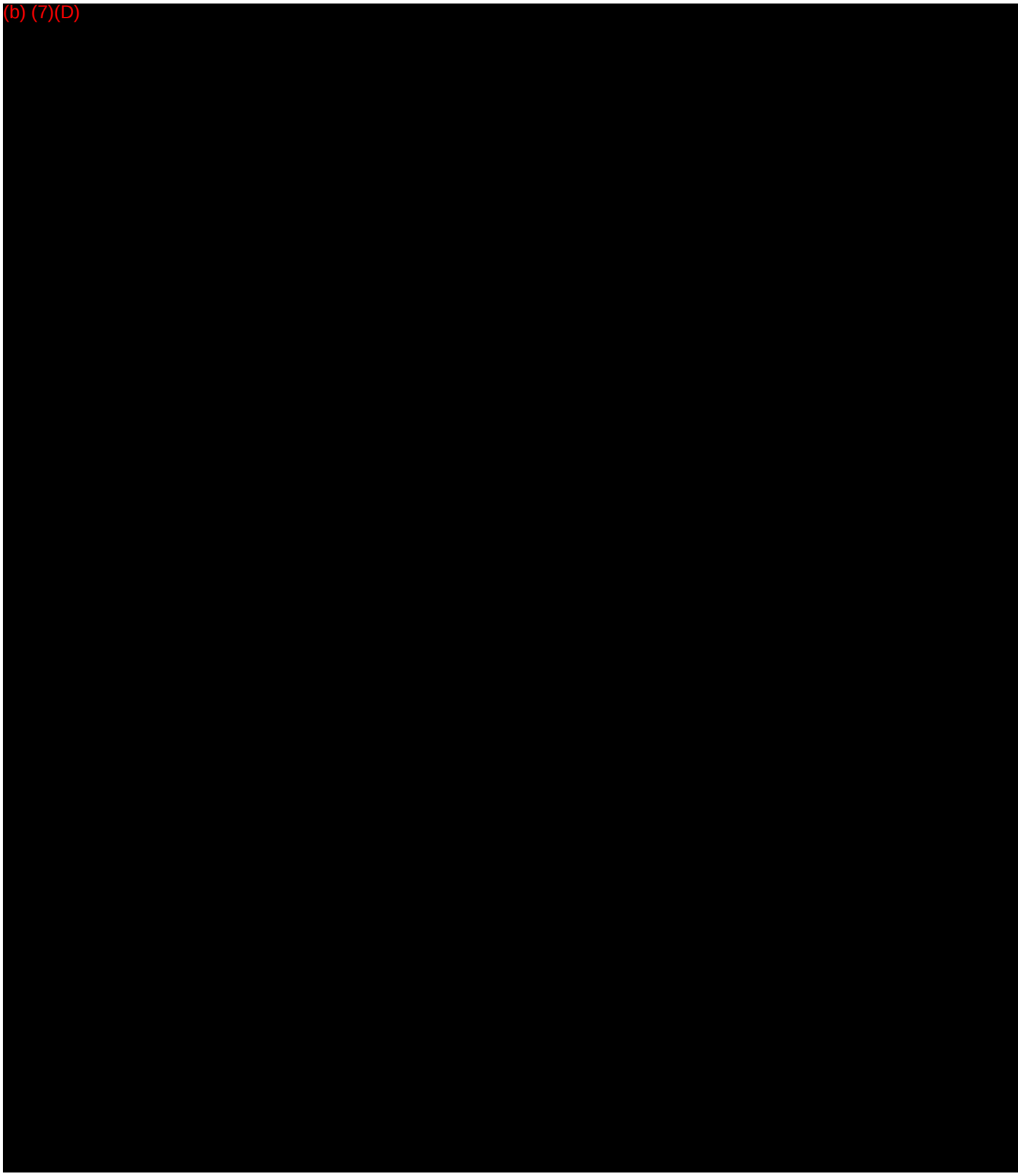


(b) (7)(D)

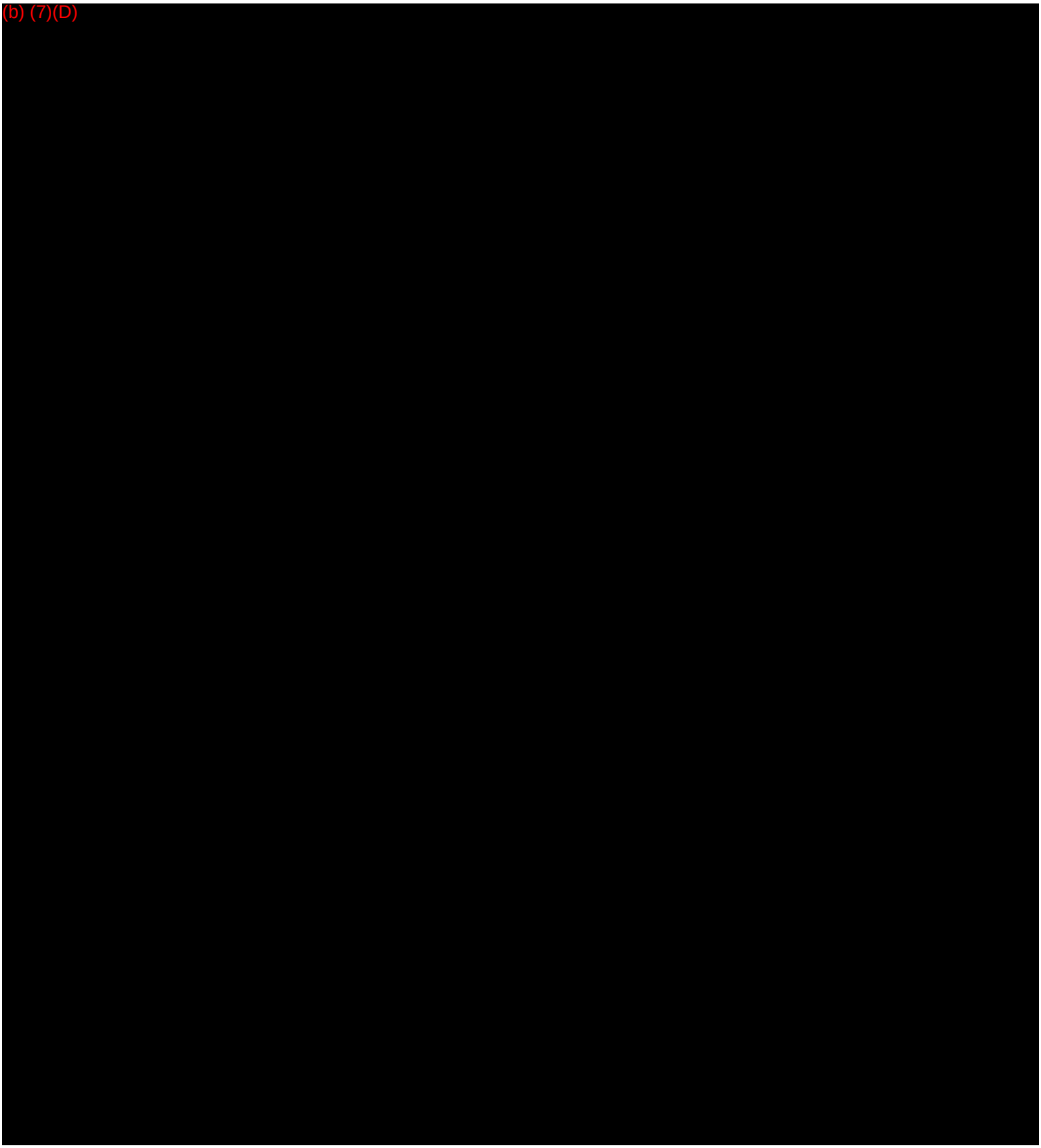
[redacted]

(b) (7)(D)

(b) (7)(D)



(b) (7)(D)



(b) (7)(D)

[redacted]

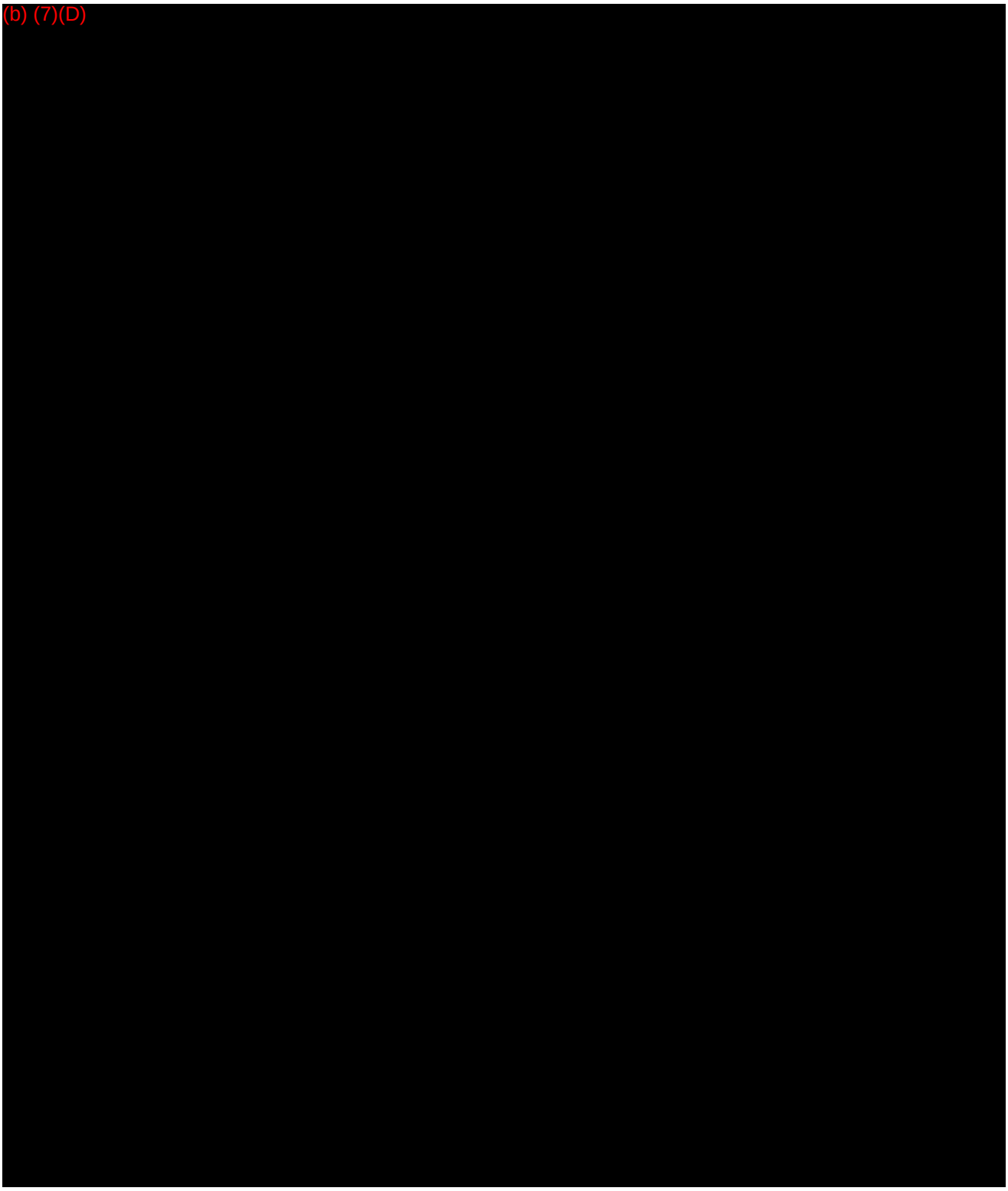
(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)



(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

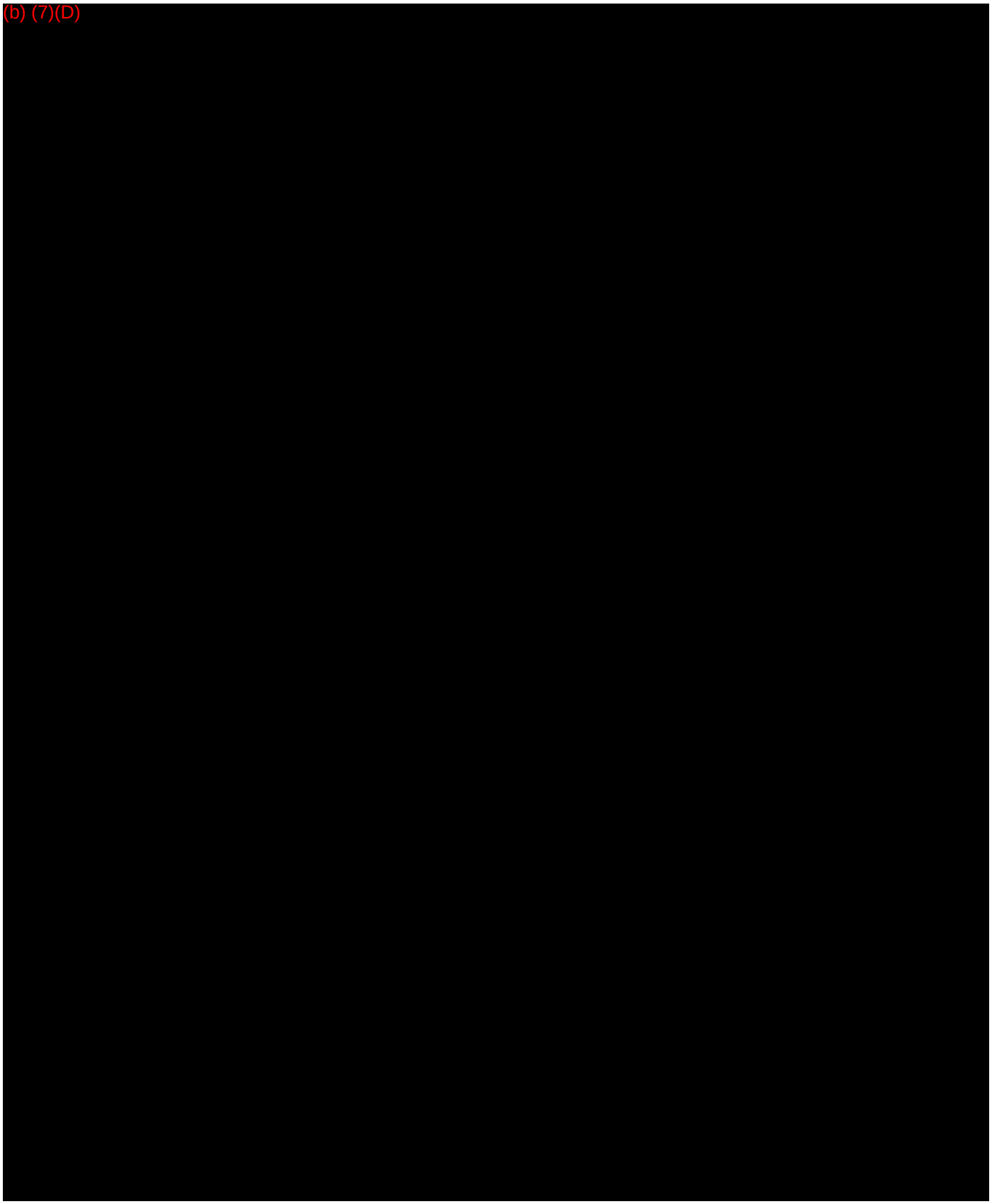
(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)



(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

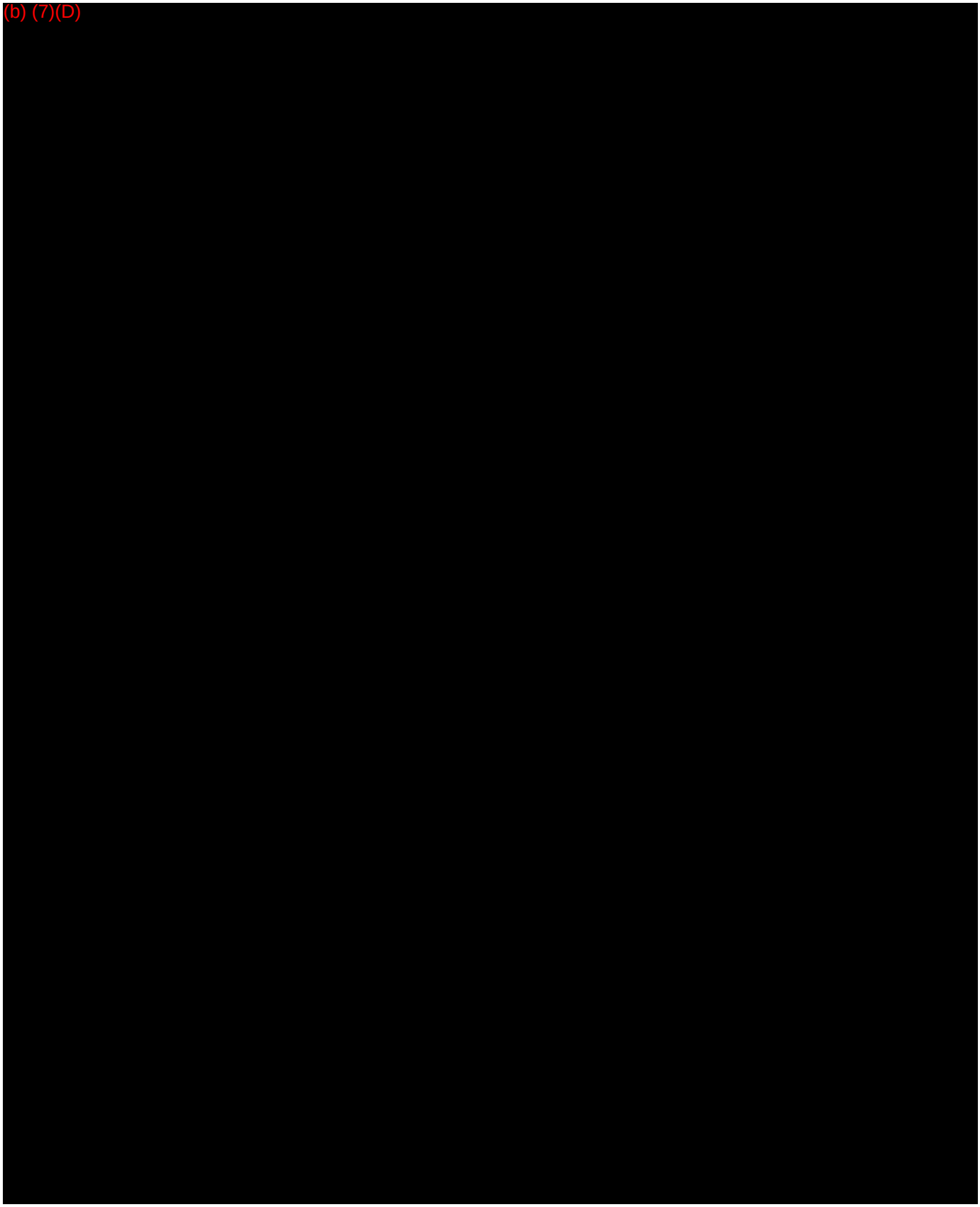
(b) (7)(D)

[redacted]

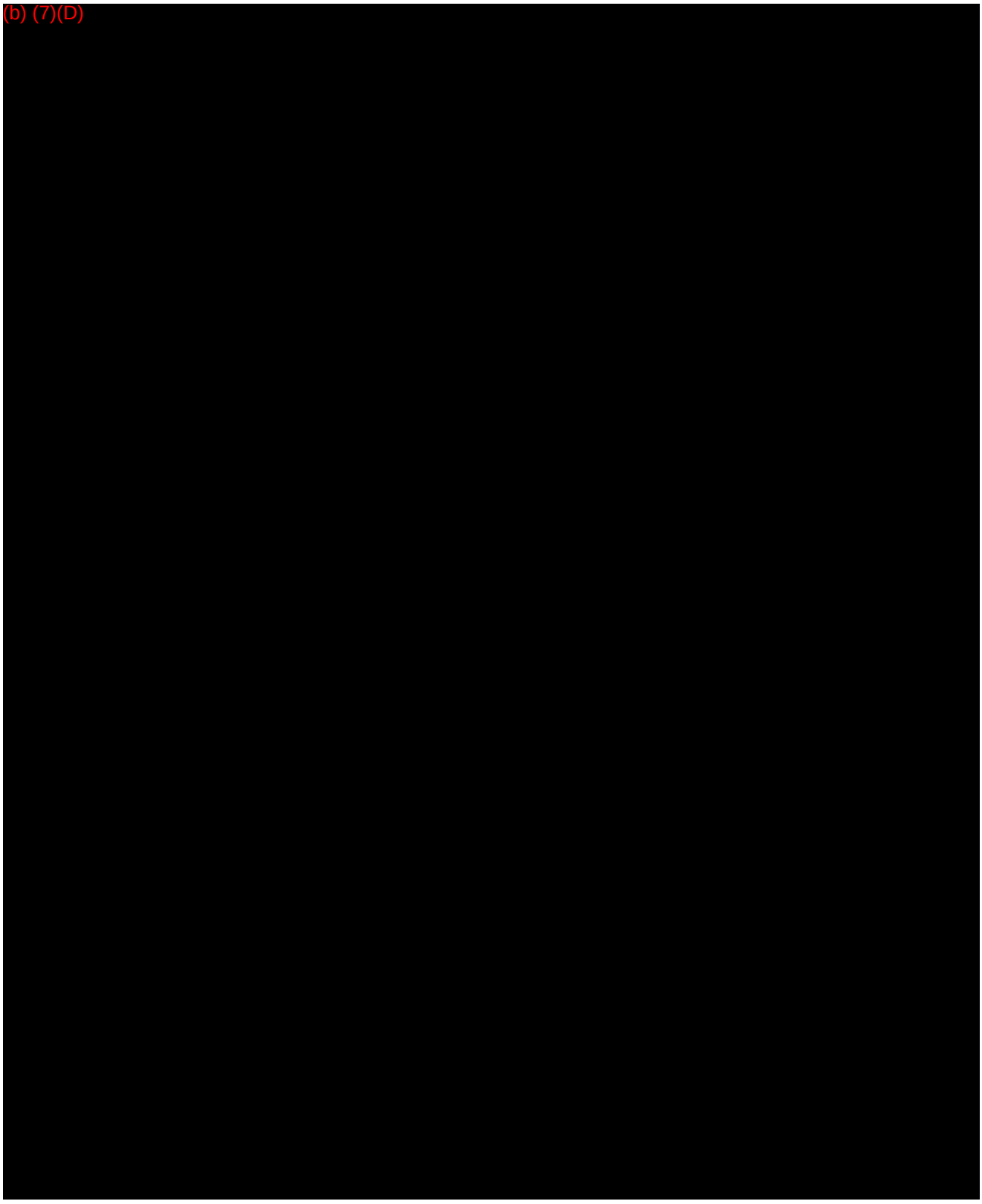
(b) (7)(D)

[redacted]

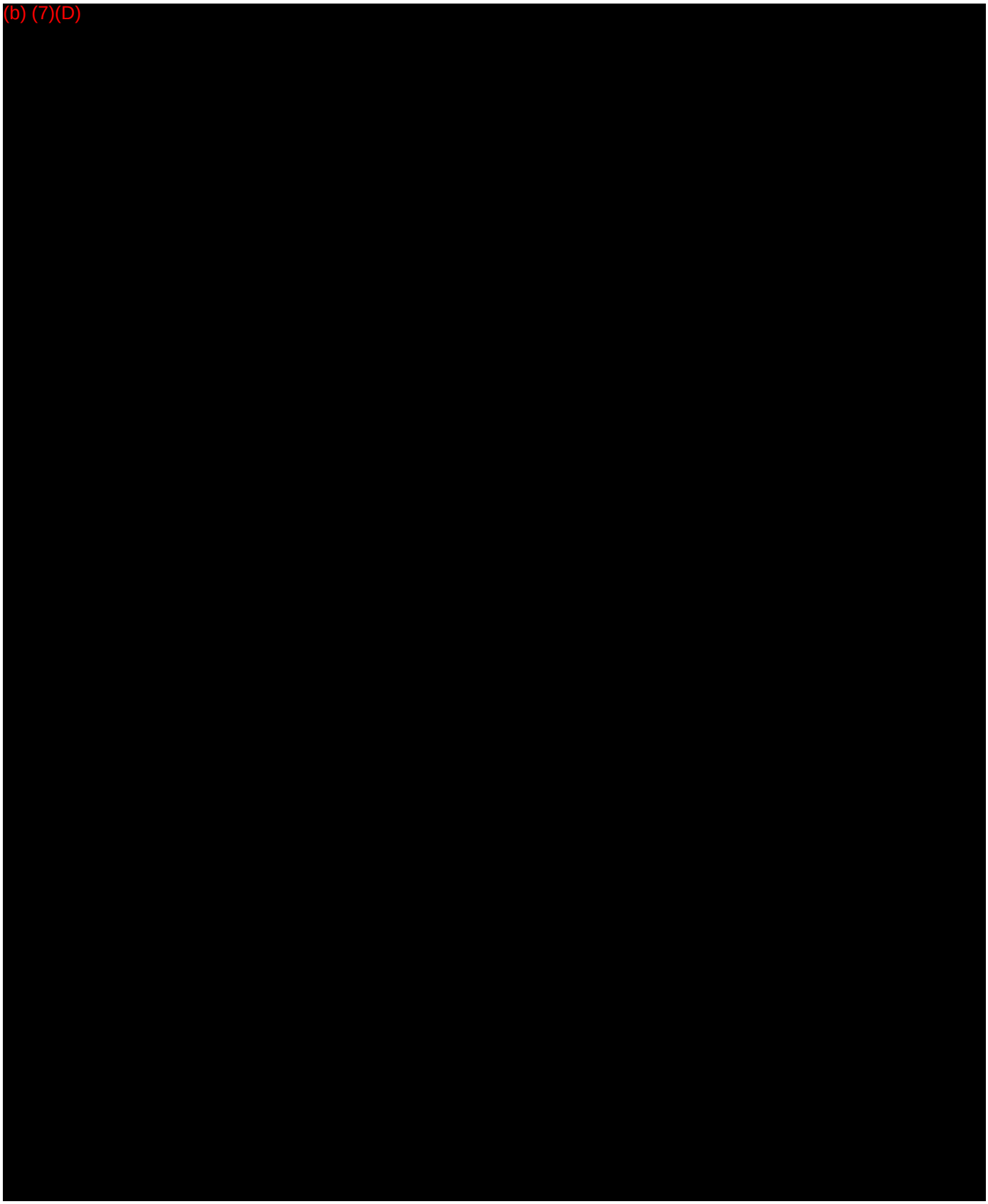
(b) (7)(D)



(b) (7)(D)



(b) (7)(D)



(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

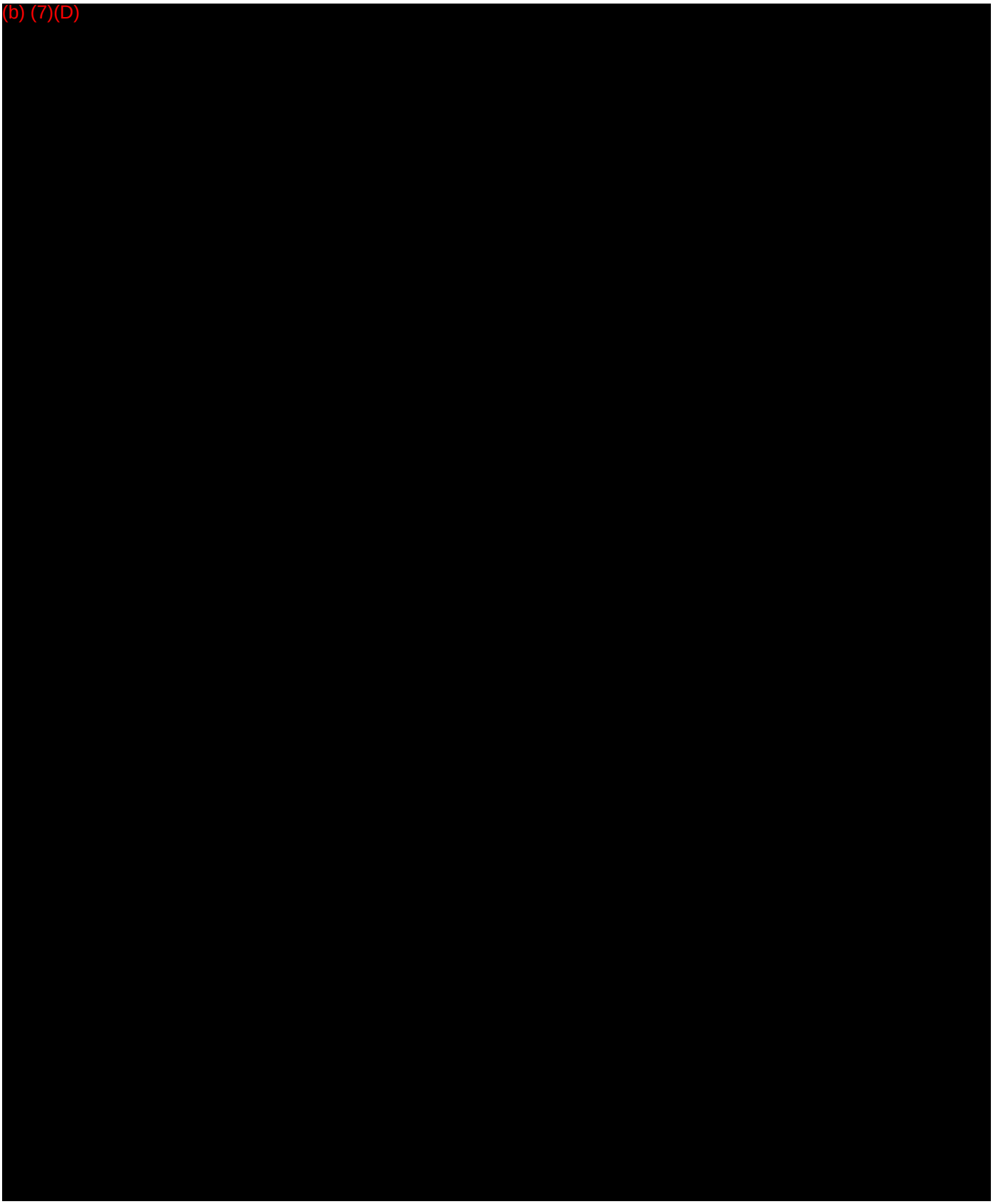
(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

(b) (7)(D)



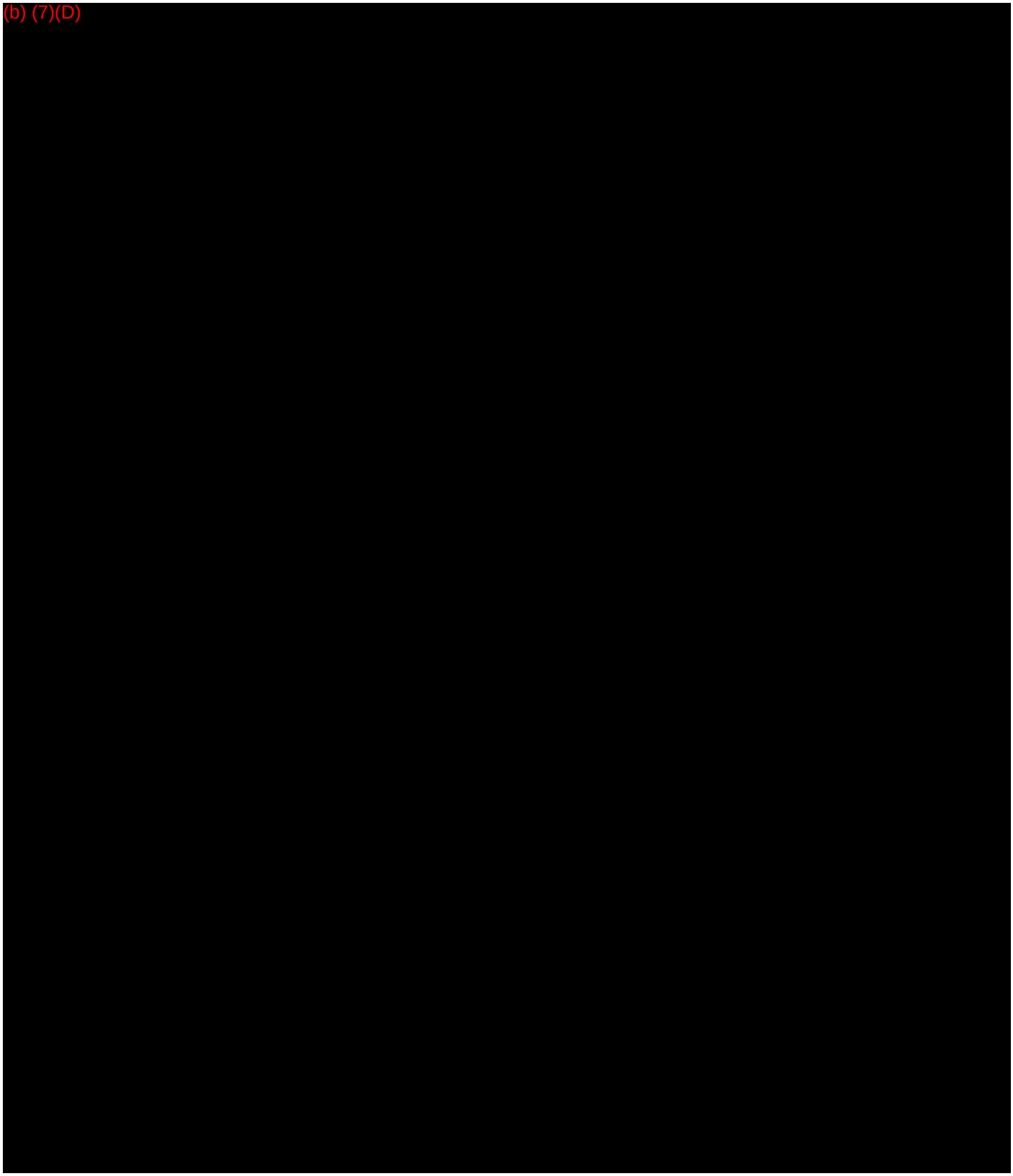
(b) (7)(D)

[redacted]

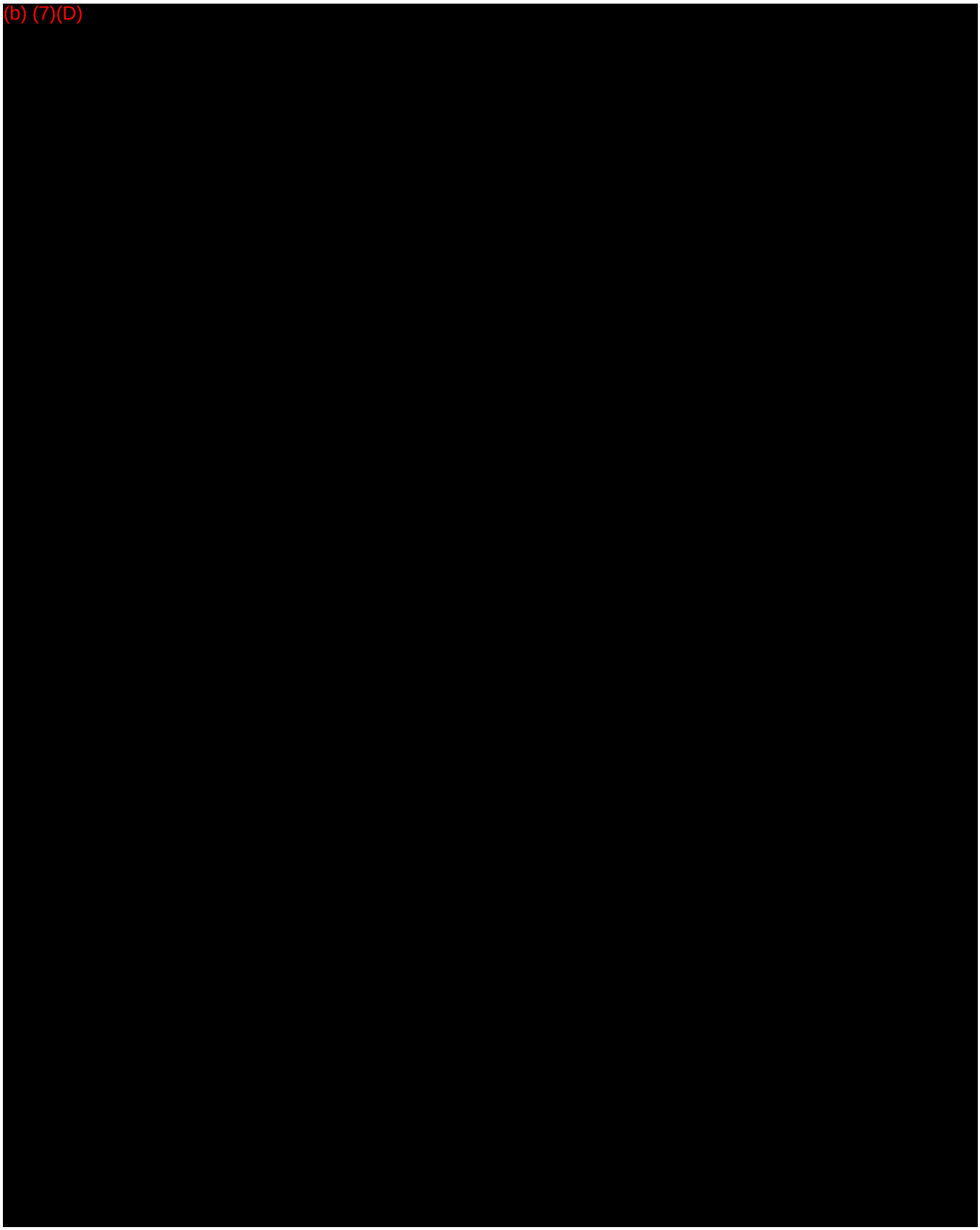
(b) (7)(D)

[redacted]

(b) (7)(D)



(b) (7)(D)



(b) (7)(D)

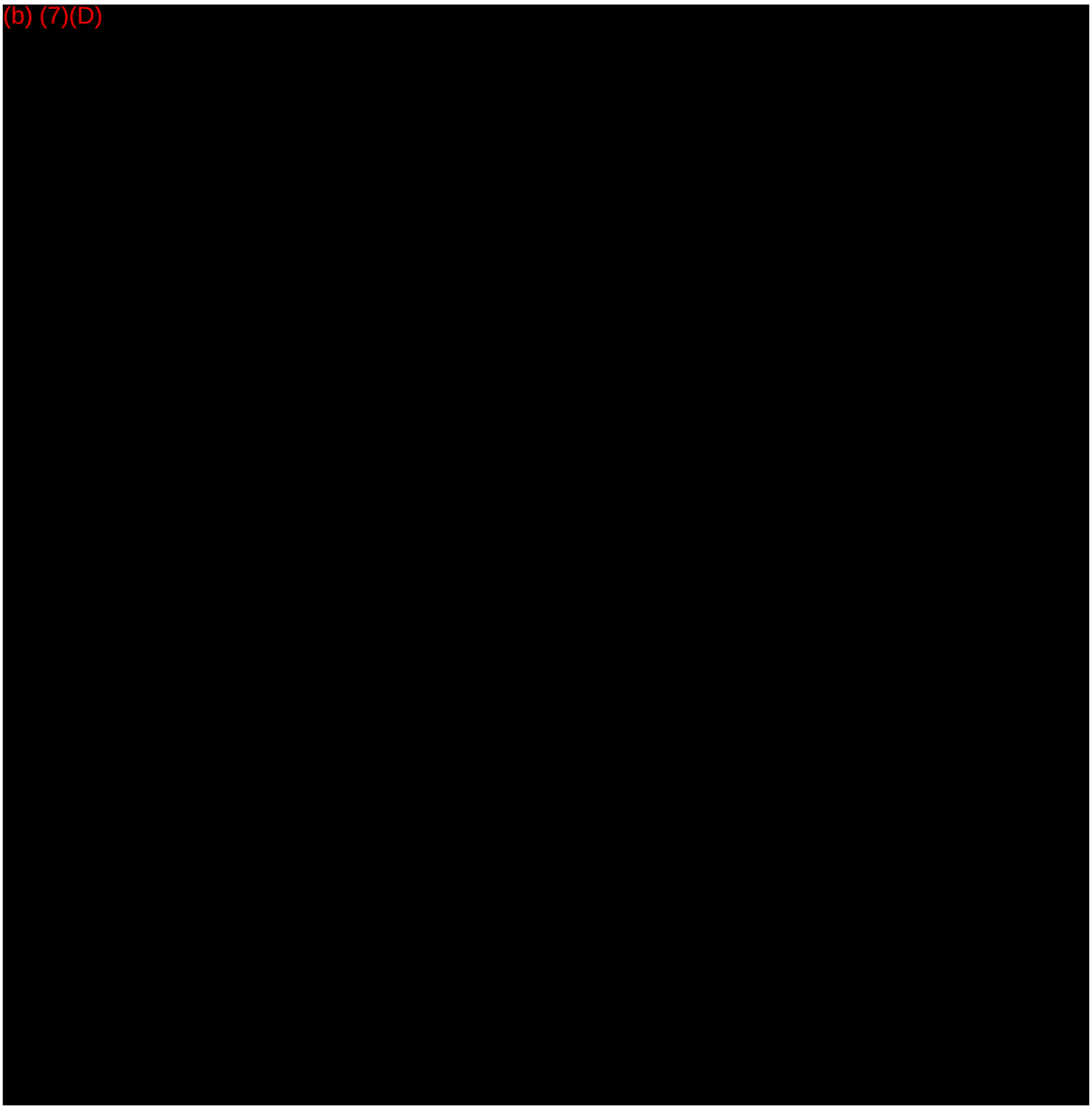
[redacted]

[redacted]

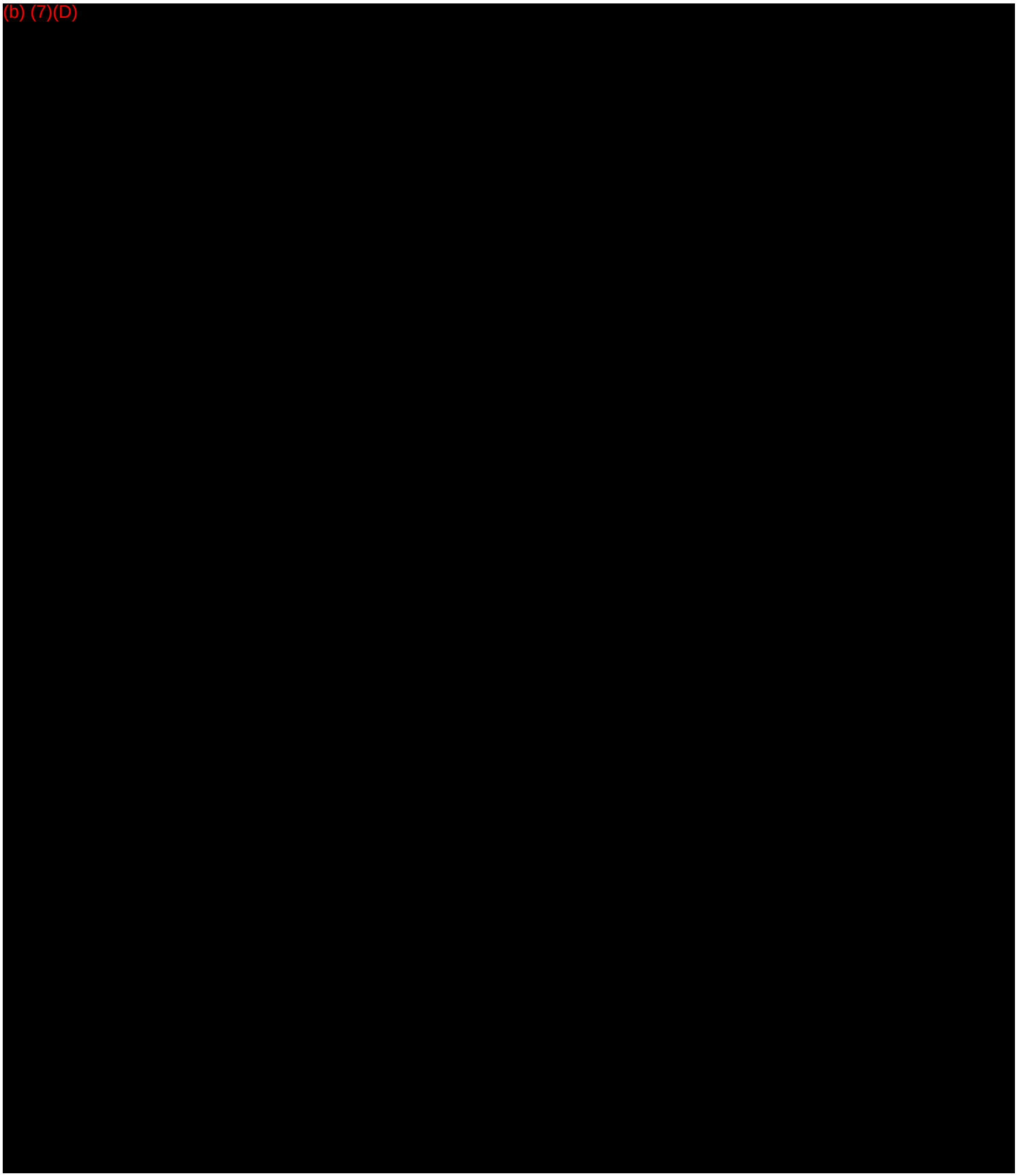
(b) (7)(D)

[redacted]

(b) (7)(D)



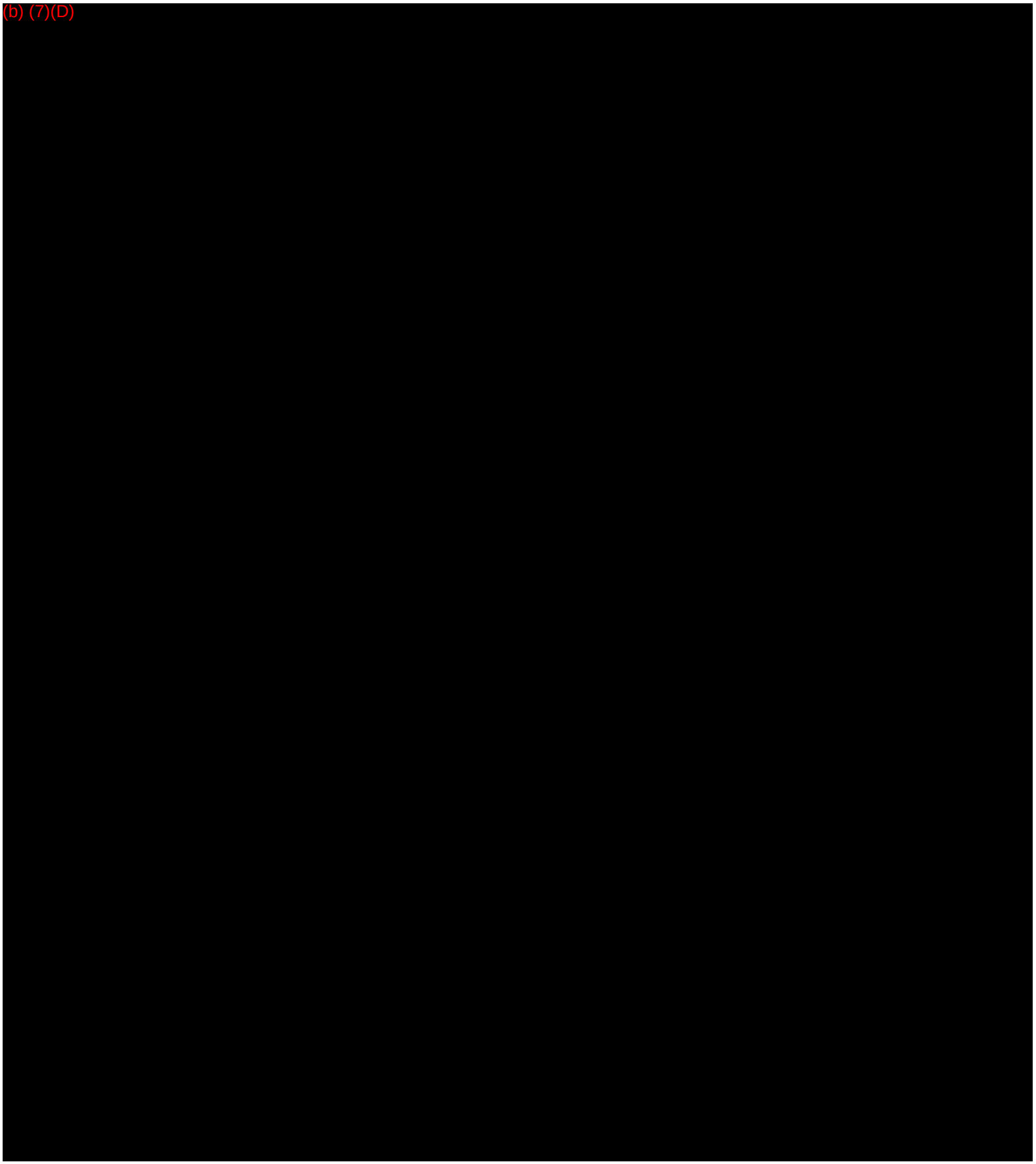
(b) (7)(D)



(b) (7)(D)

[redacted]

(b) (7)(D)



(b) (7)(D)

[redacted]

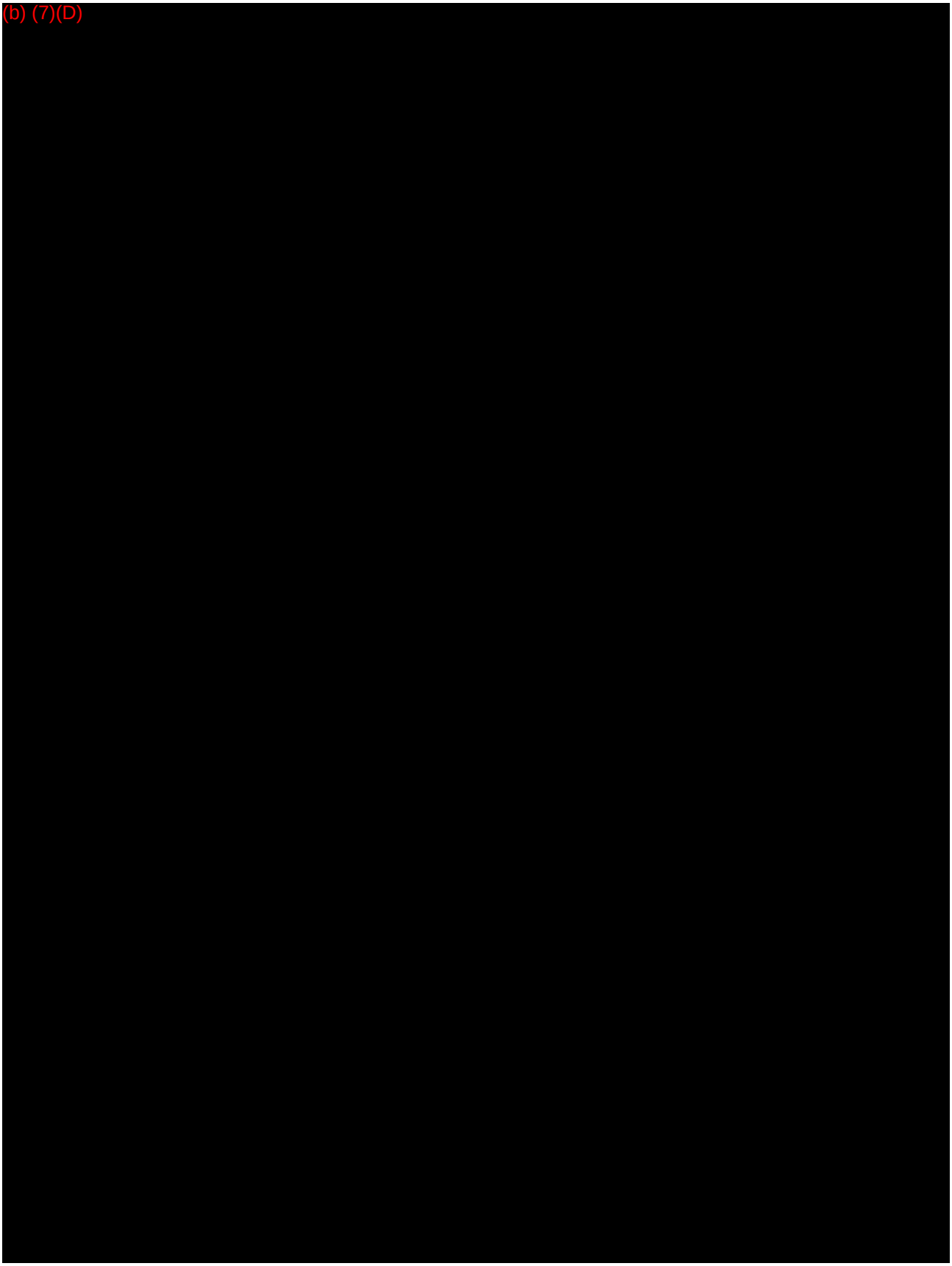
(b) (7)(D)

[redacted]

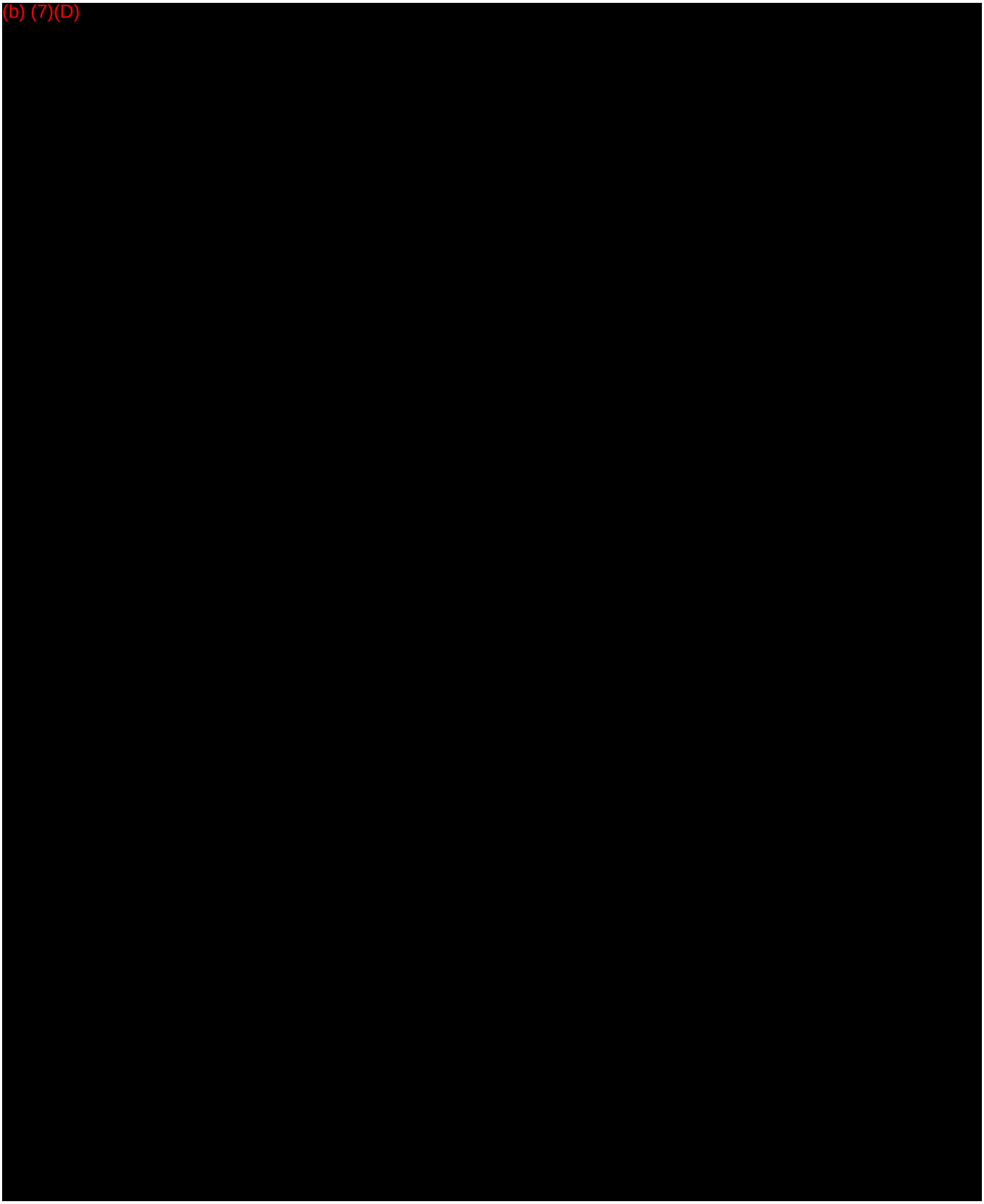
(b) (7)(D)

[redacted]

(b) (7)(D)



(b) (7)(D)



(b) (7)(D)

[redacted]

(b) (7)(D)

[redacted]

12.0 INVESTIGATIVE REPORTS

12.1 REPORT WRITING STANDARDS

A. *General Guidance and Standards*: Written reports must thoroughly address all relevant aspects of the investigation and be accurate, clear, complete, concise, logically organized, timely and objective. All reports should accurately, clearly, and concisely reflect the relevant results of the investigator's efforts. Facts should be presented in straightforward, grammatically correct language and should avoid the use of unnecessary, obscure, and confusing verbiage. Graphics should be well prepared, clearly relevant to the investigation, and supportive of the presentation.

B. *Specific Quality Standards*: Reports will conform appropriately to the following quality standards for investigations:

1. In any report, the facts should be set forth to facilitate reader comprehension. This should include a clear and concise statement of the facts and applicable law, rule, or regulation that was allegedly violated or that formed the basis for an investigation.

2. The principles of good report writing should be followed. A quality report will be logically organized, accurate, complete, concise, impartial, and clear and should be issued in a timely manner.

3. Reports should contain exculpatory evidence and relevant mitigating information when discovered during any investigation, administrative or criminal. Exculpatory evidence in a criminal or civil investigation must be brought to the attention of the assigned prosecutor.

4. Evidence outlined in a report should be supported by documentation in the investigative case file.

5. In some cases, it may be appropriate to note specific allegations that were not investigated to ensure that decision makers can take further action as they deem appropriate.

6. The outcome or accomplishment (fines, savings, recoveries, indictments, convictions, suspensions and debarments, or management recommendations, etc.) should be documented in the investigative case file.

7. Systemic weaknesses or management problems revealed in an investigation should be reported to agency officials as soon as practicable. (see Management Advisories Section 12.11)

12.2 REPORT FORMS, STYLE AND FORMAT

A. *Forms*: There are three different forms of reporting SAs should use to document investigative activity: a Report of Investigation (ROI), Abbreviated Report of Investigation (AROI), and Memorandum of Activity (MOA).

B. *Style and Formatting*: The specific report style and formatting requirements are as follows:

1. All reports will be typed in Times New Roman, 12 point font.

2. Reports should be written in third person, past tense.

3. When appropriate, acronyms should be introduced when the name, title, or entity first appears in the report and be used consistently thereafter, e.g. Special Agent (SA).

4. Dates will be expressed by spelling out the full month, followed by the day and year; e.g. April 1, 2002.

5. Times should be expressed in a 12-hour format; e.g. 10:00 a.m.

6. Individual names will not be fully capitalized, e.g. Armstrong, not ARMSTRONG.

7. States may be abbreviated using designated postal abbreviation codes, e.g. Alexandria, VA.

8. For additional guidance refer to the OIG Style Guide located at: https://oigcentral/PGF/Pages/OIGStyleGuide.aspx

12.3 INVESTIGATIVE PLAN

A. *General Description*: The Investigative Plan is created at the outset of an investigation. The plan will set forth the potential violations of law, rule or regulation involved in the investigation. The plan will also set forth the anticipated investigative steps and schedule of work.

B. *Form and Process of the Investigative Plan*: The Investigative Plan, INV Form 2 **(Exhibit 12-1)** will be prepared, if appropriate and at the discretion of the SAC at the beginning of the investigation. The plan will be completed by the assigned case agent and approved by their supervisor. Investigative Plans are flexible and subject to change as an investigation progresses.

12.4 MEMORANDUM OF ACTIVITY

A. *General Description*: The Memorandum of Activity (MOA) is a multi-purpose document used for reporting various types of investigative activity, such as interviews,

review of records, arrests, execution of search warrants, service of subpoenas, surveillance, and evidence development.

B. *Timeliness***:** MOAs will be submitted to the reporting agent's immediate supervisor for approval within five working days of the activity, or in exceptional circumstances as soon as practicable thereafter. The MOA will be incorporated into the investigative case file and uploaded into EDS within 10 business days of approval and signature, or in exceptional circumstances as soon as practicable thereafter.

C. *MOA Format and Preparation*: Each separate activity or interview will be reported in a separate MOA. MOAs are prepared using INV Form 9 **(Exhibit 12-2).** The format for the MOA will be as follows:

1. **Header:** The following information will be in the header:

   a. *Case Number*: As provided by the Enterprise Data System (EDS).

   b. *Case Title*: As reflected in EDS. i.e. First name Last name format

   c. *Type of Activity*: The nature of the investigative activity is contained in a drop down menu (i.e., personal interview, telephone contact, records review, other [describe]). Space is available to the right of the drop down selection to enter a brief description of the subject of the activity (e.g. specific name, source, record reviewed, etc.).

2. **Body**: The following information will be in the body:

   a. An introductory paragraph describing the date, time and location of investigative activity, subject of activity (full name, title and position if applicable), full name and title of other persons present during the investigative activity.

      i. Example: e.g. On date/time, the reporting agent and John Doe, Special Agent, Department of Homeland Security (DHS), Office of Inspector General (OIG), Office location, interviewed John Smith, location of the interview. Smith was informed of the identities of the interviewing agents and that the nature of the interview to obtain information relative to …..

   b. A concise and comprehensive summary report of investigative activity. Any attachments such as records, signed sworn affidavits, electronic intercepts, etc. should be summarized, not recited verbatim, in the body.

3. **Attachments**: The following applies to attachments to the MOA:

   a. Any documents that are attached to the MOA should be noted following the body of the MOA (e.g. *Attachment(s): Sworn affidavit, Miranda Warning,* etc.).

b. Attachments should be relevant and specific to the allegation and not include extraneous information. For example: TECS playback for a self-query should include the actual self-query, not all documents from the playback; and telephone call records or bank records should identify transactions that address the allegation(s), not the full response from an IG subpoena.

4. **Footer**: The following information will be in the footer:

a. *Signature Block*: The name, title, and signature of the SA who completed the MOA, and the date signed.

b. *Approval Block*: The name, title, and signature of the reviewing official, and the date signed.

c. *Item Block*: Sequential number of the MOA (optional).

d. Standard language prohibiting distribution of this report without OIG permission.

12.5 REPORT OF INVESTIGATION

A. *General Description*: The Report of Investigation (ROI) is used to report investigative results at the conclusion of a full investigation. The ROI can also be prepared to document special projects or other matters at the discretion of the SAC.

B. *Timeliness*: Under normal circumstances, the ROI will be prepared by the case agent and submitted for supervisory review within 30 days of the conclusion of the investigation. The investigation will be considered concluded on the date the last investigative activity is documented. The ROI will then be reviewed and approved by the first line supervisor and SAC in a timely manner thereafter not to exceed 30 days from the date the ROI is submitted for review. A copy of the ROI with exhibits will be placed in the official case file and uploaded into EDS within ten (10) business days of approval and signature. All of these reporting deadlines can be exceeded and met as soon as practicable after set deadlines only in exceptional circumstances.

C. *ROI Format and Preparation*: The ROI will be prepared using *Report of Investigation*, INV Form 8 **(Exhibit 12-3)**. The ROI will consist of a header, footer, synopsis, details, and exhibits sections. ROI headings ("Synopsis," "Details," and "Exhibits") will be centered, capitalized, and in bold Times New Roman 14 font. The remainder of the document will be typed in Times New Roman 12 font. Page one will contain the header and footer.

1. **Header**: The header will contain the following:

a. *Case Number*: As provided by EDS.

b. *Case Title*: Report the subject(s) of the investigation, to include full name (First,

Middle Initial, Last), job title, grade, bureau/agency, and work location.

c. *Report Status*: Interim, Final or Supplemental.

d. *Alleged Violation(s):* The predicating violation(s), to include the applicable potential violation of law (i.e. 18 U.S.C. 641, Theft of Government Property.) Non-criminal violations do not require specification of regulation, policy or procedure, but merely a summary statement of the allegation (i.e. mismanagement, inappropriate relationship, nepotism, etc.)

2. **Footer**: The footer will contain the following:

a. *Distribution Block*: Field Office, Headquarters, Component, Other

b. *Reporting Agent*: Name, Title, Signature, and Date

c. *Approving Official*: Name, Title, Signature, and Date

3. **Body**: The body of the ROI will contain the following:

a. *Synopsis:* A brief summary of the investigation, preferably limited to one page. This should include the predicating allegation(s), the name of the subject(s), the results of the investigation, and any judicial action. Subject(s) only need to be identified by first and last name in this section.

b. *Details Section – Origin of the Investigation:* Begin this section with a detailed account of the nature and origin of the investigation, to include how and when the allegation was received. The subject(s) should be fully identified by their full name (First, Middle Initial, Last), title, grade, bureau/agency, and work location.

c. *Details Section – Allegations*: Where appropriate each allegation will be listed separately and identified numerically in the body of the report. If there is only one allegation, it will not be numbered. Each allegation will be left justified, typed in bold font with the word "Allegation" underlined. For example:

*Allegation #1: John Doe accepted bribes for smuggling narcotics***.**

d. *Details Section – Summary of Investigative Activity*: After an allegation is listed, summarize the investigative activity pertaining to the allegation. This section of the report should contain only summaries of the relevant information, interviews, inquiries, and documentation, outlining what occurred in logical order. This section of the report should not contain a verbatim recitation of every interview or a complete, cut and paste repetition of the information reported in the supporting MOAs.

e. *Details Section – Citing Exhibits*: Supporting MOAs and other supporting documentation will be attached as exhibits, but they will be cited in the Details section of the report sequentially, as the exhibit corresponds with the information conveyed. The exhibit will be cited at the end of the final paragraph to which the exhibit relates. Exhibit numbers should not be placed within a sentence or paragraph.

f. *Exhibits Section - Format*: The Exhibit Section consists of two columns, labeled "Number" and "Description." Each exhibit utilized in the ROI will be identified by number and a brief description, including identification of the DHS component of any employee interviewed. The description should also indicate the dates of each document, interview, report, or when a photograph was taken, etc. *(e.g. Memorandum of Activity, Interview of John Doe, CBP, on July 4, 2014).*

g. *Exhibits Section – Order and Content*: The predicating document(s) will be the first exhibit. An MOA is not needed to document ICE/CBP JICMS reports, CIS/OSI referrals, TSA/OOI referrals, FEMA fraud reports/ referrals, or other such reports or referrals from other DHS component agencies, to include internal affairs offices. These reports can stand alone and serve as the first exhibit. Only copies of the items used as exhibits will be attached to the ROIs. Offices will retain the original exhibits.

4. **Cover Page**: An INV Form 8A, "Report of Investigation Cover Page" **(Exhibit 12-5)** will be used on ROIs (except collaterals), and these will be uploaded in EDS along with the report itself within ten (10) business days or in exceptional circumstances as soon as practicable thereafter.

5. *Responsibility for Documentation, Signatures and Transmittal*: ROIs will be reviewed, approved, signed, transmitted to the appropriate component or other entity, and the case closed in EDS by the field SACs or their designees.

12.6 ABBREVIATED REPORT OF INVESTIGATION

A. *General Principles for Using Preliminary Investigations and an Abbreviated Report of Investigation*: SACs are encouraged to conduct preliminary investigations to assess the viability of allegations and whether further investigation is warranted. SACs should be particularly vigilant in investigating allegations in the categories of misconduct where referral to OIG from DHS components is required to be transmitted immediately upon receipt of the allegation and where no investigation shall be conducted by the component prior to referral (per DHS Management Directive 0810, **Exhibit 2-10**). However, preliminary investigations often reveal no basis for further investigation. In such cases, an investigation should always be opened and investigative activity appropriately documented, even where the activity was very limited. When a determination is made to close an investigation after such preliminary investigative activity, an Abbreviated Report of Investigation (AROI) should be considered an appropriate means of doing so.

B. *General Description of the AROI*: The AROI is an alternative method for documenting and reporting investigative activities, findings or results when investigative activity was preliminary, initial, or otherwise limited and a brief summary is sufficient to adequately convey the investigative activities, findings or results.

C. *Appropriate Uses of an AROI*: An AROI can be used when investigative activity was preliminary, initial or otherwise limited and a SAC determines that an AROI is the most appropriate vehicle to document investigative findings or referrals for components or external stakeholders. It can also be used when an investigation is being administratively closed to the file and no information transmitted outside DHS OIG.

D. *Examples of Appropriate Use*: Following are examples of instances where an AROI may be used:

1. *SAC receives an allegation that a DHS employee abused a detainee in a DHS facility. Because of the nature of the allegation, a preliminary investigation is necessary. Our initial investigative activity determines that the allegation is unsubstantiated or unfounded. An investigation should be opened and an AROI can be used upon closing the investigation. The body of the AROI should summarize the limited investigative activity and state that it was determined that no further investigation by the OIG is warranted, resulting in the investigation being closed.*

2. Preliminary investigation determines the allegation is a matter that should be referred back to the component. In such instances, the AROI should reflect that no further investigation by the OIG is intended; therefore, this investigation is closed and referred.

3. In situations where civil, criminal and/or administrative action has resolved the allegation(s) and no additional significant information was developed supporting additional civil, criminal and/or administrative action.

4. In employee misconduct investigations in which the employee was terminated while under OIG investigation and no criminal charges are viable.

E. *Inappropriate Uses of an AROI*: AROIs should not be used when the investigation is not resolved by a preliminary or initial investigation. AROIs also would not typically be appropriate when an investigation involves highly complex issues, numerous distinct allegations, or a particularly serious/sensitive investigative matter, such as civil rights & civil liberties or excessive use of force allegations involving serious misconduct, injury or death.

F. *General Content and Disposition*: All relevant investigative information should be briefly synopsized in the AROI body, and any other documentation or reports, such as MOAs, should be appended to the AROI as attachments. An AROI is prepared using INV Form 8A (**Exhibit 12-4**). An AROI will be submitted, reviewed, approved by a

SAC, and uploaded to EDS in the same manner as an ROI. A signed, hard copy of the AROI will be maintained in the official case file.

G. *Timeliness*: Under normal circumstances, the ROI will be prepared by the case agent and submitted for supervisory review within 30 days of the conclusion of the investigation. The investigation will be considered concluded on the date the last investigative activity is documented. The ROI will then be reviewed and approved by the first line supervisor and SAC in a timely manner thereafter not to exceed 30 days from the date the ROI is submitted for review. A copy of the AROI will be placed in the official case file and uploaded into EDS within ten (10) business days of approval and signature. All of these reporting deadlines can be exceeded and met as soon as practicable after set deadlines only in exceptional circumstances.

H. *FBI Notification Letters:* FBI Notification Letters shall be generated for investigations resulting in AROIs, in accordance with Chapter 8, Section 9.

I. *AROI Format and Preparation:* The AROI will be prepared using the *Abbreviated Report of Investigation*, INV Form 8A **(Exhibit 12-4)**. The AROI will consist of a header, footer, and Investigative Summary section.

1. **Header**: The header will contain the following:

   a. *Case Number*: As provided by EDS.

   b. *Case Title*: Report the subject(s) of the investigation, to include full name (First, Middle Initial, Last), title, grade, bureau/agency, and work location.

   c. *Report Status*: Interim, Final or Supplemental.

   d. *Alleged Violation(s):* The predicating violation(s), to include the applicable potential violation of law (i.e. 18 U.S.C. 641, Theft of Government Property.) Non-criminal violations do not require specification of regulation, policy or procedure, but merely a summary statement of the allegation (i.e. mismanagement, inappropriate relationship, nepotism, etc.)

2. **Footer**: The footer will contain the following:

   a. *Distribution Block*: Field Office, Headquarters, Component, Other

   b. *Reporting Agent*: Name, Title, Signature, and Date

   c. *Approving Official*: Name, Title, Signature, and Date

3. **Investigative Summary**: The Investigative Summary section constitutes the body of the AROI, and should generally be no more than two pages. The AROI should note

allegations and summarize all significant investigative information. The form of the Investigative Summary section is as follows:

a. *Origin, Subjects and Allegations*: The first part of the Investigative Summary section should be an introductory paragraph outlining the reason for initiating the investigation, which usually consists of the predicate allegations(s). The Subject(s) only need to be identified by first and last name in this paragraph.

b. *Brief Summary of Findings*: The second part will be a brief summary of the findings relevant to each allegation, not a detailed review of the evidence. It will also contain a brief description of any judicial or administrative action.

c. *Attachments - No Exhibits Section*: Unlike an ROI, the AROI will not have an Exhibits section. If there are attachments, the AROI need only reflect that copies of relevant documents are appended.

4. **Cover Page**: An INV Form 8B, "Report of Investigation Cover Page" **(Exhibit 12-5)** will be used on AROIs (except collateral), and these will be uploaded in EDS along with the report itself within ten (10) business days or in exceptional circumstances as soon as practicable thereafter.

12.7 REPORTS TO CONGRESS AND THE SECRETARY

In some instances, a particularly sensitive or high-interest investigation or investigative matter may warrant preparation of a special report to the Secretary, Congress, and/or for publication on the OIG website. In such instances, the AIGI may, in consultation with the IG, direct that such a report be prepared instead of or in addition to a standard ROI. Such reports will be prepared in draft by the field office in close coordination and consultation with the AIGI and OIG Counsel.

12.8 CASE REPORT

A. *General Description*: The Case Report is a special report prepared at the request of a prosecuting attorney and is designed to provide information that will aid the prosecutor in determining whether to accept the case for prosecution and/or open a Grand Jury investigation, among other similar purposes.

B. *Form and Content*: This report will identify the subject, outline the subject's pertinent personal information such as employment and criminal histories, describe violations of criminal statutes, and provide a summary of investigative activity and evidence collected to date. The report should include a list of witnesses and evidence, and may attach pertinent MOAs, as appropriate. The case report will be prepared in letter format from the SAC to the appropriate prosecutor's office.

12.9 TRANSMITTAL AND DISTRIBUTION OF REPORTS OUTSIDE OF DHS OIG

A. *Transmitting or Distributing Reports Outside of DHS*: When an ROI or AROI is being transmitted outside of DHS OIG, an ROI Transmittal Memorandum, INV Form 3 (**Exhibit 12-6**) or INV Form 3A (**Exhibit 12-7**), will be prepared and forwarded electronically with the ROI. The transmittal memorandum is used to forward the ROI to the affected component or other agency outside of DHS OIG.

1. For transmittal to components in cases in which the allegations were not substantiated, an INV Form 3 will be used and the affected component will be advised that they are not required to respond.

2. For transmittal to components where allegations were substantiated, an INV Form 3A will be used and the affected component will be advised that they are required to respond. INV Form 3 can be used when transmitting to a non-component agency outside of DHS OIG.

B. *Transmitting or Distributing Using the Homeland Security Information Network*: The Field Office SAC or designee shall upload a completed ROI/AROI and Transmittal Memorandum (INV Form 3/3A) to the Homeland Security Information Network (HSIN) in cases involving the following DHS components: ICE, CBP, TSA, USSS, USCIS, USCG, NPPD, CRCL, FEMA Personnel and FEMA Financial. The uploaded ROI is electronically moved to a file outside of EDS and combined with the completed transmittal letter.

1. *Internal Disposition*: When the ROI has been uploaded to the component agency via HSIN, the field office will ensure all EDS entries have been completed, all supporting documents have been uploaded, and the case has been closed in EDS.

2. *Note Regarding Classified or Sensitive ROIs*: ROIs that are classified, highly sensitive, or for DHS components not listed with HSIN are transmitted manually. For guidance in assessing whether a report should be transmitted manually a SAC should consider appropriate factors in Section 12.10, below, and consult with the DAIGI.

12.10 ENHANCED REPORTING REQUIREMENTS

A. *General Provisions for Enhanced Case Reporting*: Some cases involve circumstances of a nature and characteristic warranting special attention from the IG. SACs should be vigilant in identifying such cases and ensuring the DAIGI and AIGI are made aware of them at inception. Such cases require regular updates of investigative activity and developments to enable the AIGI to provide oversight and the IG to respond to Congress and/or the Secretary and to other high-level inquiries.

B. *Enhanced Reporting Factors*: Cases warranting Enhanced Reporting Requirements involve the following factors:

1. Presidential Appointees are involved as possible subjects or witnesses

2. SES Employees are involved as possible subjects or witnesses

3. Whistleblowers cases where special interest by the Media, Congress or the Secretary is known or anticipated

4. Civil Rights, Civil Liberty or Use of Force investigations involving serious injury or death and/or where interest by the Media, Congress or the Secretary is known or anticipated

5. Congressional interest is known or anticipated

6. Media Interest is known or anticipated

7. Main DHS interest is known or anticipated

8. Component Internal Affairs agents are involved as possible subjects or witnesses

9. DHS OIG employees are involved as possible subjects or witnesses

10. Any other issues, facts or circumstances that are of a high profile nature or that the SAC believes may give rise to Congressional, Media or high-level Departmental interest

C. *Specific Reporting Provisions*: ROIs involving the above subjects/issues will be reviewed by the AIGI after review and approval by subordinate supervisors (SAC and DAIGI). All interim updates can be provided in summary by email through the DAIGI to the AIGI.

12.11 MANAGEMENT ADVISORY

A. *General Description*: A Management Advisory (MA) will be used to report systemic deficiencies and make recommendations for corrective action to DHS components. The goal of this report is to provide a decision-maker with a relevant and timely assessment of facts and circumstances related to a systematic or programmatic deficiency, and any recommendations related thereto, in order to ensure the protection and integrity of DHS programs and operations without compromising ongoing INV investigative efforts.

B. *Timeliness*: To be effective, MAs must be received by the impacted component as soon as possible. Accordingly, MAs are rarely generated at the conclusion of an investigation. Rather, MAs will be developed and submitted as quickly as possible, so as to limit the harm associated with the deficiency or problem identified.

1. *Consider Impact on Investigations*: In some instances, issuing an MA may serve to negatively impact an ongoing criminal or otherwise sensitive investigation. Under

these circumstances, the MA should also be constructed and timed in such a way as to avoid compromising the investigation. If there is a risk that the submission of an MA will compromise the underlying investigation, the SAC can delay issuing an MA, after consultation with the DAIGI and AIGI.

2. *Consultation with Prosecutors*: The SAC should also consult with a prosecutor in any investigations of criminal misconduct before an MA is issued, and must consult with the prosecutor in any investigation where prosecution is already under consideration by said prosecutor.

C. *When an MA is Appropriate*: The goal of an MA is to ensure the protection and integrity of DHS programs and operations. Accordingly, a determination that a systemic deficiency exists warranting an MA should be made in this context, and include an analysis of associated rules, regulations, policies, procedures and the following factors:

1. National Security – Does the deficiency have a detrimental effect on national security?

2. Health & Safety – Does the deficiency expose the public or government employees to health and safety risks?

3. Loss of money – Is the government losing money due to the deficiency and will a failure to correct the deficiency continue to cause the government to lose money?

4. Program has not been audited – Does the deficiency identified reveal the need for an audit to determine the extent of a systemic or programmatic problem?

5. No Policy or Procedure exists for the issue discovered – If so, does a policy need to be developed in order to correct the deficiency?

6. Did a programmatic or policy failure cause or contribute to the activity under investigation?

7. Has the investigation identified a vulnerability that leaves the component susceptible to fraud, waste, or mismanagement?

8. Media or Congressional Attention – Does the deficiency relate to a matter that has received or is likely to receive Media or Congressional attention?

D. *Format and Preparation*: The MA will be prepared in an individual format, signed by the Reporting Agent, approved by the SAC, and submitted as soon as practicable subsequent to the identification and assessment of the systemic deficiency. The format for an MA is contained in INV Form 12, Management Advisory Memorandum **(Exhibit 12-8)**.

1. The MA will contain the following:

   a. An introduction, including the identification of the program or system involved.

   b. A description of the systemic deficiency, including a summary of any relevant background facts and circumstances and a description of any relevant issues.

   c. Corrective recommendation(s), if any.

2. All MAs will carry an EDS case number and shall be accompanied by a Transmittal Memorandum outlining the summary of analysis, required response, and follow up contact information.

3. *Transmittal Memorandum*: The MA shall use a Transmittal Memorandum addressed to the DHS component director or equivalent with a copy (cc) to the associated Internal Affairs unit. A sample of a Transmittal Memorandum is attached as **Exhibit 12-9**. Generally, the Inspector General will sign transmittal memorandums if they are addressed to a Presidentially Appointed, Senate Confirmed component head. However, when determining what level of signature authority is required please refer to Directive OIG-RPP-1 (July 1, 2010) (**Exhibit 12-10**). The transmittal memorandum will advise components to direct their responses to OIGInvestigationsResponse@oig.dhs.gov.

E. *Internal OIG Review*: The MA and Transmittal Memorandum shall be reviewed and edited at the SAC field level in consultation with the DAIGI and AIGI. Upon review and concurrence from the DAIGI/AIGI, the MA and Transmittal Memorandum will be sent to Counsel and other OIG AIGs, including Office of Inspections, Office of Audits, Counsel, Integrity and Quality Oversight, Office of IT Audits, and Office of Emergency Management Oversight (if applicable), for review and approval and possible referral. Any recommended edits will come back to INV for consideration.

F. *Component Responses*: A DAIGI or designee will track component responses and follow up with components when necessary. MA recommendations and component responses will be tracked and reported appropriately in the SAR. These responses will fall into one of three categories:

1. *Open-Unresolved*: Components have not agreed to the recommendation, have not submitted a Corrective Action Plan, and have not submitted Target Completion Date.

2. *Open-Resolved*: Components have agreed with the recommendation, have submitted a Corrective Action Plan, and have assigned a Target Completion Date.

3. *Closed*: Components have implemented all recommendations and provided closure documentation. The components have 90 days to respond with up to at least one 90-day extension with DAIGI approval.

12.12 REPORTING MOTOR VEHICLE ACCIDENTS OR OTHER PROPERTY LOSSES

A. *General Provisions*: Investigations involving matters such as loss or theft of DHS OIG property, motor vehicle accidents, etc., will be reported by memorandum to the AIGI through the SAC with a cc to the DAIGI. Related investigative activities will be reported by MOA and attached to the memorandum.

B. *Contents of the Report*: Reports concerning motor vehicle accidents should include the following information:

1. date, time, location;
2. weather and road conditions;
3. vehicles involved (VIN, license plate number, and registration information);
4. persons involved, insurance contact information;
5. applicable safety devices (seatbelts/airbags);
6. injuries sustained;
7. police report(s) and witness statements;
8. description of property damage; and
9. SA statements. (Chapters 4.12, 4.13, and 5.5).

12.13 REPORTING INCIDENTS INVOLVING USE OF WEAPONS

All OIG employee incidents involving use of weapons must be reported by memorandum to the AIGI through the SAC with a cc to the DAIGI. Please refer to Chapter 5, *Firearms, Use of Force Policy, and Defensive Tactics*, for the guidelines regarding the use of weapons.

CHAPTER 12.0 - EXHIBITS

12-1 INV Form 2, Investigative Plan

12-2 INV Form 9, Memorandum of Activity

12-3 INV Form 8, Report of Investigation

12-4 INV Form 8A, Abbreviated Report of Investigations

12-5 INV Form 8B, Report of Investigation Cover Page

12-6 INV Form 3, ROI Transmittal Memorandum

12-7 INV Form 3A, ROI Transmittal Letter with Reply

12-8 INV Form 12, Management Advisory

12-9 MA Transmittal Memorandum: Sample AIG Report attached

12-10 DHS OIG Directive OIG-RPP-1, Report Processing Procedures July 1, 2010

Exhibit 12-1, INV Form 2, Investigative Plan

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

INVESTIGATIVE PLAN

CASE NUMBER: _____ **OFFICE:** _____

TITLE: _____ **CASE AGENT:** _____

_____ **SUPERVISOR:** _____

SUMMARY OF ALLEGATION(S):

IDENTIFY POSSIBLE VIOLATION(S) OF LAWS, RULES, OR REGULATIONS

- ☒ Criminal
- ☐ Administrative

CRIMINAL STATUTES
STANDARDS OF CONDUCT
DHS REGULATIONS
AGENCY SPECIFIC REGULATIONS
CIVIL STATUTES
ADMINISTRATIVE REGULATIONS

INVESTIGATIVE STEPS AND SCHEDULE OF WORK:

ACTION	ANTICIPATED DATE OF COMPLETION
☐ Review Complaint/Allegation	TBD
☐ Database Checks	TBD
☐ Witness/Complainant Interviews	TBD
☐ Document Retrieval (IG Subpoena)	TBD
☐ Subject Interview (Advisement)	TBD
☐ Presentation to USAO	TBD

Exhibit 12-2, INV Form 9, Memorandum of Activity

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

MEMORANDUM OF ACTIVITY

Type of Activity: Other

Case Number:	*Case Title:*

IMPORTANT NOTICE

This report is intended solely for the official use of the Department of Homeland Security, or any entity receiving a copy directly from the Office of Inspector General, and is disclosed only on a need to know basis. This report remains the property of the Office of Inspector General, and no secondary distribution may be made, in whole or in part, outside the Department of Homeland Security, without prior authorization by the Office of Inspector General. Public availability of the report will be determined by the Office of Inspector General under 5 U.S.C. 552. Unauthorized disclosure of this report may result in criminal, civil, or administrative penalties.

Page 1 of 1

Exhibit 12-3, INV Form 8, Report of Investigation

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

REPORT OF INVESTIGATION

Case Number:	
Case Title:	
Report Status:	
Alleged Violation(s):	

SYNOPSIS

Reporting Agent		*Distribution:*	
Name:	Signature:		Original
Title:	Date:	Headquarters	☐
Approving Official			
Name:	Signature:	Component(s)	☐
Title:	Date:	Other	☐

IMPORTANT NOTICE

This report is intended solely for the official use of the Department of Homeland Security, or any agency receiving a copy directly from the Office of Inspector General, and is disseminated only on a need to know basis. This report remains the property of the Office of Inspector General, and no unauthorized distribution may be made, in whole or in part, outside the Department of Homeland Security without prior authorization by the Office of Inspector General. Public availability of this report will be determined by the Office of Inspector General under 5 U.S.C. 552. Unauthorized disclosure of this report may result in criminal, civil, or administrative penalties.

no redactions

Page 1 of 2

REPORT OF INVESTIGATION

DETAILS

IMPORTANT NOTICE

This report is intended solely for the official use of the Department of Homeland Security, or any entity receiving a copy directly from the Office of Inspector General, and it is furnished solely on a "Need to Know" basis. This report remains the property of the Office of Inspector General, and no secondary distribution may be made, in whole or in part, outside the Department of Homeland Security without prior authorization by the Office of Inspector General. Public availability of the report will be determined by the Office of Inspector General under 5 U.S.C. 552. Unauthorized disclosure of this report may result in criminal, civil, or administrative penalties.

OIG FORM 0

Page 1 of 1

REPORT OF INVESTIGATION

EXHIBITS

NUMBER	DESCRIPTION

IMPORTANT NOTICE

This report is intended solely for the official use of the Department of Homeland Security, or any entity receiving a copy directly from the Office of Inspector General, and will be disseminated only on a "Need to Know" basis. This report remains the property of the Office of Inspector General, and no secondary distribution may be made, in whole or in part, outside the Department of Homeland Security, without prior authorization by the Office of Inspector General. Public availability of the report will be determined by the Office of Inspector General under 5 U.S.C. 552. Unauthorized disclosure of this report may result in criminal, civil, or administrative penalties.

Page 2 of 2

Exhibit 12-4, INV Form 8A, Abbreviated Report of Investigations

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

REPORT OF INVESTIGATION

Case Number:	
Case Title:	
Report Status:	
Alleged Violation(s):	

INVESTIGATIVE SUMMARY

Reporting Agent		*Distribution:*	
Name:	Signature:		Original
Title:	Date:	Headquarters	☐
Approving Official			
Name:	Signature:	Component(s)	☐
Title:	Date:	Other	☐

IMPORTANT NOTICE

This report is intended solely for the official use of the Department of Homeland Security, or any entity receiving a copy directly from the Office of Inspector General, and is disseminated only on a need to know basis. This report remains the property of the Office of Inspector General, and no unauthorized distribution may be made, in whole or in part outside the Department of Homeland Security, without prior authorization by the Office of Inspector General. Public availability of the report will be determined by the Office of Inspector General under 5 U.S.C. 552. Unauthorized disclosure of this report may result in criminal, civil, or administrative penalties.

Page 1 of 2

REPORT OF INVESTIGATION

IMPORTANT NOTICE

This report is intended solely for the official use of the Department of Homeland Security, or any entity receiving a copy directly from the Office of Inspector General. This report remains the property of the Office of Inspector General, and no secondary distribution may be made, in whole or in part, outside the Department of Homeland Security, without prior authorization by the Office of Inspector General. Public availability of the report will be determined by the Office of Inspector General under 5 U.S.C. 552. Unauthorized disclosure of this report may result in criminal, civil, or administrative penalties.

[redacted]

Page 2 of 2

Exhibit 12-5, INV Form 8B, Report of Investigations Cover Page

DEPARTMENT OF HOMELAND SECURITY
OFFICE OF INSPECTOR GENERAL

REPORT OF INVESTIGATION

IMPORTANT NOTICE

This report is intended solely for the official use of the Department of Homeland Security, or any entity receiving a copy directly from the Office of Inspector General, and is disseminated only on a need to know basis. This report remains the property of the Office of Inspector General, and no secondary distribution may be made, in whole or in part, outside the Department of Homeland Security, without prior authorization by the Office of Inspector General. Public availability of the report will be determined by the Office of Inspector General under 5 U.S.C. 552. Unauthorized disclosure of this report may result in criminal, civil, or administrative penalties.

Exhibit 12-6, INV Form 3, ROI Transmittal Memorandum

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

www.oig.dhs.gov

Date

MEMORANDUM FOR: Agency POC Name
Title
Agency Name

FROM: SAC Name
Special Agent in Charge
Office of Investigations
Field Office Name (i.e. Washington Field Office)

SUBJECT: Subject Name
Subject Title/Grade
Location

CASE NUMBER: I##-XXX-XXX-#####

Attached is our Report of Investigation (ROI) on the above subject.

The ROI is furnished to you to evaluate and make an administrative decision regarding the above listed subject. Should you take any administrative action in response to our ROI, please inform this office so we can update our records. Please destroy the ROI upon disposition of this matter.

Should you have any questions regarding the contents of the ROI or need additional information, you may contact me at [SAC's phone number].

Attachment

INV Form 3

Exhibit 12-7, INV Form 3A, ROI Transmittal Letter with Reply

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

www.oig.dhs.gov

Date

MEMORANDUM FOR: Agency POC Name
Title
Agency Name

FROM: SAC Name
Special Agent in Charge
Office of Investigations
Field Office Name (i.e. Washington Field Office)

SUBJECT: Subject Name
Subject Title/Grade
Location

CASE NUMBER: I##-XXX-XXX-#####

Attached is our Report of Investigation (ROI) on the above subject.

The ROI is furnished to you to evaluate and make an administrative decision regarding the above listed subject. A reply is requested within 30 days. Please destroy the ROI upon disposition of this matter.

Should you have any questions regarding the contents of the ROI or need additional information, you may contact me at [SAC's phone number].

Attachment

INV Form 3A

Exhibit 12-8, INV Form 12, Management Advisory Memorandum

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

File: MA#

MANAGEMENT ADVISORY

INTRODUCTION

[redacted]

Reporting Agent: Name: Title:	Signature: Date:	*Distribution:* Field Office / Headquarters / Component(s) / Other	Original
Approving Official: Name: Title:	Signature: Date:		

IMPORTANT NOTICE

This report is intended solely for the official use of the Department of Homeland Security, or any entity receiving a copy directly from the Office of Inspector General. This report remains the property of the Office of Inspector General and no secondary distribution may be made, in whole or in part, outside the Department of Homeland Security, without prior authorization by the Office of Inspector General. Public availability of the report will be determined by the Office of Inspector General under 5 U.S.C. 552. Unauthorized disclosure of this report may result in criminal, civil, or administrative penalties.

CORRECTIVE RECOMMENDATION

[redacted]

Exhibit 12-9, Sample Transmittal Letter (AIGI level)

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

MEMORANDUM FOR: TBD
Assistant Commissioner
Office of Field Operations
Customs and Border Protection

FROM: John E. Dupuy
Assistant Inspector General for Investigations

SUBJECT: *Identified deficiencies regarding the Vehicle and Cargo Inspection Systems (VACIS) located on the border nationwide*

Attached for your action is our Management Advisory, recommending *development of additional internal controls to detect, deter, and prevent the illegal entry of dangerous things into the United States.* As the result of two ongoing investigations, we determined that sites utilizing the VACIS machine should implement a multi-pronged approach to better prevent, identify, and disrupt against external and internal corruption. Moreover, it is a measured approach that will further protect against potential health and safety concerns and national security threats.

The advisory contains three recommendations aimed at improving the overall efficiency and effectiveness of examining large technology equipment, cargo, or hazardous materials. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendation(s). The memorandum should be accompanied by evidence of completion or an explanation as to why implementation cannot be achieved or what will be implemented in lieu of recommendation.

Please email a signed PDF copy of all responses and closeout requests to (b) (6) [redacted]@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we are providing copies of our report to appropriate congressional committees with oversight and appropriation responsibility over the Department of Homeland Security.

Please call me with any questions, or your staff may contact Steve Laferty, Acting Deputy Assistant Inspector General for Investigations, at (202) 254-(b) [redacted]

Attachment
CC TBD

Exhibit 12-10 DHS OIG Directive OIG-RPP-1, Report Processing Procedures Revised July 20, 2012

Office of Inspector General
U.S. Department of Homeland Security
Homeland Security

DIRECTIVE

SUBJECT: Report Processing Procedures	DIRECTIVE NUMBER: OIG-RPP-1
DISTRIBUTION: All OIG Offices and staff	DATE ISSUED: July 1, 2010

I. Purpose

1. To implement changes in processing announcement memorandum and final reports.

2. To establish general rules in signature authority for announcement and transmittal memorandums and draft and final reports.

3. To establish new changes in electronic document routing within the Project Tracking System for announcement memorandums, draft and final reports.

II. Scope

The report processing procedures will be effective beginning July 1, 2010, and applicable to our audit and inspection offices. These offices will be provided the necessary guidance to implement the new report processing procedures which affect announcement memorandum, draft and final reports.

III. Authorities

Inspector General Act of 1978, as amended.

IV. Policy/Procedures

It is the policy of the Office of Inspector General to communicate guidance to staff on how to process reporting documents to promote consistency, quality, and standardization among its reporting products.

In processing announcement memorandums, draft and final reports, certain general rules have been developed for guidance and consistency among our audit and inspection offices. Although exceptions to these general rules may arise, the following guidance outlines rules that are to be applied in general in report processing:

General Rule 1: The Inspector General will not sign final reports, Prefaces, or announcement memorandums, with a few exceptions. The Inspector General will continue to sign the Consolidated Financial Statement Audits. The Inspector General may sign other announcement memorandums and reports, if the issues involved are highly sensitive. If the document is addressed to a PAS confirmed component head (CH), the Inspector General will sign the announcement memorandum, the transmittal memorandum, and the report. This exception will not be used frequently because of General Rule 2.

General Rule 2: Draft and final report recommendations will not be addressed to a PAS CH, unless there are special circumstances approved by the Inspector General. The Inspector General expects recommendations be addressed to the department's lowest-level executive, such as SES'ers, who have the responsibility for ensuring that corrective actions are taken, instead of the PAS CH. The Inspector General will not need to sign a report if the recommendations are addressed to non-PAS executives. Office of Administration, Planning and Compliance Division, will post a list on DHS Connect of over 600 DHS SES positions to which our staff may address recommendations. See Attachment A of this policy for the list of SES'ers as of June 2010.

General Rule 3: Recommendations must not be addressed to the department's Secretary (S1), the Deputy Secretary (S2), the Under Secretary for the Directorate of Management (USM), or General Counsel.

General Rule 4: DIG for EMO and AIGs will sign all final report prefaces, and a transmittal memorandum to the SESer responsible for implementing the recommendations. The IG will sign a transmittal memorandum for each final report to transmit the report to the PAS CH. The IG will not sign these reports, if the report is addressed to SESers. The IG transmittal will alert the PAS CH that a report was sent to a section head (SESer) within the CH's organization. Office of Administration, Planning and Compliance Division, will post a list on DHS Connect of the PAS CHs and transmittal memorandum templates. See Attachment A of this policy for the list of PAS CHs as of June, 2010.

General Rule 5: Currently, we circulate reports once during the draft report stage to ask the department component(s) to identify any sensitive information. However, our program offices are encouraged to circulate sensitive reports to the applicable department component(s) twice to ensure that all sensitive information is properly identified and redacted. The second circulation will be just before the final report is forwarded to our Office of Counsel for review. OIG program offices are to circulate the *"final draft"* and the offices must circulate the report with the 'FOUO' markings and warnings. The *"final draft"* must not be numbered nor include the final report cover. Rather, our offices will continue to use the 'current blue report covers' for draft reports.

General Rule 6: When recommendations are addressed to several components, our program offices must work with the department to obtain a lead component assigned the responsibility for resolving the recommendations.

General Rule 7: The DIG-EMO and the AIGs will continue to sign draft reports. No changes are made in the report processing procedures for EMO's field office grant financial reports.

General Rule 8: The 30-day memorandum used to transmit a draft report to the department will include information about the need for the department to also develop and submit a Corrective Action Plan to our office within 90 days of receiving our final report. The Plan should include specific actions to be taken to address the recommendations and include target completion dates for implementing planned actions.

General Rule 9: Reports containing recommendations for the DHS Chief Financial Office (CFO) will be issued directly to the CFO (not to the USM) via transmittal memo from the DIG EMO or the AIG.

Major Exceptions to the New General Rules:

1. The Inspector General will still continue to sign the Consolidated Financial Statement Audits.

2. The Inspector General may choose to sign certain announcement memorandums and reports, if the issues are highly sensitive.

3. The Inspector General will still continue to sign reports, if they are addressed to a Presidentially-Appointed Senate (PAS) confirmed component head.

V. Responsibilities

Office of Administration, Planning and Compliance Division (the Division), will take the lead in assisting the offices with implementing the new changes in report processing. Guidance will include providing examples to the offices of how to format announcement memorandums, transmittal memorandums and draft and final reports. In addition, the Division will also oversee slight changes in the routing of draft and final reports within the Project Tracking System (PTS), and communicating those changes to the PTS Champions. The Division will also coordinate with appropriate department officials to obtain current listings of senior executives (SES'ers) and Presidentially-appointed and senate confirmed (PAS) executives, and component heads (CHs), to ensure our staff has access to those listings via the DHS Connect.

Audit and inspection offices are responsible for following the general rules and other guidance, as necessary, to produce reporting products that are consistently formatted and prepared in accordance with the Inspector General's guidelines.

VI. Definitions

SES'ers	senior executives (career and non-career service)
PAS	Presidentially appointed and senate confirmed
CH	component head

VIII. Questions

For questions about this directive, please contact Kim Hurley, Director, Division of Planning and Compliance, Office of Administration at 202-254-(b) or email at (b) (6) @dhs.gov. Alternate contact: (b) (6) 202-254-(b) or email at (b) (6) @dhs.gov.

APPROVED BY: _____
Charles K. Edwards
Assistant Inspector General for Administration

13.0 INVESTIGATIVE METHODS

13.1 INFORMATION DATABASES

INV has access to various commercial and law enforcement databases including, but not limited to: Lexis/Nexis, MasterFiles, and Choice Point. The Enforcement Communication System (TECS-II), Central Index System (CIS), National Crime Information Center (NCIC), National Law Enforcement Tracking System (NLETS), El Paso Intelligence Center (EPIC), and Financial Crimes Enforcement Network (FINCEN) financial databases. Information regarding the law enforcement databases available to INV personnel is located on the DHS OIG computer network. Selected INV personnel have received training in the legacy law enforcement databases so they can provide assistance, training, and resolve localized access issues.

Each Field Office will have access to NCIC through TECS. INV will appoint a TECS national point of contact who will be responsible for maintaining liaison contacts with the TECS system administrator. Additionally, four regional TECS System Control Officers (SCO) have been designated to be the points of contact for TECS. Each office having TECS access will have an individual SCO who reports to the regional SCO for TECS database issues. Regulations governing the use of TECS will be issued through INV.

The SACs will be responsible for ensuring that information such as missing/stolen law enforcement equipment, entry of arrest warrants, cancellation of warrants are made to the NCIC system through TECS. The United States Marshal Service (USMS) and the OIG have entered into an MOU which provides general guidance with administrative support and apprehension responsibility offered by the USMS to the OIG. In entering felony warrants into NCIC and the execution of OIG felony warrants. **(Exhibit 13-1)**

Additionally, SAs can access the Federal Emergency Management Agency (FEMA) funding database in the course of an investigation involving FEMA funds through the National Emergency Management Information System (NEMIS) web page. NEMIS will provide information concerning applications for Public Assistance (PA) and Individual Assistance (IA) funds.

OPD will coordinate access to databases.

13.2 AUDIT ASSISTANCE

Whenever a Field Office needs audit assistance, the SAC should forward a request via memorandum to the DAIGI Field Operations. This request should describe the allegations and state how the services of the Office of Audit (AUD) could assist in the investigation.

SAs should be aware of potential evidentiary problems arising from the "Audit Clause." The Audit Clause, in effect, waives certain Fourth Amendment rights a contractor would have to certain records. Fourth Amendment and Fifth Amendment rights against unwarranted searches and seizures and self-incrimination generally apply once an investigative interest in those records has been established.

Under the direction of an agent, the auditor may collect documents or make notes on any documents the auditor normally has access to or are within the scope of the audit during which potential fraud is disclosed. Documents of evidentiary value outside an audit clause or the normal scope should be requested by an IG subpoena where necessary.

13.3 MAIL COVERS

A mail cover is a process by which the United States Postal Service (USPS) records information appearing on the mail delivered to a particular address. The law allows a mail cover to obtain information in order to: protect the national security; locate a fugitive; obtain evidence of the commission or attempted commission of a crime; obtain evidence of a violation or attempted violation of a postal statute; or assist in the identification of property, proceeds or assets forfeitable under law. The USPS has determined that DHS OIG is a "law enforcement agency" within the meaning set forth in the Postal Service's mail cover regulations.

Mail Cover Request

A written request for a mail cover must be in letter format from the SAC (**Exhibit 13-2**) to the USPS Criminal Investigations Service Center Manager, Attn: MC Specialist, 222 South Riverside Plaza, Suite 1265, Chicago, IL, 60606-6117, and should include USPS "Request for Mail Cover" **(Exhibit 13-3)** which requires the following information:

State that an official investigation is in progress.

Stipulate and specify the reasonable grounds that exist which demonstrate that the mail cover is necessary.

Give name, address, and zip code of the individual or business whose mail is to be covered.

Give name and address of any known attorney for the mail cover subject or make a definite statement that the subject's attorney, if any, is not known. In fugitive cases, the names of known attorneys, or a statement that the attorneys are not known, must be furnished for both the fugitive and the person on whom the mail cover is desired. (Material mailed between a known attorney and the other parties, mentioned above are excluded from the coverage of a mail cover.)

Include a statement as to whether the subject is or is not under indictment in connection with the matter under investigation, and that if the subject is indicted

during the mail cover period for any cause, the USPS Inspector-in-Charge will be notified so that the cover can be terminated.

Give the federal statute alleged to have been violated and the penalty (must be over one year) involved, along with a statement as to what the subject of investigation is suspected of doing in connection with the violation of such statute.

Give the number of days and the classes of mail (first class only, first class and parcels, etc.) to be covered. No mail cover may remain in force for more than 30 days; if the information sought is obtained prior to the expiration of 30 days, the mail cover must be canceled. Requesting authorities may be granted additional 30-day periods under the same conditions applicable to the original request, but in no case may a mail cover remain in force longer than 120 days without the approval of the Chief Postal Inspector.

Protection and Return of Documentation Received from Mail Cover

All documentation received from the USPS as a result of a mail cover is to be treated in the strictest confidence while in the possession of INV. The USPS provides Mail Cover Results on USPS Form 2009. SAs may not photocopy this form. This form must be returned to the USPS within 60 days of receipt.

13.4 PHOTO SPREADS

The following guidelines should be adhered to when presenting a photo lineup:

Use at least six photographs depicting similar looking individuals.

If practical, the photos shall be unmarked. Notations (names, dates, and other information) should not be visible to witnesses. If block out is necessary to cover a notation on one photograph, then similar block out or covering marks must be placed on all photos in order that all will appear alike.

If there are two or more suspects, no two shall be presented together in a single photo spread.

If there are two or more witnesses, each witness should view the photo lineup separately and individually. Do not allow witnesses to talk to one another during the photo lineup procedure. Witnesses must not be permitted to consult with one another regarding their identification before, during, or after this procedure.

Each witness should initial and date a photocopy of the photo spread for the record, indicating whether or not any identification was made. The photo spread and copies shall be maintained in the case file for possible later use in court

proceedings.

When possible the photos used should be affixed into a Photo Display Folder, INV Form 15. Before showing the photo lineup, the witness should be informed that the group of photographs may or may not contain a photograph of the suspect.

The photo display folder containing all photos and or initialed photocopies used in the photo line-up must be processed as evidence. (Chapter 16.5)

The presentation of a photo line-up to a witness should be documented on an MOA.

13.5 PHOTOGRAPHY

When photographs and/or videotapes are taken during the course of an investigation, they will be appropriately labeled. Photographs, negatives, videotapes and digital images having investigative value should be placed in the evidence control system. (Chapter 16.5)

SAs should videotape and/or photograph sites both prior to and after the execution of a search warrant.

13.6 POLYGRAPH EXAMINATIONS

FO SACs may arrange for the services of polygraph examiners located in their districts when circumstances warrant.

All other polygraph requests will be directed to the DAIGI Field Operations through the FO SAC. The DAIGI will coordinate the request with the appropriate point of contact at the agency conducting the examination.

The United States Secret Service (USSS), the Defense Criminal Investigative Service (DCIS) and the OIG have entered into MOUs, which provides that they may administer polygraph examinations in DHS OIG investigations. (Exhibits 13-4 and 13-5)

Upon completion of the examination, the examiner will provide INV with a written report detailing the results.

All costs related to the administration of the polygraph examination (travel, lodging, and miscellaneous expenses) by the examining agency will be the responsibility of the DHS OIG.

13.7 COMPUTER FORENSICS

SACs will coordinate with the DAIGI Field Operations when they require computer forensic support. Field Operations will coordinate the request with SAs trained in Seized Computer Evidence Recovery System (SCERS). The USSS and the OIG have entered into an MOU that states that the USSS will provide INV with the forensic examination of computers and other electronic evidence. When the SCERS agent works for another agency, a written request may be required. All costs associated with forensic examination of computers will be the responsibility of DHS OIG. (**Exhibit 13-5**)

13.8 OTHER FORENSIC EXAMINATIONS

The USSS and the OIG have entered into an MOU which states that the USSS will provide INV with forensic support, such as document analysis, forensic photography, audio-video enhancement, handwriting examination, latent fingerprint examination, etc. **(Exhibit 13-5)**

Questions regarding forensic examinations should be directed to the DAIGI Field Operations.

13.9 TACTICAL PLANS FOR FIELD OPERATIONS

Tactical plans will be prepared prior to the initiation of field operations such as the execution of a search warrant, execution of an arrest warrant, engaging in an undercover operation, or other investigative activity as determined by the SAC. The plan should be prepared by an SA using INV Form 39, "Tactical Plan" and must be approved by a supervisor. The plan will be made part of the official case file. **(Exhibit 13-6)**

13.10 UNDERCOVER ACTIVITIES AND OPERATIONS

The OIG may use undercover activities or conduct undercover operations, which are appropriate to carry out its law enforcement responsibilities. The objective in utilizing undercover techniques is to obtain needed evidence against suspected criminals; and/or to advance an investigation to a higher or wider scale; and to reduce time and expenses involved in the completion of an investigation.

OIG investigations may require the use of undercover techniques. These techniques can prove to be essential in detecting, preventing, and prosecuting offenses involving the sale of federal documents, contractor fraud, alien smuggling conspiracies, and other violations of federal law. However, these techniques inherently involve an element of deception and may require cooperation with persons whose motivation and conduct are open to question, and so must be carefully considered and monitored.

Undercover Operations conducted by INV will comply with the Attorney General's Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority, and CIGIE standards for undercover operations. Depending on the type of undercover operation being planned, varying levels of approval will be needed before any proposed

operation can be initiated These guidelines do not apply to investigations utilizing confidential informants, cooperating witnesses or cooperating subjects, unless the investigation also utilizes an undercover DHS OIG employee or an employee of another OIG.

Undercover Employee: Any employee of DHS OIG, or employee of a Federal, state, or local law enforcement agency working under the direction and control of DHS OIG or another OIG in a particular investigation, whose relationship with DHS OIG or another OIG is concealed from third parties in the course of an investigative operation by the maintenance of a cover or alias identity.

Undercover Activities: Include any activities involving the use of an assumed name or cover identity by an employee of DHS OIG, or another Federal, state, or local law enforcement organization working with the OIG.

Undercover Operations: Include any investigation involving a series of related undercover activities over a period of time by an undercover employee(s). A series of related undercover activities generally consists of more than three separate substantive contacts by an undercover employee with the individual(s) under investigation. In the context of on-line communications such as e-mail and Internet Relay Chat, multiple transmissions or email messages can constitute one contact much like a series of verbal exchanges can comprise a single conversation.

Undercover activities involving sensitive or certain fiscal circumstances, constitutes an undercover operation regardless of the number of contacts involved.

Sensitive circumstances include:

> Sensitive targets, including members of Congress, a Federal judge, a member of the executive branch occupying a position for which compensation is set at the Executive Level IV of above, or a person who has served in such capacity within the previous two years;
>
> A significant investigation of a public official for bribery, conflict of interest, or extortion relating to the official's performance of duty;
>
> A significant investigation of a federal law enforcement official acting in his or her official capacity;
>
> An investigation of a member of the diplomatic corps of a foreign country;
>
> A person who is or has been a member of the Witness Security Program if that fact is known by the OIG;
>
> A public official, federal law enforcement officer, or other government employee or contract employee who is or has been involved in the operation of the Witness

Security program;

The use or targeting, in an undercover capacity, of a person who is in the custody of the Federal Bureau Of Prisons or the United States Marshals Service, or is under Federal Bureau of Prisons' supervision; (Chapter 11.3)

The use or targeting, in an undercover capacity, of a Federal Bureau of Prisons employee, if any part of the activity will occur within the confines of, or otherwise would be likely to affect security of, a Bureau of Prisons-administered facility. (Chapter 11.3)

Undercover operations that necessitate any of the following fiscal circumstances will need the approval of the IG:

1. [redacted]

2. Require the deposit of appropriated funds or proceeds generated by the undercover operation into banks or other financial institutions;

3. Use the proceeds generated by the undercover operation to offset necessary and reasonable expenses of the operation;

4. Require a reimbursement, compensation, or indemnification agreement with cooperating individuals or entities for services or losses incurred by them in aid of the operation (any such agreement entered into with third parties must be reviewed by the OIG's General Counsel and the OIG's resource management official or equivalent official); or

5. Exceed the limitations on duration or commitment of resources established by the IG for operations initiated.

Undercover Activities involving sensitive circumstances and all Undercover Operations require the approval of the AIGI. Requests for approval will be made through the SAC to the DAIGI Field Operations by memorandum and submitted two weeks prior to the beginning of the operation. When exigent circumstances exist, approval may be obtained verbally and a written request submitted as soon as possible, but not later than three working days. "Exigent circumstances" are those where there is a potential threat to life

or of bodily injury, or where failure to act could mean the destruction of essential evidence or the escape of a fleeing offender.

The memorandum must contain the following information:

Reason for activity: The request must include a reasonably detailed statement of the background of the case and related circumstances as to the need for the operation.

Offense: Include citation of the primary alleged offense.

Danger/Contingency Plans: Proposed actions to protect any participant in a special operation or the operation itself must be noted in this section. The request must also state the intended contingency plans.

Description and Location of Devices/Equipment: The request must specify what special equipment, such as monitoring or recording devices, will be used and where the devices will be concealed (i.e. on the person, in personal effects, or in a fixed location). When appropriate, this section should make reference to a Consensual Non-Telephone Monitoring Request. (Chapter 15.5)

Location of Operation: The request must specify the location and primary judicial district where the operation will take place. If the location changes, notice should be given promptly to the approving AUSA and INV official.

Duration and Dates: The request must state the length of time needed for the operation. Initially, an authorization may be granted for up to 90 days beginning with the day the operation is scheduled to begin. If there is a need to continue the operation beyond the approved date, extensions for periods of up to 90 days may be granted. The request must show the anticipated starting and ending dates of the activity.

Names: The names of the expected targeted individuals and/or enterprises in special or undercover operations must be provided, as well as the names of all operatives and their roles and responsibilities.

Trial Attorney Approval: The request must state that the facts of the investigation have been discussed with the Assistant United States Attorney in the judicial district where the activity will occur.

Potential for Criminal Activity: The request must include a discussion of anticipated activity during the operation that would constitute a crime under Federal, State, or local law if engaged in by a private person without approval of an appropriate Government official, and a proposal for dealing with the situation.

Unusual Expenses: If it is anticipated that the operation will incur expenses that

are above normal costs of business, the request must show the projected costs in detail; include travel, per diem, supplies, rewards, payments for information, and equipment necessary for the operation.

Before conducting an undercover operation lasting longer than six months or any undercover activity involving any of the sensitive circumstances listed above, INV must first notify the FBI. The FBI may choose to join the investigation, in which case the undercover operation would be subject to review by the FBI's Criminal Undercover Operations Review Committee. If the FBI decides not to join the investigation, the undercover operation will be reviewed by an Undercover Review Committee comprised from the community of Inspectors General as outlined in the Attorney General's guidelines for OIG with statutory law enforcement authority. (Chapter 2.5)

No undercover operation or activity involving sensitive circumstances may be conducted without the approval of one of these committees. The approval for each undercover operation involving sensitive circumstances must be renewed for each six-month period, or less, during which the undercover operation is ongoing.

All undercover operations must be documented in EDS by the investigating office.

13.11 INVESTIGATIONS INVOLVING ESPECIALLY SENSITIVE TARGETS

Criminal investigations involving especially sensitive targets typically result in a high level of public and governmental attention. Investigations involving one of the following circumstances require coordination with the DOJ Office of Enforcement Operations, and may be conducted without the participation of the FBI. In such instances notification of the investigation should not be made to any other agency without the explicit approval of the Office of Enforcement Operations.

A person who is or has been a member of the Witness Security Program, if that fact is known by the OIG;

A public official, federal law enforcement officer, or other government employee or contract employee who is or has been involved in the operation of the Witness Security program;

The use or targeting, in an undercover capacity, of a person who is in the custody of the Federal Bureau Of Prisons or the United States Marshals Service, or is under Federal Bureau of Prisons' supervision;
The use or targeting, in an undercover capacity, of a Federal Bureau of Prisons employee, if any part of the activity will occur within the confines of, or otherwise would be likely to affect security of, a Bureau of Prisons-administered facility.

The OIG is required to notify the FBI when investigations involve any of the following sensitive targets. The SAC should notify the FBI in writing within thirty days on

determining involvement of a sensitive target. The FBI may choose to join the investigation but is not required to do so.

Sensitive targets, including members of Congress, a Federal judge, a member of the executive branch occupying a position for which compensation is set at the Executive Level IV of above, or a person who has served in such capacity within the previous two years;

A significant investigation of a public official for bribery, conflict of interest, or extortion relating to the official's performance of duty;

A significant investigation of a federal law enforcement official acting in his or her official capacity;

An investigation of a member of the diplomatic corps of a foreign country.

13.12 ESTABLISHING UNDERCOVER IDENTITIES

[redacted]

13.13 IMMIGRATION SEARCHES

SAs have the specific authority by which, in the performance of official duties, they may board or search any vessel, aircraft, railway car, or other conveyance or vehicle in which aliens are believed to be transported into the United States illegally. Additionally, OIG SAs may detain individuals suspected of being undocumented aliens.

13.14 RACIAL PROFILING

SAs will follow provisions outlined in DOJ "Guidance Regarding the Use of Race by Federal Law Enforcement Agencies," dated June 2003. **(Exhibit 13-6)** Use of racial profiling is prohibited.

In making routine or spontaneous law enforcement decisions, federal law enforcement officers may not use race or ethnicity. Officers may rely on race and ethnicity in a specific suspect description.

In conducting activities in connection with a specific investigation, federal law enforcement officers may consider race and ethnicity only to the extent that there is trustworthy information, relevant to the locality or timeframe, that links persons of a particular race or ethnicity to identified criminal incident, scheme, or organization.

In investigating or preventing threats to national security or other catastrophic events, or in enforcing laws protecting the integrity of the Nations borders, federal law enforcement officers may not consider race or ethnicity except to the extent permitted by the Constitution and laws of the Unite States.

13.15 AFFECTING AN ARREST

INV policy provides that generally, an INV Form 39, "Tactical Plan" **(Exhibit 13-7)** will be prepared and approved by the investigating office SAC before the arrest warrant is executed.

Ideally, a minimum of two SAs should be present to affect an arrest. In all cases, the arrestee will be handcuffed (double-locked) and thoroughly searched. **Arrestees will be handcuffed behind their back.** SAs will inform all arrestees of their constitutional rights per Miranda at the earliest possible opportunity and prior to any interrogation. (Chapter 10.4)

Chapter 17.4 further outlines procedures for executing arrest warrants.

It is OIG policy that arrests will not be affected without a warrant unless exigent circumstances exist.

Prior to the arrest of a DHS employee or contractor, an INV Form-40, "Planned Employee Arrest Notification" **(Exhibit 13-8)** will be completed and forwarded to the DAIGI Field Operations and as far in advance as practical, but not later than 24-hours prior to the planned arrest absent exigent circumstances. This notification is to be emailed to the [redacted] email box with a carbon copy to the DIAGI Field Operations and SAC of Field Support. **No arrest warrant will be executed on DHS property without prior notification to the AIGI.**

After an individual has been arrested for whom you completed an INV-Form 40 or any individual associated with a DHS OIG investigation, an INVForm-40A, "Arrest Notification Report" is to be completed and submitted by the close of business the next business day after the arrest has occurred. The INV Form-40A has an email button and when selected, it will generate a draft email with the required INV headquarters email addresses preloaded for distribution and will automatically populate the email subject line with the following information: "SIA – Arrest Notification Report-." The case number

is to be inserted behind the last dash of the subject line before emailing the INV Form-40A.

13.16 OIG MUTUAL ASSISTANCE IN EXECUTION OF SEARCH AND ARREST WARRANTS

The Attorney General Order No. 3168-2010 **(Exhibit 13-9)** authorizes special agent of OIGs with law enforcement authority under 6(e) (1) (C) of the IG Act, to assist other OIGs. Assistance is authorized only for the purpose of supporting a specified search or arrest operation, not for other investigative activities, and for a specified period of time, generally not to exceed five days. When loaned to another OIG, agents can seek and execute federal warrants for arrest, conduct searches and seize evidence. Agents of the loaning IG will operate under the sole direction of the IG to whom they are providing assistance. The agreement and other terms of the loans will be memorialized in writing under provisions established by CIGIE. **(Exhibit 13-10)**

CHAPTER 13.0 - EXHIBITS

13-1 Memorandum of Understanding between the OIG and the United States Marshal Service, undated.

13-2 Mail Cover Letter of Request.

13-3 United States Postal Inspection Service Request for Mail Cover.

13-4 Memorandum of Understanding between the OIG and the Defense Criminal Investigative Service, dated August 11, 2003.

13-5 Memorandum of Understanding between the OIG and the United States Secret Service, Forensic Services Division, dated March 19, 2003.

13-6 DOJ Guidance Regarding the Use Of Race by Federal Law Enforcement Agencies.

13-7 INV Form 39, Tactical Plan.

13-8 INV Form 40, Notification of Planned Arrest.

13-8A INV Form 40A, Arrest Notification Report.

13-9 Attorney General Order No. 3168-2010.

13-10 CIGIE procedures for obtaining assistance from another OIG in the execution of search and arrest warrants.

Exhibit 13-1, MOU between the OIG and the United States Marshal Service

THE UNITED STATES MARSHALS SERVICE
AND
DEPARTMENT OF HOMELAND SECURITY
OFFICE OF INSPECTOR GENERAL

MEMORANDUM OF UNDERSTANDING
REGARDING ADMINISTRATIVE SUPPORT FOR
NATIONAL CRIME INFORMATION CENTER ENTRIES
AND FUGITIVE APPREHENSION RESONSIBILITIES

I. INTENT

This Memorandum of Understanding (MOU) provides general guidance with administrative support and apprehension responsibility offered by the United States Marshal Service (USMS) to the Department of Homeland Security, Office of Inspector General (DHS OIG) in entering felony warrants into the National Crime Information Center (NCIC) and the execution of DHS OIG felony warrants. In larger part, it formalizes procedures that are already in general practice by the parties to this agreement.

II. RESPONSIBILITIES OF THE DHS OIG

The DHS OIG will delegate administrative responsibility to the USMS with respect to NCIC entries. The DHS OIG may delegate apprehension authority to the USMS with respect to its felony warrants. The DHS OIG will provide to the USMS, at the field level, the following documents and information for all felony warrants to be entered into NCIC and investigated by the USMS:

1. The original warrant as received by the Clerk of the Court.
2. All mandatory information necessary to enter the warrant into NCIC; including, but not limited to: Name, Sex, Race, Date of Birth, Height, Weight, and Eye color.
3. Photograph and fingerprints, if available.
4. The name and twenty-four hour contact number of a DHS OIG Agent who will be responsible to respond in the event the fugitive is captured by another agency.

Upon receipt of a DHS OIG arrest warrant, DHS OIG will provide all information necessary to prepare an NCIC entry (see 1-4 above), along with a cover memorandum requesting that the USMS enter the warrant into NCIC.

Upon receipt of a DHS OIG arrest warrant; DHS OIG shall have seven (7) days to determine apprehension responsibility. If the subject of the arrest warrant is not

apprehended within seven (7) days after issuance of the arrest warrant, DHS OIG may delegate apprehension responsibility to the USMS. The delegation becomes effective upon written notification to the USMS by the DHS OIG. Warrants referred to the USMS for apprehension responsibility must be made, in writing, within one (1) year of the issuance of the warrant. The DHS OIG will retain apprehension responsibility for all warrants older that one (1) year.

III. RESPONSIBILITY OF THE USMS

The USMS will assume all NCIC administrative responsibility for DHS OIG wanted persons entries, updates, validations, and clears.

The USMS will utilize all available resources to locate and arrest the fugitive.

The USMS will provide twenty-four hour "hit" confirmation.

IV. EXCEPTIONS

Exceptions to these conditions may be made on a case-by-case basis with the concurrence of both agencies at the local level.

The USMS may refuse to accept administrative and apprehension responsibility for a DHS OIG fugitive warrant if DHS OIG fails to provide any one of the following:

1. The original warrant,
2. the mandatory information necessary to enter the fugitive into NCIC,
3. a twenty-four hour contact number for a DHS OIG Agent.

Upon refusal, the USMS will provide a written explanation of why the refusal occurred.

V. POST APPREHENSION GUIDELINES

DHS OIG agents will respond when notified by the USMS that a DHS OIG fugitive has been captured by another law enforcement agency. Upon positive verification, DHS OIG will immediately notify the USMS to expediently remove the fugitive from NCIC. The DHS OIG will immediately notify the appropriate USMS office if DHS OIG agents arrest a fugitive with an associated USMS NCIC entry, or if DHS OIG dismissed or otherwise disposed of the case involving the fugitive.

The USMS will advise the lead DHS OIG agent, or his designee, of a DHS OIG fugitive arrest, in order to ensure timely access to the arrestee.

VI. USMS AND DHS OIG

The USMS and DHS OIG generally agree that no NCIC entries will be made on sealed indictments, "Last Name Unknown/John Doe" cases, or any other case for which available data does not meet the minimal NCIC input requirements.

This agreement will remain in effect until terminated by written notice from either party. The written notice will be provided at least sixty days prior to the termination date. This agreement is effective upon approval and signature of both parties.

VII. ANNUAL REVIEW

This MOU becomes effective on the date it is signed by each participating agency. It will be reviewed annually and revised as necessary. The MOU may be revised at anytime upon agreement by both parties.

Elizabeth M. Redman
Assistant Inspector General for Investigations
Department of Homeland Security
Office of Inspector General

Robert J. Finan, II
Assistant Director of Investigations
United States Marshals Service

Exhibit 13-2, Mail Cover Letter of Request

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

DATE

Office of Investigations

U.S. Postal Inspection Service
Criminal Investigations Service Center Manager
ATTN: MC Specialist
222 South Riverside Plaza, Suite 1265
Chicago, IL 60606-6117

RESTRICTED INFORMATION

My office is currently conducting an official investigation, which involves the obtaining of evidence regarding the commission of a felony. The following reasons support my official request for a mail cover.

The Department of Homeland Security, Office of Inspector General (DHS-OIG), is conducting a criminal investigation regarding (b) (6) who is alleged to be conducting unauthorized government database queries regarding criminal associates. The mail cover would assist in identifying co-conspirators and financial institutions used by the subject. The subject utilizes the following address to receive mail.

Subject of mail cover:

All other names should be included, as the subject is known to use aliases and nominees. All mail received at the address is intended for delivery to

A mail cover for 30 days, for the aforementioned addresses, is requested for first class mail.

This investigation involves possible violations of the following criminal statutes:

Statute	Description	Penalty
18 USC 1030	Computer Fraud	10 Years
18 USC 798	Disclosing of Classified Information	10 Years

To the best of my knowledge, the name and the address of an attorney who represents the mail cover subject is unknown. If, during the period of the mail cover, the name and address of an attorney who is retained by subject becomes known to my office, such information will be promptly furnished to the U.S. Postal Inspection Service.

The subject of this mail cover is not under indictment. Should the subject be indicted or formally charged during the period of the mail cover, your office will be promptly notified so that the mail cover can be canceled.

The results of the mail cover should be sent to the agent below. If there are any questions concerning this request, he may be contacted at .

Name
Special Agent
DHS-OIG
Address

We understand the results of the mail cover, PS Forms 2009, are the property of the U.S. Postal Inspection Service, that they can be retained and maintained in our office or the appropriate agent's office, as an investigative tool for a period of 60 days. They then must be returned to the U.S. Postal Inspection Service, Criminal Investigations Service Center in Chicago, Illinois.

Sincerely,

Special Agent-in-Charge

Exhibit 13-3, United States Postal Inspection Service Request for Mail Cover

External Law Enforcement Agency
REQUEST FOR MAIL COVER

Complete all sections of the mail cover template below and attach a cover letter on your agency letterhead with an original signature by your immediate supervisor. These should be placed in an envelope endorsed RESTRICTED INFORMATION. Seal the request in the envelope, place it in a second envelope, and mail to the CISC. The mail cover request should be addressed as follows:

CISC Manager
Attn: MC Specialist
222 South Riverside Plaza, Suite 1265
Chicago, IL 60606-6117

For further instructions on mail cover requests submitted by external law enforcement agencies, please see Publication 55, USPS Procedures for Mail Cover Requests. This publication may be requested by contacting our Mail Covers Unit at 312-669-5673.

1. DATE OF REQUEST	2. TYPE OF REQUEST	3. NUMBER OF DAYS: Indicate the number of days requested:
	New Request: ☐ Extension: ☐ *(Complete **only** item 13)* Fugitive: ☐ *(Refer to Item 7)* Forfeiture: ☐ *(Refer to Item 8)*	30 days ☐ ***Fugitive Only:*** 30 days ☐ 60 days ☐

4. SUBJECT OF MAIL COVER NAME & ADDRESS: **Only one subject address may be requested on each mail cover template.** Identify the individual(s) or business(es) to be covered by indicating full name(s), address, and ZIP+4 Code:

Name(s):

Address:

City:

State & Zip +4:

If coverage of "All Other Names" receiving mail at the subject address listed above is needed, provide justification. Also, indicate any names that should be excluded from this request.

All Names at Subject Address: ☐ Yes (provide justification below) ☐ No

Justification:

5. INDICTMENT: Has the subject been formally charged, i.e. indictment or information with the offence that is the basis of this mail cover request? ☐ Yes ☐ No

6. ATTORNEY:

a) Does the subject(s) of the investigation have a known attorney? ☐ Yes ☐ No
If so, state the attorney's name and address.

b) If this request involves a fugitive, does the fugitive have a known attorney? ☐ Yes ☐ No
If so, state the attorney's name and address.

c) Is the mail cover subject a judicial officer (e.g. attorney, judge, etc.)? ☐ Yes ☐ No

October 2005

- 1 -
-RESTRCITED INFORMATION-

7. FUGITIVE: If the cover involves a fugitive, state the fugitive's name, aliases, and any relationship between the fugitive and the mail cover subject.

8. FORFEITURE: If the only purpose of the mail cover is to identify property for forfeiture, state the legal basis for the forfeiture investigation, including the applicable forfeiture statute.

9. VIOLATION: State the applicable violation description, statute number, and penalty. If this involves a fugitive and the statute for the warrant is Unlawful Flight or Failure to Appear, also state the original charge.

Violation Description, *e.g. Wire Fraud*:

Statute, *e.g. Title 18 USC 1343*:

Penalty, *e.g. Ten Years*:

Is this violation a felony with imprisonment more than one year? ☐ Yes ☐ No

10. REASONABLE GROUNDS:

a) Basis - How has the mail cover subject violated, or is suspected of violating, the criminal statute? Make a definite statement that an official investigation into the possible violation of this criminal statute, fugitive search, or asset forfeiture is being conducted and cite the applicable section(s) of the United States Code or applicable State or Local law. Explain in detail your justification.

b) Purpose – What information do you expect to obtain from the mail cover? How will the mail cover facilitate the investigation, including the location of property or assets for forfeiture, or the location of a fugitive, e.g. banking information, co-conspirators, etc.?

c) Connection - If the mail cover subject is not the subject of the investigation, describe the affiliation of the mail cover subject to the subject of the investigation.

11. CLASS OF MAIL: Indicate the class of mail requested. Justification must be included for other than First Class.

☐ First-Class Mail (Personal or business correspondence: Includes Priority Mail [generally over 11 oz.] and Express Mail)

☐ Package Services (Parcel Post, bound printed materials, media mail and library mail)

Provide further justification for these classes of mail:

☐ Periodicals (Magazines, newspapers) ☐ Foreign Mail

Justification: Justification:

☐ Standard Mail (Bulk Business Mail)

Justification:

12. SPECIAL INSTRUCTIONS: State any special instructions or concerns about this particular request.

13. REQUEST FOR EXTENSION: *(For an extension request, complete only the section below.)*

At the expiration of the mail cover period, or prior thereto, the requesting authority may request and be granted additional 30-day periods (60-day periods for fugitives). To ensure there is no gap in the mail cover, the extension request should be submitted a minimum of 10 days prior to the end of the mail cover. The requesting authority must provide a statement of the investigative benefits of the mail cover and the anticipated benefits to be derived from its extension. The request for an extension must state whether the subject has been indicted or an information filed and if the subject is represented by an attorney.

Per Postal Regulations, no mail cover shall remain in force longer than 120 continuous days unless personally approved for further extension by the Chief Postal Inspector.

(a) MAIL COVER REFERENCE NO.:

(b) State, in detail, how the results of the prior mail cover assisted, or did not assist, the investigation.

(c) Describe the anticipated benefits to be derived from this mail cover extension.

(d) Regarding the violation under investigation, has the subject's indictment status changed since the previous mail cover approval? ☐ Yes ☐ No

(e) Has the subject's legal representation status changed since the last mail cover approval? If so, state the nature of the change, including attorney's name and address. ☐ Yes ☐ No

October 2005

- 3 -

-RESTRCITED INFORMATION-

Mail covers are issued only to law enforcement agencies empowered by statute or regulation to conduct criminal investigations and are strictly controlled to assure proper use.

Mail Covers are an investigative tool, and are not to be used as an initial investigative step.

14. AGENCY NAME, REQUESTOR NAME, ADDRESS WHERE MAIL COVER RESULTS SHOULD BE MAILED (with Zip +4 code), TELEPHONE NUMBER, FAX NUMBER AND E-MAIL ADDRESS:

In order to process this request, all fields below are required to be completed (fax and e-mail are optional fields)

Agency Name:

Is this a law enforcement agency? ☒ Yes ☐ No

Requestor's First Name:

Requestor's Last Name:

Requestor's Title:

Address:

City/State/Zip + 4:

Telephone Number:

Fax Number:

E-Mail Address:

15. NAME, TITLE, AND SIGNATURE OF SUPERVISOR AUTHORIZING MAIL COVER REQUEST:

Supervisor's First Name

Supervisor's Last Name

Supervisor's Title

Supervisor's Address:

Supervisor's City/State/Zip + 4:

Supervisor's Telephone Number:

Supervisor's Signature and Date: _____

AN ELECTRONIC VERSION OF THIS FORM IS AVAILABLE UPON REQUEST BY CONTACTING THE MAIL COVERS UNIT AT 312-669-5673.

AS INFORMATION, ALL COMPLETED MAIL COVER REQUESTS WILL NEED TO BE SENT VIA THE UNITED STATES MAIL TO THE CRIMINAL INVESTIGATIONS SERVICE CENTER PER INSTRUCTIONS AT THE TOP OF THE FIRST PAGE OF THIS TEMPLATE.

(For CISC Internal Use Only)

Reviewer's Initials & Date: _____

October 2005

- 4 -

-RESTRCITED INFORMATION-

Exhibit 13-4, MOU between the OIG and the Defense Criminal Investigative Service

MEMORANDUM OF UNDERSTANDING
BETWEEN
THE DEFENSE CRIMINAL INVESTIGATIVE SERVICE
AND
THE OFFICE OF INSPECTOR GENERAL
U.S. DEPARTMENT OF HOMELAND SECURITY

I. Introduction

This Memorandum of Understanding (MOU) is entered into between the Defense Criminal Investigative Service (DCIS) and the U.S. Department of Homeland Security (DHS), Office of Inspector General (OIG), for the administration of polygraph examinations by DCIS polygraph examiners in OIG-DHS investigations.

II. Administration

The determination to administer a polygraph examination will be made on a case-by-case basis following receipt by DCIS of a request letter from the OIG-DHS. The letter will detail the investigative activities to date, to include the results of the subject interview.

After consultation between the DCIS examiner and the OIG-DHS case agent, the decision to utilize the polygraph will be made by DCIS. Upon completion of the test, the DCIS examiner will provide the OIG-DHS case agent with a written report detailing the results of the examination.

III. Areas of Cooperation

All costs related to the administration of the polygraph examination outside the Washington, D.C. Metropolitan Area (travel, lodging, and miscellaneous expenses) will be the responsibility of the OIG-DHS.

IV. Implementation

It is DCIS' policy to handle all polygraph examinations in an expeditious manner; however, if competition for staff resources is present, DCIS cases will have priority over OIG-DHS cases unless extenuating conditions warrant a change in priority.

V. **Administration**

This Memorandum of Understand between DCIS and the OIG-DHS will remain in effect until such time as either party rescinds the agreement in writing.

Approved by:

Charles W. Beardall Date
Director
Defense Criminal Investigative Service

Clark Kent Ervin Date
Acting Inspector General
U.S. Department of Homeland Security

Exhibit 13-5, MOU Between OIG and U.S. Secret Service Forensic Services Division

MEMORANDUM OF UNDERSTANDING
BETWEEN
FORENSIC SERVICES DIVISION,
UNITED STATES SECRET SERVICE,
AND
DEPARTMENT OF HOMELAND SECURITY
OFFICE OF THE INSPECTOR GENERAL

I. INTRODUCTION

This document constitutes an agreement between the United States Secret Service (USSS) and the Department of Homeland Security, Office of Inspector General (DHS-OIG). The purpose of this agreement is to formalize policies, procedures, and responsibilities related to the USSS providing forensic support and expert testimony on behalf of the DHS-OIG.

II. MISSION STATEMENT

The Forensic Services Division (FSD) mission is to provide forensic/technical support services to USSS elements and other federal, state, county, and local law enforcement agencies when requested and available.

III. AREAS OF COOPERATIONS

a. Assistance is offered to the DHS-OIG, in the examination of handwriting / hand-printing, threat letter searches through the Forensic Information System for Handwriting (FISH), document examination, ink comparisons and age determination, audio/video enhancement, fingerprint development and comparison, Automated Fingerprint Identification System (AFIS) searches, forensic photography, polygraph examinations and forensic examination of computer and other electronic evidence.

b. Seminars will be offered to the DHS-OIG officials, when requested to familiarize DHS-OIG personnel with the capabilities of FSD support. Crime scene search operations are available, but will be authorized on a case-by-case basis.

c. DHS-OIG will pay all mission specific travel costs (per diem and transportation) incurred by FSD representatives. All requests for services will be made and provided consistent with the provisions of the Economy Act, 31 USC 1535.

IV. IMPLEMENTATION

The DHS-OIG understands that USSS cases have priority in forensic examinations. The USSS FSD currently prioritizes cases submitted for examination based on the importance placed on the investigation by the USSS or upon the requirements of the judicial system. The DHS-OIG will establish a similar system to ensure that those cases deemed most important will be given the proper attention by FSD. At its discretion, DHS-OIG may use other forensic technology and other laboratories.

V. ADMINISTRATION

This Memorandum of Understanding between the USSS - FSD and DHS-OIG will remain in effect unless revoked, in writing, by either party.

APPROVED BY:

for James D. Dunlap 3/19/03
George D. Rogers Date
Assistant Director-Investigations
United States Secret Service

3/18/03
Clark K. Ervin Date
(Acting) Inspector General
Department of Homeland Security

Exhibit 13-6, INV Form 39, Tactical Plan

Office of Inspector General - Investigations
U.S. Department of Homeland Security

Homeland Security

TACTICAL PLAN

Case Name:

Case Number:

Case Agent: **Telephone:**

Supervisor: **Telephone:**

Case Synopsis:

Operation Prosecutor: **Telephone:**

Target Information:

	Name	Physical Description	Photo (Y/N)
1.			
2.			
3.			
4.			
5.			
6.			

Target Vehicles:

	State/License Plate	Year	Make	Model	Color/Misc.
1.					
2.					
3.					
4.					
5.					
6.					

INV FORM-39

Page 1 of 5

TACTICAL PLAN

Warnings (i.e. [redacted]

Communications:

Radio – Primary:
Radio – Secondary:

Name	Cell Number

Emergency Services:

Hospital:
Address:
Map Attached (Y/N):

Local Police Coordination:

Agency:
Telephone:
Watch Commander:

Team Staging ***(Briefing Locations, Time, etc.)***:

TACTICAL PLAN

Equipment:

Personnel Responsibilities:

Assignment Codes:

[redacted]

	Name	Agency	Assignment	Equipment	Vehicle	Phone/Pager
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10						

TACTICAL PLAN

Undercover agent and/or confidential informant present:

☐ No ☐ Yes (*explain situation & details*)

Danger Signals:

☐ Visual (*describe*):

☐ Verbal (*describe*):

Target Location:

Address:

Type: ☐ Business (*name*):
☐ Residence
☐ Apartment (*name*):
☐ Farm Building
☐ Other (*describe*):

Owner/Occupant of Target Location (*name & description*):

Date & time for warrant execution:

Date & time for debriefing:

Tactical Plan prepared by SA: **Date:**

Tactical Plan approved by SAC/ASAC: **Date:**

INV FORM-39

Exhibit 13-7, DOJ Guidance Regarding the Use of Race by Fed. Law Enforcement Agencies

U.S. Department of Justice
Civil Rights Division

GUIDANCE REGARDING THE USE OF RACE BY FEDERAL LAW ENFORCEMENT AGENCIES

June 2003

INTRODUCTION AND EXECUTIVE SUMMARY

In his February 27, 2001, Address to a Joint Session of Congress, President George W. Bush declared that racial profiling is "wrong and we will end it in America." He directed the Attorney General to review the use by Federal law enforcement authorities of race as a factor in conducting stops, searches and other law enforcement investigative procedures. The Attorney General, in turn, instructed the Civil Rights Division to develop guidance for Federal officials to ensure an end to racial profiling in law enforcement.

"Racial profiling" at its core concerns the invidious use of race or ethnicity as a criterion in conducting stops, searches and other law enforcement investigative procedures. It is premised on the erroneous assumption that any particular individual of one race or ethnicity is more likely to engage in misconduct than any particular individual of another race or ethnicity.

Racial profiling in law enforcement is not merely wrong, but also ineffective. Race-based assumptions in law enforcement perpetuate negative racial stereotypes that are harmful to our rich and diverse democracy, and materially impair our efforts to maintain a fair and just society.[1]

The use of race as the basis for law enforcement decision-making clearly has a terrible cost, both to the individuals who suffer invidious discrimination and to the Nation, whose goal of "liberty and justice for all" recedes with every act of such discrimination. For this reason, this guidance in many cases imposes more restrictions on the consideration of race and ethnicity in Federal law enforcement than the Constitution requires.[2] This guidance prohibits racial profiling in law enforcement practices without hindering the important work of our Nation's public safety officials, particularly the intensified anti-terrorism efforts precipitated by the events of September 11, 2001.

---

[1] *See United States v. Montero-Camargo*, 208 F.3d 1122, 1135 (9th Cir. 2000) ("Stops based on race or ethnic appearance send the underlying message to all our citizens that those who are not white are judged by the color of their skin alone.").

[2] This guidance is intended only to improve the internal management of the executive branch. It is not intended to, and does not, create any right, benefit, trust, or responsibility, whether substantive or procedural, enforceable at law or equity by a party against the United States, its departments, agencies, instrumentalities, entities, officers, employees, or agents, or any person, nor does it create any right of review in an administrative, judicial or any other proceeding.

I. **Traditional Law Enforcement Activities.** Two standards in combination should guide use by Federal law enforcement authorities of race or ethnicity in law enforcement activities:

- **In making routine or spontaneous law enforcement decisions, such as ordinary traffic stops, Federal law enforcement officers may not use race or ethnicity to any degree, except that officers may rely on race and ethnicity in a specific suspect description. This prohibition applies even where the use of race or ethnicity might otherwise be lawful.**

- **In conducting activities in connection with a specific investigation, Federal law enforcement officers may consider race and ethnicity only to the extent that there is trustworthy information, relevant to the locality or time frame, that links persons of a particular race or ethnicity to an identified criminal incident, scheme, or organization. This standard applies even where the use of race or ethnicity might otherwise be lawful.**

II. **National Security and Border Integrity.** The above standards do not affect current Federal policy with respect to law enforcement activities and other efforts to defend and safeguard against threats to national security or the integrity of the Nation's borders,[3] to which the following applies:

- **In investigating or preventing threats to national security or other catastrophic events (including the performance of duties related to air transportation security), or in enforcing laws protecting the integrity of the Nation's borders, Federal law enforcement officers may not consider race or ethnicity except to the extent permitted by the Constitution and laws of the United States.**

Any questions arising under these standards should be directed to the Department of Justice.

[3] This guidance document does not apply to U.S. military, intelligence, protective or diplomatic activities conducted consistent with the Constitution and applicable Federal law.

2

THE CONSTITUTIONAL FRAMEWORK

"[T]he Constitution prohibits selective enforcement of the law based on considerations such as race." *Whren v. United States*, 517 U.S. 806, 813 (1996). Thus, for example, the decision of federal prosecutors "whether to prosecute may not be based on 'an unjustifiable standard such as race, religion, or other arbitrary classification.'"[4] *United States v. Armstrong*, 517 U.S. 456, 464 (1996) (quoting *Oyler v. Boles*, 368 U.S. 448, 456 (1962)). The same is true of Federal law enforcement officers. Federal courts repeatedly have held that any general policy of "utiliz[ing] impermissible racial classifications in determining whom to stop, detain, and search" would violate the Equal Protection Clause. *Chavez v. Illinois State Police*, 251 F.3d 612, 635 (7th Cir. 2001). As the Sixth Circuit has explained, "[i]f law enforcement adopts a policy, employs a practice, or in a given situation takes steps to initiate an investigation of a citizen based solely upon that citizen's race, without more, then a violation of the Equal Protection Clause has occurred." *United States v. Avery*, 137 F.3d 343, 355 (6th Cir. 1997). "A person cannot become the target of a police investigation solely on the basis of skin color. Such selective law enforcement is forbidden." *Id.* at 354.

As the Supreme Court has held, this constitutional prohibition against selective enforcement of the law based on race "draw[s] on 'ordinary equal protection standards.'" *Armstrong*, 517 U.S. at 465 (quoting *Wayte v. United States*, 470 U.S. 598, 608 (1985)). Thus, impermissible selective enforcement based on race occurs when the challenged policy has "'a discriminatory effect and . . . was motivated by a discriminatory purpose.'" *Id.* (quoting *Wayte*, 470 U.S. at 608).[5] Put simply, "to the extent that race is used as a proxy" for criminality, "a racial stereotype requiring strict scrutiny is in operation." *Cf. Bush v. Vera*, 517 U.S. at 968 (plurality).

I. GUIDANCE FOR FEDERAL OFFICIALS ENGAGED IN LAW ENFORCEMENT ACTIVITIES

A. Routine or Spontaneous Activities in Domestic Law Enforcement

In making routine or spontaneous law enforcement decisions, such as ordinary traffic stops, Federal law enforcement officers may not use race or ethnicity to any degree, except that officers may rely on race and ethnicity in a specific suspect description. This prohibition

[4] These same principles do not necessarily apply to classifications based on alienage. For example, Congress, in the exercise of its broad powers over immigration, has enacted a number of provisions that apply only to aliens, and enforcement of such provisions properly entails consideration of a person's alien status.

[5] Invidious discrimination is not necessarily present whenever there is a "disproportion" between the racial composition of the pool of persons prosecuted and the general public at large; rather, the focus must be the pool of "*similarly situated* individuals of a different race [who] were not prosecuted." *Armstrong*, 517 U.S. at 465 (emphasis added). "[R]acial disproportions in the level of prosecutions for a particular crime may be unobjectionable if they merely reflect racial disproportions in the commission of that crime." *Bush v. Vera*, 517 U.S. 952, 968 (1996) (plurality).

applies even where the use of race or ethnicity might otherwise be lawful.

Federal law enforcement agencies and officers sometimes engage in law enforcement activities, such as traffic and foot patrols, that generally do not involve either the ongoing investigation of specific criminal activities or the prevention of catastrophic events or harm to the national security. Rather, their activities are typified by spontaneous action in response to the activities of individuals whom they happen to encounter in the course of their patrols and about whom they have no information other than their observations. These general enforcement responsibilities should be carried out without *any* consideration of race or ethnicity.

- ***Example***: While parked by the side of the George Washington Parkway, a Park Police Officer notices that nearly all vehicles on the road are exceeding the posted speed limit. Although each such vehicle is committing an infraction that would legally justify a stop, the officer may not use race or ethnicity as a factor in deciding which motorists to pull over. Likewise, the officer may not use race or ethnicity in deciding which detained motorists to ask to consent to a search of their vehicles.

Some have argued that overall discrepancies in certain crime rates among racial groups could justify using race as a factor in general traffic enforcement activities and would produce a greater number of arrests for non-traffic offenses (*e.g.*, narcotics trafficking). We emphatically reject this view. The President has made clear his concern that racial profiling is morally wrong and inconsistent with our core values and principles of fairness and justice. Even if there were overall statistical evidence of differential rates of commission of certain offenses among particular races, the affirmative use of such generalized notions by federal law enforcement officers in routine, spontaneous law enforcement activities is tantamount to stereotyping. It casts a pall of suspicion over every member of certain racial and ethnic groups without regard to the specific circumstances of a particular investigation or crime, and it offends the dignity of the individual improperly targeted. Whatever the motivation, it is patently unacceptable and thus prohibited under this guidance for Federal law enforcement officers to act on the belief that race or ethnicity signals a higher risk of criminality. This is the core of "racial profiling" and it must not occur.

The situation is different when an officer has specific information, based on trustworthy sources, to "be on the lookout" for specific individuals identified at least in part by race or ethnicity. In such circumstances, the officer is not acting based on a generalized assumption about persons of different races; rather, the officer is helping locate specific individuals previously identified as involved in crime.

- ***Example***: While parked by the side of the George Washington Parkway, a Park Police Officer receives an "All Points Bulletin" to be on the look-out for a fleeing bank robbery suspect, a man of a particular race and particular hair color in his 30s driving a blue automobile. The Officer may use this description, including the race of the particular suspect, in deciding which speeding motorists to pull over.

4

B. **Law Enforcement Activities Related to Specific Investigations**

In conducting activities in connection with a specific investigation, Federal law enforcement officers may consider race and ethnicity only to the extent that there is trustworthy information, relevant to the locality or time frame, that links persons of a particular race or ethnicity to an identified criminal incident, scheme, or organization. This standard applies even where the use of race or ethnicity might otherwise be lawful.

As noted above, there are circumstances in which law enforcement activities relating to particular identified criminal incidents, schemes or enterprises may involve consideration of personal identifying characteristics of potential suspects, including age, sex, ethnicity or race. Common sense dictates that when a victim describes the assailant as being of a particular race, authorities may properly limit their search for suspects to persons of that race. Similarly, in conducting an ongoing investigation into a specific criminal organization whose membership has been identified as being overwhelmingly of one ethnicity, law enforcement should not be expected to disregard such facts in pursuing investigative leads into the organization's activities.

Reliance upon generalized stereotypes is absolutely forbidden. Rather, use of race or ethnicity is permitted only when the officer is pursuing a specific lead concerning the identifying characteristics of persons involved in an *identified* criminal activity. The rationale underlying this concept carefully limits its reach. In order to qualify as a legitimate investigative lead, the following must be true:

- The information must be relevant to the locality or time frame of the criminal activity;
- The information must be trustworthy;
- The information concerning identifying characteristics must be tied to a particular criminal incident, a particular criminal scheme, or a particular criminal organization.

The following policy statements more fully explain these principles.

1. ***Authorities May Never Rely on Generalized Stereotypes, But May Rely Only on Specific Race- or Ethnicity-Based Information***

This standard categorically bars the use of generalized assumptions based on race.

- ***Example***: In the course of investigating an auto theft in a federal park, law enforcement authorities could not properly choose to target individuals of a particular race as suspects, based on a generalized assumption that those individuals are more likely to commit crimes.

This bar extends to the use of race-neutral pretexts as an excuse to target minorities. Federal law enforcement may not use such pretexts. This prohibition extends to the use of other, facially race-

5

neutral factors as a proxy for overtly targeting persons of a certain race or ethnicity. This concern arises most frequently when aggressive law enforcement efforts are focused on "high crime areas." The issue is ultimately one of motivation and evidence; certain seemingly race-based efforts, if properly supported by reliable, empirical data, are in fact race-neutral.

- ***Example***: In connection with a new initiative to increase drug arrests, local authorities begin aggressively enforcing speeding, traffic, and other public area laws in a neighborhood predominantly occupied by people of a single race. The choice of neighborhood was not based on the number of 911 calls, number of arrests, or other pertinent reporting data specific to that area, but only on the general assumption that more drug-related crime occurs in that neighborhood because of its racial composition. This effort would be improper because it is based on generalized stereotypes.

- ***Example:*** Authorities seeking to increase drug arrests use tracking software to plot out where, if anywhere, drug arrests are concentrated in a particular city, and discover that the clear majority of drug arrests occur in particular precincts that happen to be neighborhoods predominantly occupied by people of a single race. So long as they are not motivated by racial animus, authorities can properly decide to enforce all laws aggressively in that area, including less serious quality of life ordinances, as a means of increasing drug-related arrests. *See, e.g., United States v. Montero-Camargo*, 208 F.3d 1122, 1138 (9th Cir. 2000) ("We must be particularly careful to ensure that a 'high crime' area factor is not used with respect to entire neighborhoods or communities in which members of minority groups regularly go about their daily business, but is limited to specific, circumscribed locations where particular crimes occur with unusual regularity.").

By contrast, where authorities are investigating a crime and have received *specific information* that the suspect is of a certain race (*e.g.*, direct observations by the victim or other witnesses), authorities may reasonably use that information, even if it is the only descriptive information available. In such an instance, it is the victim or other witness making the racial classification, and federal authorities may use reliable incident-specific identifying information to apprehend criminal suspects. Agencies and departments, however, must use caution in the rare instance in which a suspect's race is the only available information. Although the use of that information may not be unconstitutional, broad targeting of discrete racial or ethnic groups always raises serious fairness concerns.

- ***Example***: The victim of an assault at a local university describes her assailant as a young male of a particular race with a cut on his right hand. The investigation focuses on whether any students at the university fit the victim's description. Here investigators are properly relying on a description given by the victim, part of which included the assailant's race. Although the ensuing investigation affects students of a particular

race, that investigation is not undertaken with a discriminatory purpose. Thus use of race as a factor in the investigation, in this instance, is permissible.

2. ***The Information Must be Relevant to the Locality or Time Frame***

Any information concerning the race of persons who may be involved in specific criminal activities must be locally or temporally relevant.

- ***Example***: DEA issues an intelligence report that indicates that a drug ring whose members are known to be predominantly of a particular race or ethnicity is trafficking drugs in Charleston, SC. An agent operating in Los Angeles reads this intelligence report. In the absence of information establishing that this intelligence is also applicable in Southern California, the agent may not use ethnicity as a factor in making local law enforcement decisions about individuals who are of the particular race or ethnicity that is predominant in the Charleston drug ring.

3. ***The Information Must be Trustworthy***

Where the information concerning potential criminal activity is unreliable or is too generalized and unspecific, use of racial descriptions is prohibited.

- ***Example***: ATF special agents receive an uncorroborated anonymous tip that a male of a particular race will purchase an illegal firearm at a Greyhound bus terminal in a racially diverse North Philadelphia neighborhood. Although agents surveilling the location are free to monitor the movements of whomever they choose, the agents are prohibited from using the tip information, without more, to target any males of that race in the bus terminal. *Cf. Morgan v. Woessner*, 997 F.2d 1244, 1254 (9th Cir. 1993) (finding no reasonable basis for suspicion where tip "made all black men suspect"). The information is neither sufficiently reliable nor sufficiently specific.

4. ***Race- or Ethnicity-Based Information Must Always be Specific to Particular Suspects or Incidents, or Ongoing Criminal Activities, Schemes, or Enterprises***

These standards contemplate the appropriate use of both "suspect-specific" and "incident-specific" information. As noted above, where a crime has occurred and authorities have eyewitness accounts including the race, ethnicity, or other distinguishing characteristics of the perpetrator, that information may be used. Federal authorities may also use reliable, locally relevant information linking persons of a certain race or ethnicity to a particular incident, unlawful scheme, or ongoing criminal enterprise – even absent a description of any particular individual suspect. In certain cases, the circumstances surrounding an incident or ongoing criminal activity will point strongly to a perpetrator of a certain race, even though authorities lack an eyewitness account

- ***Example***: The FBI is investigating the murder of a known gang member and has information that the shooter is a member of a rival gang. The FBI knows that the members of the rival gang are exclusively members of a certain ethnicity. This information, however, is not suspect-specific because there is no description of the particular assailant. But because authorities have reliable, locally relevant information linking a rival group with a distinctive ethnic character to the murder, Federal law enforcement officers could properly consider ethnicity in conjunction with other appropriate factors in the course of conducting their investigation. Agents could properly decide to focus on persons dressed in a manner consistent with gang activity, but ignore persons dressed in that manner who do not appear to be members of that particular ethnicity.

It is critical, however, that there be reliable information that ties persons of a particular description to a specific criminal incident, ongoing criminal activity, or particular criminal organization. Otherwise, any use of race runs the risk of descending into reliance upon prohibited generalized stereotypes.

- ***Example***: While investigating a car theft ring that dismantles cars and ships the parts for sale in other states, the FBI is informed by local authorities that it is common knowledge locally that most car thefts in that area are committed by individuals of a particular race. In this example, although the source (local police) is trustworthy, and the information potentially verifiable with reference to arrest statistics, there is no particular incident- or scheme- specific information linking individuals of that race to the particular interstate ring the FBI is investigating. Thus, without more, agents could not use ethnicity as a factor in making law enforcement decisions in this investigation.

Note that these standards allow the use of reliable identifying information about planned future crimes. Where federal authorities receive a credible tip from a reliable informant regarding a planned crime that has not yet occurred, authorities may use this information under the same restrictions applying to information obtained regarding a past incident. A prohibition on the use of reliable prospective information would severely hamper law enforcement efforts by essentially compelling authorities to wait for crimes to occur, instead of taking pro-active measures to prevent crimes from happening.

- ***Example***: While investigating a specific drug trafficking operation, DEA special agents learn that a particular methamphetamine distribution ring is manufacturing the drug in California, and plans to have couriers pick up shipments at the Sacramento, California airport and drive the drugs back to Oklahoma for distribution. The agents also receive trustworthy information that the distribution ring has specifically chosen to hire older couples of a particular race to act as the couriers. DEA agents may properly target older couples of that particular race driving vehicles with indicia such as Oklahoma plates near the Sacramento airport.

8

II. GUIDANCE FOR FEDERAL OFFICIALS ENGAGED IN LAW ENFORCEMENT ACTIVITIES INVOLVING THREATS TO NATIONAL SECURITY OR THE INTEGRITY OF THE NATION'S BORDERS

In investigating or preventing threats to national security or other catastrophic events (including the performance of duties related to air transportation security), or in enforcing laws protecting the integrity of the Nation's borders, Federal law enforcement officers may not consider race or ethnicity except to the extent permitted by the Constitution and laws of the United States.

Since the terrorist attacks on September 11, 2001, the President has emphasized that federal law enforcement personnel must use every legitimate tool to prevent future attacks, protect our Nation's borders, and deter those who would cause devastating harm to our Nation and its people through the use of biological or chemical weapons, other weapons of mass destruction, suicide hijackings, or any other means. "It is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation." *Haig v. Agee*, 453 U.S. 280, 307 (1981) (quoting *Aptheker v. Secretary of State*, 378 U.S. 500, 509 (1964)).

The Constitution prohibits consideration of race or ethnicity in law enforcement decisions in all but the most exceptional instances. Given the incalculably high stakes involved in such investigations, however, Federal law enforcement officers who are protecting national security or preventing catastrophic events (as well as airport security screeners) may consider race, ethnicity, and other relevant factors to the extent permitted by our laws and the Constitution. Similarly, because enforcement of the laws protecting the Nation's borders may necessarily involve a consideration of a person's alienage in certain circumstances, the use of race or ethnicity in such circumstances is properly governed by existing statutory and constitutional standards. *See, e.g., United States v. Brignoni-Ponce*, 422 U.S. 873, 886-87 (1975).[6] This policy will honor the rule of law and promote vigorous protection of our national security.

As the Supreme Court has stated, all racial classifications by a governmental actor are subject to the "strictest judicial scrutiny." *Adarand Constructors, Inc. v. Peña*, 515 U.S. 200, 224-25 (1995). The application of strict scrutiny is of necessity a fact-intensive process. *Id.* at 236. Thus, the legality of particular, race-sensitive actions taken by Federal law enforcement officials in the context of national security and border integrity will depend to a large extent on the circumstances at hand. In absolutely no event, however, may Federal officials assert a national security or border integrity rationale as a mere pretext for invidious discrimination. Indeed, the very purpose of the strict scrutiny test is to "smoke out" illegitimate use of race, *Adarand*, 515 U.S. at 226 (quoting *Richmond v. J.A.*

[6] Moreover, as in the traditional law enforcement context described in the second standard, *supra*, officials involved in homeland security may take into account specific, credible information about the descriptive characteristics of persons who are affiliated with identified organizations that are actively engaged in threatening the national security.

Croson Co., 488 U.S. 469, 493 (1989)), and law enforcement strategies not actually premised on *bona fide* national security or border integrity interests therefore will not stand.

In sum, constitutional provisions limiting government action on the basis of race are wide-ranging and provide substantial protections at every step of the investigative and judicial process. Accordingly, and as illustrated below, when addressing matters of national security, border integrity, or the possible catastrophic loss of life, existing legal and constitutional standards are an appropriate guide for Federal law enforcement officers.

- ***Example***: The FBI receives reliable information that persons affiliated with a foreign ethnic insurgent group intend to use suicide bombers to assassinate that country's president and his entire entourage during an official visit to the United States. Federal law enforcement may appropriately focus investigative attention on identifying members of that ethnic insurgent group who may be present and active in the United States and who, based on other available information, might conceivably be involved in planning some such attack during the state visit.

- ***Example***: U.S. intelligence sources report that terrorists from a particular ethnic group are planning to use commercial jetliners as weapons by hijacking them at an airport in California during the next week. Before allowing men of that ethnic group to board commercial airplanes in California airports during the next week, Transportation Security Administration personnel, and other federal and state authorities, may subject them to heightened scrutiny.

Because terrorist organizations might aim to engage in unexpected acts of catastrophic violence in any available part of the country (indeed, in multiple places simultaneously, if possible), there can be no expectation that the information must be specific to a particular locale or even to a particular identified scheme.

Of course, as in the example below, reliance solely upon generalized stereotypes is forbidden.

- ***Example***: At the security entrance to a Federal courthouse, a man who appears to be of a particular ethnicity properly submits his briefcase for x-ray screening and passes through the metal detector. The inspection of the briefcase reveals nothing amiss, the man does not activate the metal detector, and there is nothing suspicious about his activities or appearance. In the absence of any threat warning, the federal security screener may not order the man to undergo a further inspection solely because he appears to be of a particular ethnicity.

Exhibit 13-8, INV Form 40, Notification of Planned Arrest

Office of Inspector General - Investigations
U.S. Department of Homeland Security

Homeland Security

INTERNAL PLANNED ARREST NOTIFICATION

INV Field Office:

Case Number:

Expected Date of Arrest:

Expected Time of Arrest:

Name of Arrestee:

Position/Job Title:

Grade:

Duty Station:

Expected location of arrest:

Name of lead agency:

Description of crime allegedly committed by arrestee:

United States Attorney's Office Prosecuting the Employee:

INV FORM-40 (March 2011)

Law Enforcement Sensitive

Exhibit 13-8A, INV Form 40A, Arrest Notification Report

Office of Inspector General - Investigations
U.S. Department of Homeland Security

Arrest Notification

Homeland Security

Case Number: _____ Arrest Date : _____ Arrest Location: _____

Subject Name: _____ Alias/Nickname: _____

Sex: _____ Race: _____ DOB : _____ SSN: _____

Field Office: _____ Violation: _____ Jurisdiction: _____

Bureau Affected: _____ ☐ DHS Employee Only ☐ Non-DHS Employees

Position: _____ Grade: ___ Duty Station: _____

Disposition (If Known): _____ Other Agency Number: _____

ICE Alien Number: _____ Misc Number: _____

Details:

INV Form - 40A (March 2011)

Office of Inspector General - Investigations
U.S. Department of Homeland Security

Arrest Notification

Homeland Security

Details - continued:

Special Agent in Charge: _____

Public Affairs : _____

Other Points of Contact: _____

INV Form - 40A (March 2011)

Exhibit 13-9, Attorney General Order No. 3168-2010

Office of the Attorney General
Washington, D.C. 20530

ORDER NO. 3168-2010

AUTHORIZATION FOR THE FEDERAL OFFICES
OF INSPECTOR GENERAL TO PROVIDE MUTUAL ASSISTANCE
IN THE EXECUTION OF SEARCH AND ARREST WARRANTS

By virtue of the authority vested in me as the Attorney General by law, including by the Inspector General Act of 1978 (the "IG Act"), as amended, I hereby order as follows:

1. I authorize special agents of each Office of Inspector General ("OIG") otherwise authorized to exercise powers under subsection 6(e)(1)(C) of the IG Act, when loaned to another OIG whose Inspector General ("IG") is also otherwise authorized to exercise powers under subsection 6(e)(1)(C) of the IG Act, to seek and execute warrants issued under the authority of the United States for arrest, search of a premises, or seizure of evidence. This authorization shall extend to the number of agents that the loaning IG or, at his discretion the Assistant Inspector General for Investigations reporting to him, deems appropriate. Agents of the loaning IG shall operate under the direction of the IG to whom they are providing assistance. The loaning IG shall not direct agents as they assist the requesting IG.

2. Assistance provided by one IG to another pursuant to the authority granted in this order must comply with procedures to be established by the Council of Inspectors General on Integrity and Efficiency.

3. Such assistance is authorized only for the purposes of supporting a specified search or arrest operation. Assistance is not authorized for other investigative activities. The duration of the assistance shall be agreed upon by both IGs and generally should not exceed five days. The IGs shall memorialize this agreement and the other terms of the loan in writing.

June 28, 2010
Date

Eric H. Holder, Jr.
Attorney General

2

Exhibit 13-10, Procedures for Obtaining Assistance from Another OIG in the Execution of Search and Arrest Warrants

PROCEDURES TO OBTAIN ASSISTANCE FROM ANOTHER OIG IN THE EXECUTION OF SEARCH AND ARREST WARRANTS

I. Purpose

The purpose of this policy is to provide procedures through which willing Federal Offices of Inspector General may seek and obtain additional manpower for the execution of search and/or arrest warrants.

II. Background

On June 28, 2010, the Attorney General issued Order No. 3168-2010, which authorized

> special agents of each Office of Inspector General ("OIG") otherwise authorized to exercise powers under subsection 6(e)(1)(C) of the IG Act, when loaned to another OIG whose Inspector General ("IG") is also otherwise authorized to exercise powers under subsection 6(e)(1)(C) of the IG Act, to seek and execute warrants issued under the authority of the United States for arrest, search of a premises, or seizure of evidence.

The Order authorizes such assistance only for "supporting a specified search or arrest operation," and for no other investigative activity, and states that the "duration of the assistance shall be agreed upon by both IGs and generally should not exceed five days."

The Order also states that "assistance provided by one IG to another … must comply with procedures to be established by the Council of Inspectors General on Integrity and Efficiency."

III. Procedures

Pursuant to the Attorney General's instruction in Order No. 3168-2010, the Council of Inspectors General on Integrity and Efficiency establishes the procedures contained herein. These procedures reflect the sole means by which an OIG may obtain from other OIGs the assistance authorized by the Attorney General's Order. These procedures are applicable only to assistance provided pursuant to this Attorney General's Order, and are not applicable to any other form of assistance provided by one OIG to another.

a. The Inspectors General, or their designees, must individually determine whether their OIGs will participate in the program of inter-OIG mutual assistance authorized by the Attorney General. The decision to participate in the program does not obligate an IG to commit personnel in response to any particular request, which is a decision that will be made on a case-by-case basis.

b. A participating OIG in need of additional manpower for the execution of a Federal search or arrest warrant (Requesting OIG) must submit a request in writing to the appropriate Inspector General, or his or her designee, of another

participating OIG (Assisting OIG). The written request must contain, at minimum, the following:

- case background sufficient to establish the Requesting OIG's jurisdiction;
- the type of operation (search or arrest);
- the operational plan (including the number of personnel needed and the duration of the assistance to be provided and a discussion of foreseeable risks); and
- a statement that the appropriate Federal prosecutor has been notified of the request.

c. The written request -- once approved and signed by the Inspectors General (or their designees) of both the Requesting and Assisting OIG -- will serve as the basis for an Inter-Agency Agreement governing the Requesting OIG's use of the Assisting OIG's personnel, but only for the purposes of the operation described therein.

d. Nothing in the Attorney General's Order or in these procedures obligates reciprocal assistance on the part of an OIG that has received assistance in the past. It remains within the discretion of an OIG to approve or to deny, in whole or in part, a request for assistance. Additionally, the Attorney General's Order and these procedures do not specifically prohibit other types of mutual assistance that is consistent with law and regulation.

e. Special Agents designated to participate in response to a request may be provided to the requesting agency on a reimbursable basis, unless otherwise prohibited by law.

14.0 SEARCH AND SEIZURE

14.1 FOURTH AMENDMENT AND EXCLUSIONARY RULE

The Fourth Amendment to the United States Constitution provides:

> **"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."**

By the terms of the Fourth Amendment, a search for, or seizure of, evidence must be reasonable. The test of reasonableness is met by the production of facts and circumstances amounting to probable cause to believe the evidence sought is located at the place or on the person to be searched.

Exclusionary Rule: Since a United States Supreme Court ruling in 1914, any evidence obtained by federal officers as the result of an unreasonable search is excluded in a federal court prosecution of the person whose rights had been violated. In 1961, the Supreme Court extended this holding to all state court prosecutions. Thus, any evidence obtained by law enforcement officers through an unreasonable search is not admissible in a criminal prosecution of the person whose rights were violated.

In numerous decisions the Supreme Court and other Federal courts have shown a strong preference for the validity of searches conducted pursuant to a search warrant.

14.2 SEARCH WARRANTS

A search warrant is issued by a federal magistrate judge or judge of a state court, upon request of an authorized federal law enforcement officer or an attorney for the government.

Under the authority derived from the Homeland Security Act of 2002, OIG SAs have the authority to request and execute search warrants. (Chapter 2.1)

14.3 EXECUTION OF THE WARRANT

A search warrant will be valid only for the time period (not to exceed 10 days) stated in the warrant. Unless otherwise stated in the warrant, it must be executed between 6:00 a.m. and 10:00 p.m. A search begun during this time frame may extend past 10:00 p.m.

18 U.S.C. § 3109 provides that an officer "may break open any outer or inner door or window of a house…. to execute a search warrant, if, after notice of his authority and

purpose, he is refused admittance. . .” Agents must wait a “reasonable” amount of time for the occupant to open the door unless there is some indication that the occupant is fleeing, destroying evidence, or taking some action that may jeopardize the safety of the agents. An agent is not required to announce when there is reasonable belief that the announcement will place the agent or other persons in imminent peril of bodily harm or that evidence is being destroyed.

Thoroughness is the primary consideration when a search is being conducted; however, agents will not unnecessarily damage or destroy property while conducting a search.

The “plain view” doctrine is an exception to the search warrant requirement developed by the courts. The doctrine holds that an officer who has a legal right to be where he is and observes items, which are immediately apparent to be of an incriminating nature, may seize such items without a warrant. Thus, a SA may seize items not named in a search warrant if operating within the confines of a valid search warrant and it is immediately apparent that the items are of an incriminating nature; e.g., illegal narcotics.

SAs conducting a search pursuant to a search warrant have the right to do so without forcible interference. If an SA can articulate a reasonable basis for suspecting that a person who is present may be armed, the SA may conduct a frisk of the individual for weapons.

When executing a search warrant, a copy of the warrant (not the warrant affidavit) must be given to the resident. If no one is present, a copy of the warrant must be left at the premises.

The search may commence upon the approval by the magistrate. A copy of the warrant is not necessary at the site prior to initiation of the warrant execution.

All property seized must be listed on the back of the warrant or on a separate document. If the items seized are listed on a separate document, this document should be referenced on the back of the warrant. At the conclusion of the search, copies of the list of items seized must be left with a copy of the warrant at the warrant site. The list of items seized must be witnessed by at least one person other than the SA preparing the inventory.

A prompt return of the executed warrant and a copy of the items seized must be made to the federal magistrate who authorized the warrant.

Tactical Plans must be completed using INV Form 39. (Chapter 13.9)

Sample Search Warrant affidavits and applications are included as exhibits. **(Exhibit 14-1)** Also included as reference is a “Checklist for a Search Warrant,” INV Form 37, **(Exhibit 14-2).**

Photographs or videotapes of the warrant site will be taken before and after the execution of a search warrant

14.4 WARRANTLESS SEARCHES

The courts strongly prefer that searches be conducted pursuant to a valid warrant. SAs should always err on the side of obtaining a warrant and when in doubt, seek advice from the USAO. However, the Supreme Court and other Federal courts have recognized certain exceptions to search warrant requirements. The following situations outline exceptions to the search warrant requirement:

Consent Search

A person who has authority, access, and control over a place or thing may give law enforcement officers permission to search the place or thing.

The consent must be completely voluntary and can extend only as far as the consenting party has such authority. Although a verbal consent is permissible, a signed consent to search is the best evidence of the voluntary nature of the consent. Whenever possible, INV Form 36(S) "Consent to Search," should be utilized prior to any search being conducted. For electronic media, INV Form 38, "Consent to Search Electronic Media" should be utilized. **(Exhibits 14-3, 14-4 and 14-5)**

Search Incident to Arrest

Contemporaneous with a lawful arrest, an SA may make a complete and thorough search of the arrested person and areas under their immediate control, including areas into which they might reach to obtain a weapon and/or destroy evidence. The scope of the search does not permit strip searches and body cavity searches.

The legality of the search depends upon the validity of the arrest and the limited nature of the search. For example, arresting a person in their home would not validate a complete search of other rooms of the house. A limited search of other areas is permissible, however, to detect anyone who might harm the officers or aid in an escape.

All items seized during a search incident to an arrest must be inventoried, and a copy of the inventory given to the arrestee.

Stop and Frisk

In *Terry v. Ohio*, 392 U.S. 1, 88 S.Ct. 1968 (1968), the Supreme Court recognized certain circumstances in which an officer could conduct a limited search for weapons. The Court held that if a law enforcement officer reasonably believes that a suspect they have stopped to question may be armed and dangerous, the officer may conduct a frisk of the suspect's outer clothing to discover weapons that might be used against the officer. SAs must be able to articulate the basis for their "reasonable suspicion of criminal behavior" for briefly stopping the suspect, and the frisk must be limited to a search for weapons.

Exigent Circumstances/Vehicular Searches

Federal court decisions have recognized that there are occasions when an officer must conduct an immediate search to prevent the loss or destruction of evidence.

The most obvious example of the justification for this type of warrantless search is the search of an automobile used in the commission of a crime. The mobility of the automobile is the basis for the exception, but if the car can be secured and rendered immobile, a search warrant should be obtained.

A 2009 Supreme Court decision (Arizona v Gant) limited the searches of vehicles incident to arrest. The Court held that the search of a vehicle incident to an arrest can only be conducted when the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search or when it is reasonable to believe that evidence relative to the crime of arrest might be found in the vehicle.

The exigent circumstance exception still requires that the searching officer must have probable cause to believe that a crime has been committed and that evidence of that crime is located in the place to be searched which is in danger of being destroyed

If a conveyance (vehicle, vessel or aircraft) is lawfully seized or impounded, an inventory of its contents will be completed as soon as practical. INV policy dictates that an inventory of the contents of the conveyance will be completed on INV Form 35, (Inventory of Seized Conveyance) **(Exhibit 14-6).** INV policy extends the inventory to any locked or unlocked containers located within the conveyance and any personal effects not returned to the owner. This inventory will be conducted to safeguard the owner's property and protect special agents against claims or disputes over lost or stolen property and protect law enforcement officers from potential dangers that may be located in the conveyance. Personal property should, when practical, be returned to the owner/operator. The vehicle will also be photographed.

Any items considered to be evidentiary will be inventoried separately on INV Form 30.

14.5 SEARCHES OF GOVERNMENT PROPERTY

As an employer, the government has the right to ensure that the property and office space it furnishes are being used for their intended purposes. The Supreme Court has held that a public employee can have, depending upon the specific circumstances, a reasonable expectation of privacy in their desk, office, and filing cabinet. The Court also recognized a greater right of inspection by a supervisor than by a law enforcement officer. *O'Connor v. Ortega*, 480 U.S. 709, 107 S.Ct. 1492 (1987).

The SAC will be consulted prior to any such searches. The USAO should be consulted if any questions arise regarding the search.

14.6 SEARCHES OF COMPUTERS

The searching and seizing of computers and electronic evidence by INV personnel will be governed by the policies and procedures as delineated in "*Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*," dated January 2001, from the DOJ, Criminal Division, Computer Crime and Intellectual Property Section (CCIPS), Washington, D.C. An electronic copy of this document is available from the CCIPS's website at http://www.cybercrime.gov./

SAs will coordinate questions and requests regarding searching and seizing computers and obtaining electronic evidence with their supervisor. Additionally, each USAO has a designated Computer/Telecommunications Coordinator that is available for consultation. (Chapter 13.7)

SAs can search for electronic evidence in one of three ways: by consent, subpoena, or search warrant. However, the most frequent method used to seize electronic media evidence from a computer is the issuance of a search warrant. It should be noted that there might be exigent circumstances, such as the destruction of evidence, which would allow for a warrantless search.

Once the role of the computer in the investigation is established, the type of computer and if possible, the electronic data it contains should be determined. For example:

Was/is the system a stand-alone home computer located in a residence?

Was/is the computer connected to a local-area network, an area wide network, the intranet, or the Internet?

What type of operating system does the computer utilize?

Was/is the computer utilized in a business?

Did/does the electronic data have legal protections under the Electronic Communications Privacy Act or the Privacy Protection Act?

Generally, in a search warrant affidavit, there are three topical subject areas that should be addressed:

The computer hardware consisting of the central processing unit (CPU), the monitor, the keyboard, and the mouse and any peripheral devices found on-site.

If the search warrant obtained is only for the computer software and or the electronic files stored in the computer, language should be included in the search warrant that allows for the seizure of the CPU if the files can not be

electronically replicated by the SCERS SA during the execution of the Search Warrant on-site.

The computer software operating system that controls the CPU and makes it possible for the user to install, run and store information on their own programs. This should include all user manuals for all of the programs installed on the computer.

The electronic data stored in the software inside the computer. The warrant should describe as much as possible the specific type of storage files or information being sought. Such files include spreadsheets, letters, memorandums, pictures, and programs.

In instances where a general "consent to search" has been obtained, SAs should obtain a separate and more detailed consent to search for computers or other electronic media and storage devices. SAs should have INV Form 38 (Consent to Search Electronic Media) executed by the consenting party. (**Exhibit 14-5**)

CHAPTER 14.0 - EXHIBITS

Exhibit 14-1, Sample Application and Affidavit for Search Warrant

AO 106 (Rev. 7/87) Application and Affidavit for Search Warrant

United States District Court

_____DISTRICT OF_____

In the Matter of the Search of:

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

CASE NUMBER:

(Name, address and brief description of the person, property or premises to be searched)

I, Special Agent [Name], being duly sworn, depose and say:

I am a Federal Special Agent assigned to the Department of the Treasury, Office of Inspector General, [Field Office location], and have reason to believe that on the "property or premises known as

[FULL ADDRESS]

in the _____Di_____, there is now concealed a certain person or property, namely

[Brief description of evidence to be subject of the search warrant,]

which are the fruits, instrumentalities and evidence of crimes concerning a violation of Title 18, United States Code, Section (s) __[274]__. The facts to support a finding of probable cause are as follows:

SEE ATTACHED AFFIDAVIT

Continued on the attached sheet and made a part hereof: _X_ Yes ___ No

_____
Signature of Complainant

Approved to Form_____,[Name], AUSA

Sworn to before me and subscribed in my presence,

_____ at _____
Date City and State

_____ _____
Name & Title of Judicial Officer Signature of Judicial Officer

Exhibit 14-2, INV Form 37, Checklist for Search Warrant

Office of Inspector General - Investigations
U.S. Department of Homeland Security

Homeland Security

CHECK LIST FOR SEARCH WARRANT

Date: _____
Case Number: _____
Offense: _____
Location to be Searched: _____
Special Agent: _____

An application for a search warrant is being made based on facts and circumstances established during investigation of the above captioned case.

This form serves as documentation of the attendant procedures used in making the original application and service by personnel of the entity making the application.

Section #1 - General

Yes	No	
☐	☐	1. The source is a law enforcement officer? List agency: _____
☐	☐	2. The source is a civilian or cooperating subject? (If yes, complete Section #3.)
☐	☐	3. The source is a confidential informant? (If yes, complete Section #4.)

Section 2 – Legal Description of Premises

☐	☐	1. Has the affiant or a designee personally observed the premises?
☐	☐	2. Has the following information been acquired?
☐	☐	a. Color of building.
☐	☐	b. Compass direction the front door faces.
☐	☐	c. Street sign number (if posted), type, color, and where affixed.
☐	☐	d. Any distinguishing characteristics (e.g. wrought iron bars, fence type, awnings, out buildings, garage vs. carport, and landscaping).
☐	☐	e. The side of the street where the building is located (north, south, east, or west).
☐	☐	f. How many structures from the nearest corner (e.g., third structure east of NW 3rd Avenue on NW 16th Street).
☐	☐	3. Does the description sufficiently distinguish the premises from all other places of the same type?
☐	☐	4. Has a photograph of the premises been taken? If not, explain: _____
☐	☐	5. Was the County, Parish, and or Property Records checked for verification?
☐	☐	6. Was the telephone directory checked?
☐	☐	7. Was a utilities check conducted?
☐	☐	8. If vehicles are parked at the premises, have registration checks been performed?

INV FORM-37

CHECK LIST FOR SEARCH WARRANT

10. Is the scene to be searched currently occupied?
    If yes, has surveillance been established?
11. Is the building a duplex or apartment building? If yes,
    a. Have the mailboxes been checked?
    b. Has the building name directory been checked?
    c. Has the landlord/manager been contacted?
    d. Has the specific doorway of the structure been identified (e.g., 3rd door east of the elevator)?

[redacted]

(b) (7)(D)

[redacted]

INV FORM-37

CHECK LIST FOR SEARCH WARRANT

(b) (7)(D) [redacted]

Section #5 – Computer/Electronic Review

1. Are computers anticipated at the search site?
2. Have you obtained intelligence about the computer environment? If yes, provide details: _____
3. Has the OIG Electronic Crimes Team been contacted for assistance?
4. Will a computer forensic special agent be required as part of the search team?
5. Is one available by telephone?
6. Has electronic information been included in the warrant affidavit and the search warrant?
7. Has the designated "Computer Crimes" Assistant U.S. Attorney been contacted?

Section #6 – Final Review

1. Has an Assistant U.S. Attorney been notified?
   If yes, name: _____
2. Is the Affidavit for Search Warrant consistent with the investigation?
3. Does the description of the premises coincide on the affidavit and the search warrant?
4. Is/are the statute number(s) correct?
5. Are all pages numbered and initialed or signed by a judge of competent jurisdiction?
6. Have the described premises identified in the warrant been reviewed with the service team?
7. Has a drive-by been conducted with the service team to verify the correct location for the search?
8. Has the service team been briefed as to any known hazards (e.g., weapons, security enhancements, explosives, etc.)?

Notes

_____

INV FORM 37

Exhibit 14-3, INV Form 36, Consent to Search

Office of Inspector General - Investigations
U.S. Department of Homeland Security

Homeland Security

CONSENT TO SEARCH

Date: _____ Location: _____

I, _____, hereby authorize Special Agents of the Department Homeland Security Office of the Inspector General to conduct a complete search of :

_____ at _____ .

_____ .

I have been informed of my right not to have a search made without a search warrant, and the right to refuse to consent to such a search.

I understand that any contraband or evidence discovered in this search may be used against me in a court of law.

This consent is being given by me to the above person(s) voluntarily and without threats, duress, or promises of any kind. I understand that I may ask for and receive a receipt for all things taken.

Signature of Witness(es): **Signature of Consenter:**

Witness	Date	Consenter's Signature	Date
Witness	Date	Printed Name of Consenter	

INV FORM-36

Exhibit 14-4, INV Form 36S, Consent to Search (Spanish)

Oficina del Inspector General - Investigaciones
Departamento de Seguridad De la Patria

Homeland Security

CONSENTIMIENTO A BUSQUEDA

Fecha _____ Lugar: _____

_____, por este medio, autorizo a _____ Agentes Especiales del Departamento de la Seguridad de la Patria, Oficina del Inspector General que conduzcan una búsqueda completa de: _____ en_____

Me han informado de mi derecho a no permitir la búsqueda sin una orden de búsqueda, y me han informado de mi derecho ha rechazar tal búsqueda.

Entiendo que cualquier descubrimiento de contrabando o evidencia durante esta búsqueda podrá ser usados en mi contra en una corte de ley.

Este consentimiento es otorgado voluntariamente a los Agentes ya mencionado, sin amenazas, coacción o promesas de cualquier tipo. Entiendo que puedo pedir un recibo por todas las cosas tomadas.

Firma de Testigo(s): **Firma:**

Testigo	Fecha	Firma	Fecha
Testigo	Fecha	Nombre	

INV FORM-36S

Exhibit 14-5, INV Form 38, Consent to Search Electronic Media

Office of Inspector General - Investigations
U.S. Department of Homeland Security

Homeland Security

CONSENT TO SEARCH ELECTRONIC MEDIA

I, _____, hereby authorize _____, who has identified himself / herself as a law enforcement officer, and any other person(s), including but not limited to, a computer forensics examiner, he / she may designate to assist him / her to remove, take possession of and / or conduct a complete search of the following: computer systems, electronic data storage devices, computer data storage diskettes, CD-ROMs, or any other electronic equipment capable of storing, retrieving, processing and / or accessing data.

The aforementioned equipment will be subject to data duplication / imaging and a forensic analysis for any data pertinent to the incident / criminal investigation.

I give this consent to search freely and voluntarily without fear, threat, coercion, or promises of any kind and with full knowledge of my constitutional right to refuse to give my consent for the removal and / or search of the aforementioned equipment / data, which I hereby waive. I am also aware that if I wish to exercise this right of refusal at any time during the seizure and / or search of the equipment / data, it will be respected.

This consent to search is given by me this _____ day of _____, 20_____

at _____AM / PM.

Consenter Signature: _____

Consenter Printed Name: _____

Location items taken from:_____

Witness Signature: _____

Witness Title: _____

Witness Signature: _____

Witness Title: _____

INV Form 38

Exhibit 14-6, INV Form 35, Inventory of Seized Conveyance

Office of Inspector General-Investigations
U.S. Department of Homeland Security

Homeland Security

INVENTORY OF SEIZED CONVEYANCE			OFFICE		CASE NO.	
TYPE OF CONVEYANCE ☐ CAR ☐ TRUCK ☐ VESSEL ☐ AIRCRAFT			YEAR	MAKE	MODEL	STYLE
ENGINE OR IDENTIFICATION No.	BODY OR HULL SERIAL NO.	NO OF CYL.	BODY OR HULL COLOR	SEATING CAPACITY	NO. OF WHEELS	
TRANSMISSION TYPE ☐ STD ☐ AUTO ☐ O.D.	ODOMETER READING	TRUCK LOAD CAP TONS	LICENSE (STATE/YEAR/NO.)		ENGINE TYPE:	

EQUIPMENT AND ACCESSORIES	Y/N	EQUIPMENT AND ACCESSORIES	Y/N	EQUIPMENT AND ACCESSORIES	Y/N
HEADLIGHTS		POWER STEERING		CLOCK	
PARKING LIGHTS		POWER BRAKES		LIGHTER	
TAIL LIGHTS		POWER WINDOWS		SEATH CUSHIONS	
BACK UP LIGHTS		POWER SEAT ADJUST		SEAT COVERS	
SPOT LIGHTS		POWER WINCH		SUN VISORS	
FOG LIGHTS		HORN(S)		FLOOR MATS	
TURN SIGNALS		WINDSHIELD WIPERS		JACK	
REARVIEW MIRROR		WINDSHIELD WASHER		TIRE CHAINS	
SIDEVIEW MIRROR(s)		TINTED WINDSHIELD		KEPS	
AIR CONDITIONER		HEATER		VIANAL COVERED ROOF	
BATTERY: ☐ 0 V. ☐ 12 v.		CARBURETOR: ☐ SINGLE ☐ DUAL		RADIO: ☐ SAT ☐ AM/FM☐	
TIRES (SPARE)					

REMARKS (INCLUDING OTHER ARTICLES NOT SHOWN ABOVE:			
GENERAL CONDITION			
CONVEYANCE WAS SEIZED FROM: (NAME AND ADDRESS)		FOR VIOLATION OF: (TITLE & SECTION) **USC**	
PLACE WHERE SEIZED		DATE SEIZED:	
SEIZING AGENT(S)		AGENTS RECOMMENDATION: SUITABLE FOR OFFICIAL USE: ☐ YES ☐ NO	
CONVEYANCE IS REGISTERED TO: (NAME AND ADDRESS)			
ESTIMATED VALUE	AMOUNT OF LIEN	NAME AND ADDRESS OF LIENOR	
RECEIPT OF THE ABOVE DESCRIBED PROPERTY IS ACKNOWLEDGED BY: (NAME AND ADDRESS OF FIRM OR CONTRACT CUSTODIAN)		DATE RECEIVED	STORAGE RATE
		RECEIPT SIGNATURE OF REPRESENTATIVE	
		TITLE OR POSITION OF REPRESENTATIVE	
NOTICE TO STORAGE CONTRACTOR: BILL STORAGE CHARGES TO DHS OIG			
FIELD RECOMMENDATION: SUTABLE FOR OFFICIAL USE: ☐ YES ☐ NO		SEIZING AGENT (SIGNATURE)	DATE
APPROVING OFFICIAL (SIGNATURE):			DATE

15.0 ELECTRONIC INTERCEPTS, ELECTRONIC SURVEILLANCE, AND ONLINE INVESTIGATIVE ACTIVITY

15.1 ELECTRONIC INTERCEPTS, ELECTRONIC SURVEILLANCE, AND ONLINE INVESTIGATIVE ACTIVITY: GENERAL PROVISIONS

A. *Content of the Chapter*: This chapter contains the policies and procedures applicable to the use of electronic intercepts and surveillance techniques as well as the collection of digital evidence by the Department of Homeland Security, Office of Inspector General (DHS OIG), Office of Investigations (INV) personnel. This chapter sets forth the specific mechanisms, including applicable approval requirements, for the use of wiretaps, "bugs" (oral interception devices), roving taps, video surveillance, aircraft transponders, telephone decoders, consensual monitoring of wire or oral communications, and the collection of digital evidence, among other things.

B. *General Policy*: DHS OIG will conduct all electronic surveillance operations consistent with federal law and applicable policies. Electronic surveillance is intrusive in nature and may implicate the Fourth Amendment. As such, violations of the statutes prohibiting electronic surveillance of communications can lead to both criminal and civil sanctions. Accordingly, the use of most electronic surveillance devices is restricted and closely guided and may include the requirement for approval by a high-level U.S. Department of Justice (DOJ) official prior to a federal prosecutor obtaining a court order authorizing interception. DHS OIG Special Agents (SAs) should clearly understand when DOJ review and approval are required, and what such a process entails. Caution should be exercised and doubt resolved in favor of the privacy of the conversation and the individual. Questions and advice concerning the legality of DHS OIG investigative electronic surveillance techniques should be addressed to the Assistant Inspector General for Investigations (AIGI) for resolution in conjunction with the DHS OIG Counsel. Issues in ongoing investigations concerning the operational use of techniques, court decisions, and this chapter should be discussed beforehand with the Assistant United States Attorney (AUSA) or prosecutor handling the underlying investigation. Requests for permission to use electronic monitoring and surveillance are limited to investigations involving alleged violations within DHS OIG's jurisdiction.

C. *Scope*: The provisions of this chapter apply to all employees in the DHS OIG engaged in investigative activity covered by this chapter, including the interception of communications without the consent of all parties, access to stored wire and electronic communications and transactional records, and the use of pen registers and trap and trace devices.

D. *Reference*: This chapter is issued under the *Inspector General Act of 1978*, title 5 appendix of the United States Code (5 U.S.C. app) as amended; the *Electronic Communications Privacy Act of 1986* (Pub. L. No. 99-508), 18 U.S.C. chapters 119, 121, and 206; "Procedures for Lawful, Warrantless Monitoring of Verbal Communications"

issued by the Attorney General on May 30, 2002; and the Inspector General Delegation of Authority Concerning Interception or Recording of Conversations With the Consent of One Party, dated April 19, 1991.

E. *Overview of the Electronic Communications Privacy Act of 1986*: The *Electronic Communications Privacy Act of 1986* is divided into three separate but closely related titles: Title I, "Interception of Communications and Related Matters"; Title II, "Access to Stored Wire and Electronic Communications and Transactional Records Access"; and Title III, "Pen Registers and Trap and Trace Devices."

F. *Interception of Communications and Related Matters*:

1. *The Electronic Communications Privacy Act of 1986*: The Electronic Communications Privacy Act of 1986 defines and regulates three types of communications: (1) wire, (2) oral, and (3) electronic. Electronic communications are those types of non-oral or wire communications that occur over computers, digital display pagers, and facsimile machines. Only crimes enumerated in the statute may be investigated through the interception of wire or electronic communications. The enumerated crimes that are most likely to be the subject of DHS OIG investigation include but are not limited to:

   a. 18 U.S.C. § 201 (bribery of public officials and witnesses);

   b. 18 U.S.C. § 1510 (obstruction of criminal investigations);

   c. 18 U.S.C. § 1341 (mail fraud);

   d. 18 U.S.C. § 1029 (fraud and related activity in connection with access devices); and

   e. 18 U.S.C. § 1343 (fraud by wire, radio, or television).

2. *Title III Statute References*: Law enforcement agents typically refer to wiretaps or other nonconsensual interceptions of communications as "title IIIs," after the section of the 1968 legislation that first regulated their use. (For this reason, this chapter uses "Title III" to refer to such interceptions.)

G. *Stored Wire and Electronic Communications and Transactional Records Access*:

1. Title II of the 1986 act is designed to protect the privacy of stored electronic communications (for example electronic mail messages).

2. Electronic communications are divided into two categories:

   a. Communications during the transmission stage.

b. Communications in "storage" incident to transmission.

3. Electronic storage is defined in 18 U.S.C. § 2510(17) as both any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission and as the storage of a communication by an electronic communication service for purposes of backup protection.

4. For purposes of the Fourth Amendment, stored communications are akin to regular mail handled by the U.S. Postal Service. A search warrant is required to intercept mail, and electronic mail in storage incident to transmission is accorded the same protection. However, once the communication is no longer in temporary storage incidental to transmission, it may be obtained by an administrator with proper notice to the customer.

5. A warrant is required to obtain the contents of a wire or electronic communication that has been stored for 180 days or less.

H. *Pen Register and Trap and Trace Devices*: The applicable statutes generally prohibit the use of a pen register or trap and trace device without a court order.

15.2 RESPONSIBILITIES

A. *Assistant Inspector General for Investigations*: The AIGI is responsible for ensuring that the provisions of this chapter are met by all personnel assigned to the INV.

B. *Deputy Assistant Inspector General for Investigations*: A Deputy Assistant Inspector General for Investigations (DAIGI), either the DAIGI Field Operations Division (FOD) or DAIGI Headquarters Operations Division (HOD), receives requests and determines DHS OIG approval on requests to conduct electronic surveillance operations under this chapter, consistent with delegation from the Inspector General and the provisions of this chapter. The DAIGI reviews and submits all requests for electronic surveillance that require DOJ approval.

C. *Special Agent in Charge, Digital Forensics and Analysis Unit, INV Headquarters*: The Special Agent in Charge (SAC), Digital Forensics and Analysis Unit (DFAU), INV Headquarters, working under the general direction of the DAIGI FOD and direct supervision of the DAIGI HOD, is responsible for maintaining consultation with DHS OIG Counsel and liaison with the DOJ Criminal Division, Office of Enforcement Operations (OEO), on issues involving electronic surveillance operations. The SAC DFAU receives and reviews all requests to conduct electronic surveillance operations under this chapter, consistent with the delegation from the Inspector General and the provisions of this chapter. The SAC DFAU refers requests to the DAIGI FOD or DAIGI HOD for approval. The SAC DFAU also stores, maintains and distributes technical equipment under the direction of the DAIGI HOD.

D. *Special Agents in Charge*: SACs receive, review, and grant DHS OIG approval on requests to conduct consensual telephone intercepts and, with consultation and concurrence with a Federal Prosecuting Office, consensual non-telephone intercepts under the guidelines in this chapter. On all other requests, SACs are responsible for reviewing and submitting to the SAC DFAU, INV Headquarters, requests for approval of electronic surveillance operations.

E. *Assistant Special Agent in Charge/Resident Agent in Charge*: Where extraordinary circumstances exist, Assistant Special Agents in Charge (ASACs) or Resident Agents in Charge (RACs) may also receive, review, and grant DHS OIG approval for requests to conduct consensual telephone intercepts under the guidelines in this chapter. (See Section 15.8 B.) ASACs/RACs are responsible for ensuring that SAs under their supervision follow the provisions of this chapter when conducting any electronic surveillance activity.

F. *Electronic Intercept and Surveillance Program Manager*: Working under the direction and supervision of the SAC DFAU, the Electronic Intercept and Surveillance Program Manager (EISPM) receives and reviews requests to conduct electronic surveillance operations under this chapter; assists field offices in the conduct of intercepts and electronic surveillance; coordinates with equivalent managers at partnering federal agencies; ensures that technical equipment is maintained and distributed efficiently; and maintains all central records associated with the use and maintenance of electronic intercept and surveillance equipment.

G. *Technical Equipment Coordinator*: The Technical Equipment Coordinator (TEC), is a Special Agent (SA), appointed by the field office SAC, who is appropriately certified and responsible for the proper use, maintenance and oversight of the technical equipment in possession of the local field office.

H. *Special Agents*: Special Agents (SAs) are responsible for preparing requests to use electronic surveillance techniques and will not employ monitoring activities until appropriate approvals have been obtained.

15.3 DEFINITIONS

A. *Aural Transfer*: A transfer containing the human voice at any point between and including the point of origin and the point of reception (18 U.S.C. 2510(18)).

B. *Consensual Interception or Monitoring*: Interception or monitoring of a wire or oral communication is "consensual" when one or more parties to the communication is aware of and gives prior verbal or written consent for the interception or monitoring. The consenting party may be an agent, an informant, or any other individual.

C. *Contents*: When used with respect to any wire, oral, or electronic communication, "contents" includes any information concerning the substance, purport, or meaning of that communication. (18 U.S.C. § 2510(8)).

D. *Electronic Communications*: Any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic or photo-optical system that affects interstate or foreign commerce. (18 U.S.C. § 2510(12)). Such communications may include text messages, electronic mail ("email"), facsimiles ("faxes"), and other such non-voice wireless communication. "Electronic communications" do not include:

1. any wire or oral communication (see definitions above);

2. any communication made through a tone-only paging device;

3. any communication from a tracking device; or

4. electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.

E. *Electronic Communication Service*: Any service which provides to users thereof the ability to send or receive wire or electronic communications. Cf. 18 U.S.C. § 2510(15).

F. *Electronic Communications System*: Any wire, radio, electromagnetic, photo-optical, or photo-electronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications. Cf. 18 U.S.C. § 2510(14).

G. *Electronic, Mechanical, or other Device:* Any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than — (a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties; (b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal. (18 U.S.C. § 2510(5)).

H. *Electronic Storage*: Any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
any storage of such communication by an electronic communication service for purposes of backup protection of such communication, 18 U.S.C. § 2510(17).

I. *Intercept*: The aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device. (18 U.S.C. § 2510(4)).

J. *Investigative or Law Enforcement Officer*: Any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in 18 U.S.C., chapter 119, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses, (18 U.S.C. § 2510(7)). This includes DHS OIG SAs.

K. *Mobile Tracking Device*: An electronic or mechanical device which permits the tracking of the movement of a person or object (18 U.S.C. § 3117(b)).

L. *Nonconsensual Conversation*: Monitored conversation where none of the participants is aware of or has consented to the monitoring."

M. *Oral Communication*: Any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication. (18 U.S.C. § 2510(2)).

N. *Pen Register*: A device, requiring a court order, which records or decodes electronic or other impulses, which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached.

O. *Person*: Any employee, or agent of the United States or any State or political subdivision thereof (including confidential informants), and any individual, partnership, association, joint stock company, trust, or corporation. (18 U.S.C. § 2510(6)).

P. *Readily Accessible to the General Public*: With respect to a radio communication, that such communication is not:

1. scrambled or encrypted;

2. transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;

3. carried on a subcarrier or other signal subsidiary to a radio transmission;

4. transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or

5. transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio. (18 U.S.C. § 2510(16)).

Q. *Reasonable Expectation of Privacy*: A legal term that is not susceptible to a definition in absolute terms. It is a constitutional concept founded in the Fourth Amendment principles of search and seizure and must be measured on a case-by-case basis. In the context of electronic surveillance of conversations, a reasonable expectation of privacy exists when all parties to the conversation have taken reasonable steps to ensure that their conversations are not intercepted or monitored through the use of any electronic, mechanical, or other device. (By statute, this concept is only relevant to the interception of oral communications.) If a conversation can be overheard by a nonparty through the utilization of his normal hearing capacity, there is generally no reasonable expectation of privacy. SAs should consult the prosecutor with case-specific questions regarding reasonable expectation of privacy.

R. *Trap and Trace Device*: A technique or procedure, requiring a court order, to determine the origin, by telephone number and location, of a telephone call made to a known telephone instrument. The terms 'lock-out' and 'trapping' are also used to describe this technique.

S. *User*: any person or entity who uses an electronic communication service and is duly authorized by the provider of such service to engage in such use. (18 U.S.C. § 2510(13)).

T. *Wire Communication*: Any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable or other like connection between the point of origin and the point of reception, (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce. (18 U.S.C. § 2510(1)).

15.4 STORAGE AND USE OF TECHNICAL EQUIPMENT

A. *Storage and Maintenance of Technical Equipment*: Technical equipment used under the policies of this chapter will be maintained either in the assigned field office or with the EISPM, under the supervision of the SAC DFAU, at INV Headquarters. Where the equipment is stored and maintained in the field office, generally the TEC will be responsible to ensure that the field office maintains a log of all electronic surveillance equipment issued and covered in this chapter, setting forth the date and time issued, the date and time returned, and the name of the agent receiving the equipment. Where the equipment is stored and maintained at Headquarters, the EISPM will be responsible for distributing the equipment to the field upon request, and ensuring that the equipment is properly logged, including the date and time issued, the date and time returned, and the name of the agent receiving the equipment.

B. *Specific Procedures*: When an interception device or other technical equipment is withdrawn from main storage at headquarters or in field storage, the EISPM or TEC, depending on the permanent storage location, shall record in EDS the time and date, case number and the requesting user's name for each specific piece of equipment. The

requesting user will be fully accountable for the equipment until it is returned. When the equipment is returned, the EISPM or TEC must record the time and date of return and note any damaged or missing items. Logs will be maintained for 10 years. The SAC DFAU will ensure that an audit is conducted at the end of each fiscal year of the logs and physical inventories for all equipment.

C. *Technical Equipment Coordinators*: Each SAC or Acting SAC shall appoint an SA as the TEC, who will be currently certified through either the Federal Law Enforcement Training Center (FLETC) or a nationally recognized organization as approved by the SAC DFAU. The SAC or ASAC will act as the central point of coordination to process requests for DAIGI approval for those types of electronic surveillance that require it, as specified in this chapter.

D. *Movement of Technical Equipment*: Where a need arises to use electronic surveillance in an area outside the originating office's jurisdiction, the originating office will obtain the necessary approvals and ensure that the appropriate equipment is available to the other office.

E. *Limitations of Use*: Any use of electronic surveillance equipment outside the confines of an official investigation is expressly prohibited. Limited use of equipment for training or evaluation purposes may be performed only when explicitly approved by the SAC DFAU.

15.5 TELEPHONE COMMUNICATIONS GENERALLY

A. *General Distinctions Relating to Telephone/Wire Communications*: Case law and DOJ policy regarding telephone or wire communications are sufficiently distinct to warrant separate treatment in this chapter. Four telephone-related areas are covered here: (1) obtaining subscriber/toll information, (2) use of telephone decoder (pen registers), (3) consensual monitoring of telephonic or wire communications, and (4) nonconsensual monitoring of telephonic or wire communications.

B. *Text Messages*: Text messages are considered a form of "electronic communication" as described in 18 U.S.C. 2510.

15.6 OBTAINING SUBSCRIBER/TOLL INFORMATION

A. *General Provision*: Under an administrative, Inspector General (IG), or grand jury subpoena, DHS OIG may access transactional records or other non-content-related information pertaining to a subscriber or customer of a telephone company.

B. *What can be Obtained*: Subscriber/toll information commonly available includes (for a specified telephone number):

1. Name and address of the subscriber, number of telephones at that address, and the date of installation.

2. General information, such as marital status, name of spouse, employment, and history of previous service.

3. Charges to that number for a specified period of time: toll, collect, credit card calls, and telegram charges.

C. *Basis for Request*: Requests for subscriber/toll information must be based on reasonable suspicion that the information sought will be pertinent to an investigation. Requests for subscriber/toll information without such indication are prohibited.

D. *Notification to Customers*: DHS OIG is not required to notify the subscriber/customer that his or her records have been subpoenaed. Telephone companies often will notify customers that toll records have been subpoenaed, but there is no requirement under federal law that they do so. A DHS OIG subpoena can request a company to delay notification but cannot require it. Generally, telephone companies honor requests by DHS OIG to delay customer notification for a 90-day period, however, some telephone companies have suggested they will honor only a court order directing a delay in notification (under 18 U.S.C. § 2705). Accordingly, the only assurance DHS OIG has against premature notification is a court order and SAs should be cognizant of how the subpoena will affect their investigation.

E. *Requesting a Delay of Notification*: To request that the telephone company delay customer notification, DHS OIG must certify that notification could impede an investigation. DHS OIG certification requesting nondisclosure should be considered in all active investigations if there is a basis to believe that disclosure would impede the investigation or prosecution.

1. *Certification*: Certifications requesting nondisclosure for an initial 90-day period will be by letter from the SAC. This letter will accompany the subpoena upon service and will contain the following language:

> "Pursuant to an official criminal investigation being conducted by the U.S. Department of Homeland Security, Office of the Inspector General, of a suspected felony, we request that your company furnish on (date) toll record information pertaining to (name) for the period (month, day, year) through (month, day, year) inclusive, and that you not disclose the existence of such request for a period of 90 days from the date of its receipt. Any such disclosure could impede the investigation being conducted and thereby interfere with enforcement of the law."

2. *Extensions*: Telephone companies have honored requests for additional 90-day periods when required. Recertification request letters will use the following language:

> "Pursuant to an official criminal investigation being conducted by the U.S. Department of Homeland Security, Office of the Inspector General, of a suspected

felony, we received on (date) toll record information pertaining to (name) for the period (month, day, year) through (month, day, year) inclusive and at that time requested that you not disclose the existence of such request for a period of 90 days. Because this investigation continues, we request that you not disclose the existence of this request for another 90 days from the date of this request. Any such disclosure could impede the investigation being conducted and thereby interfere with enforcement of the law."

F. *Procedures for Issuing a Subpoena*: A request for DHS OIG subpoena should be initiated in accordance with procedures found in Chapter 18. The requesting SA should explain the necessity or purpose of the request and include the caller's name and telephone number.

G. *Payment to Telephone Companies*: Telephone companies are not required to be paid when complying with DHS OIG subpoenas for toll records or subscriber information (18 U.S.C. 2706(c)). However, if a court determines that the information required is unduly burdensome to the company or unusually voluminous, reimbursement for reasonably necessary costs may be awarded as determined by DHS OIG Office of Counsel.

15.7 [redacted]

A. [redacted]

B. [redacted]

C. [redacted]

[redacted]

D. [redacted]

E. *Basis to Request Court Order for Decoders and Trap and Trace Devices*: Court orders are required by statute for use of telephone decoders and trap and trace devices under 18 U.S.C. § 3121 et seq. Probable cause is not necessary for obtaining a decoder or trap and trace order, only a reasonable belief that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by the agency.

F. *Form of Application*: A short affidavit in support of the application may inform the judge of the facts of the investigation although an affidavit is not required. Any AUSA may make an application for installation and use of a telephone decoder or trap and trace device. The application must identify the AUSA and the law enforcement agency conducting the investigation. The application must include a certification that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by the agency.

G. *The Court Order*: Judges and magistrate judges have the statutory authority to issue the court order, including the court order requiring technical assistance from the telephone company. In addition to the information required in the application, the court order must specify [redacted] The above information will be included in the application.

H. *Duration*: The duration of the court order must not exceed 60 days. The order should include a nondisclosure provision (18 U.S.C. § 3123(d)) for the owner or lessor of the line or facility to which the device will be attached. Should additional time be necessary, an extension may be applied for in no more than 60-day increments. The application for an extension need only meet the requirements for an original application as listed in paragraph E above.

I. *Emergency Conditions*: Under certain circumstances where an emergency situation exists involving immediate danger of death or serious bodily injury to a person or

conspiratorial activities characteristic of organized crime, a law enforcement officer or principal prosecuting attorney may direct an emergency installation of a pen register or trap and trace device under 18 U.S.C. § 3125. DHS OIG SAs should consult with a duty AUSA if it is reasonably determined that such circumstances exist.

J. *Special Requirements for Internet Communications*:

1. [redacted]

2. [redacted]

K. *Specific Procedures and Record Requirements*:

1. *Memorandum to Headquarters*: Upon obtaining the court order for the initial installation and for extension, the SAC will submit a memorandum to their DAIGI with a copy to the SAC DFAU. The memorandum, which can be submitted by email, should include the following information:

   a. SUBJECT: Installation of Telephone Decoder or Trap and Trace Device.

   b. The memorandum should contain the following information:

      i. case title and case number;

ii. telephone number and listing;

iii. dates of court order and installation; and

iv. number of days authorized.

2. [redacted]

3. [redacted]

4. [redacted]

15.8 CONSENSUAL INTERCEPTS OF TELEPHONE COMMUNICATIONS WHERE NO SENSITIVE CIRCUMSTANCES ARE PRESENT

A. *General Use and Considerations*: Consensual telephone intercepts are commonly used as a means of documenting a conversation between a suspect and the undercover agent or informant. Under federal law, consensual monitoring requires the consent of at least one of the parties participating in the conversation. Some states impose greater requirements upon investigators and private citizens than those required by federal law. For example, some states may require two – or all – parties to a communication to consent to a recording or monitoring. In general, these state laws do not supersede federal law and do not impact federal investigators operating under federal law.

B. *Approval Procedure*: Consensual telephone intercepts require the prior approval of the SAC. Where extraordinary circumstances preclude prior approval, the intercept may be conducted but must be subsequently reported to the ASAC/SAC at the earliest practical time. In this context, extraordinary circumstances are those in which the failure to conduct the intercept could potentially threaten the loss of life, property, or key investigative evidence. SAs will document their prior approval of the intercept on the authorization section of the INV Form 71, Authorization and Report of Consensual Intercept **(Exhibit 15-1)**. After SAC approval is obtained and the intercept conducted, SAs will complete the report section of the INV Form 71 and submit it to their SACs as soon as practicable and without delay (in no event later than 5 days) after the interception. The original INV Form 71 will be filed in the case file.

C. *Documentation of Consent*: To exempt the interception from the general warrant requirement, 18 U.S.C. § 2511(2) (c) requires prior consent from one of the parties to the conversation. To document conformance to the requirements of the statute, DHS OIG SAs will obtain a signed INV Form 72/72S, Consent to Intercept, Monitor and Record Communications **(Exhibit 15-2 and 15-2S Spanish Version)** from the consenting party prior to conducting the intercept. The original INV Form 72 will be placed in the investigative case file and in the CI File when the consenting party is a CI.

D. *No Exception to Use of INV Form 72*: No exception should be made to executing and properly witnessing the consent form in the situation when an informant, a SA, or any other law enforcement officer or person is the consenting party. The INV Form 72/72S, Consent to Intercept, Monitor and Record Communications constitutes an accurate, reliable official record that may be used in a court in the event the issue of consent is raised or if the administrative procedure needs to be documented to assure the court that DHS OIG complied with 18 U.S.C. 2511(2)(c).

E. *Recording Required*: Unless it is totally impractical, consensual intercepts will be recorded. Where recording is not possible, an agent should monitor the conversation from an extension telephone, speaker phone, or some equivalent arrangement. If a recording is not possible, SAs are required to take contemporaneous notes of the intercepted conversation, unless this is not feasible. If SAs are unable to take contemporaneous notes, these circumstances should be appropriately documented in the investigative casefile. The original recording used in the interception should be dated, initialed by the seizing agent, and placed into evidence. Working copies of the original recording will be used for transcription and investigative purposes.

F. *Documentation of the Conversation*: For recorded intercepts, it is generally sufficient to report the substance of a consensual intercept in a Memorandum of Activity (MOA), without having to transcribe the conversation. However, where the conversation is of particular significance to the investigation, it should be transcribed. When not transcribed, the case agent must listen to the recordings in their entirety to ensure recording quality and to verify the undercover agent's version of events. The recordings will be handled as evidence in accordance with Special Agent Handbook (SAH) provisions.

G. T*ext Messages*: Text messages are considered a form of "electronic communication" as described in 18 U.S.C. 2510 and as such, can be consensually intercepted and monitored. SAs should seek guidance from their local United States Attorney's Office (USAO) when considering consensual interception of text messages.

H. *Approval of Prosecutor not Required*: Other than when one of the specified sensitive circumstances outlined in Section 15.10, below, is present, consensual telephone monitoring does not require prior review and advice from a Federal Prosecutor's Office (e.g., AUSA or Criminal Division Trial Attorney).

15.9 PROCEDURES FOR CONSENSUAL INTERCEPTION/MONITORING OF ORAL (NON-TELEPHONIC) COMMUNICATION WHERE NO SENSITIVE CIRCUMSTANCES ARE PRESENT

A. *General Provisions*: The consensual intercept or monitoring of non-telephone verbal communications is governed by the Attorney General Memorandum, Procedures to Lawful, Warrantless Monitoring of Verbal Communications (May 2002) (**Exhibit 15-3**). The following procedures cover the investigative use of devices which intercept and record certain consensual verbal conversations where a body transmitter or recorder or a fixed location transmitter or recorder is used during a conversation that does not take place over the telephone or by other wire transmissions (i.e., generally a face-to-face-meeting). The interception of a conversation in the absence of a consenting party is a nonconsensual intercept. Advice from a Federal Prosecuting Office must be obtained before approval, but no written authorization is required unless one of the specified sensitive circumstances outlined in Section 15.10, below, is present. If one of these sensitive circumstances is present, DHS OIG must obtain advance written authorization from DOJ.

B. *Advice from a Federal Prosecution Office Required*: In most circumstances, the interception/monitoring of oral communications with the consent of one of the parties to the communication can be approved by a SAC. Prior to granting approval for consensual monitoring, however, SAs must obtain advice from the United States Attorney, an AUSA, or DOJ attorney responsible for a particular investigation that the consensual monitoring is both legal and appropriate. The advice may be obtained orally from the attorney, but should be documented in an MOA and included in the case file. If the attorneys described above cannot provide this advice for reasons unrelated to the legality or propriety of the consensual monitoring, the advice must be sought and obtained from an attorney of the Criminal Division of the DOJ designated by the Assistant Attorney General in charge of that Division. Before providing such advice, the designated Criminal Division Attorney will notify the appropriate United States Attorney or other attorney who would otherwise be authorized to provide the required advice under this paragraph.

C. *Special Limitations*: [redacted]

2. [redacted]

b. [redacted]

D. *Specific Procedures*:

1. *Documentation of Consent*: The consent will be documented on INV Form 72/72S, Consent to Intercept, Monitor and Record Communications **(Exhibit 15-2 and 15-2S Spanish Version).** The original INV Form 72 will be placed in the investigative case file and in the CI File if the consenting party is a CI.

2. *No Exception to Use of INV Form 72*: No exception should be made to executing and properly witnessing the consent form in the situation when an informant, a SA, or any other law enforcement officer or person is the consenting party. The INV Form 72/72S, "Consent to Intercept, Monitor and Record Communications" constitutes an accurate, reliable official record that may be used in a court in the event the issue of consent is raised or if the administrative procedure needs to be documented to assure the court that DHS OIG complied with 18 U.S.C. 2511(2)(c).

3. *Recording Required*: Unless it is not possible, consensual intercepts will be recorded. Where recording is not possible, an agent should monitor the conversation from an extension telephone, speaker phone, or some equivalent arrangement. The original recording used in the interception should be dated, initialed by the seizing agent, and placed into evidence. Working copies of the original recording will be used for transcription and investigative purposes.

4. *Documentation of Intercept*: SAC approval and the advice from the prosecuting authority will be documented on INV Form 71, Authorization and Report of Consensual Intercept **(Exhibit 15-1)**. Before each intercept, SAs will seek the necessary advice from the federal prosecution office, as detailed above, and request approval through the ASAC to the SAC through the use of the INV Form 71. The SAC will ensure that the proper advice from the prosecutor was obtained before signing the authorization section of the INV Form 71, thereby approving the intercept. The activity will also be reported in an MOA. SAs will complete the report section of the INV Form 71 and submit it to their SAC as soon as practicable and without delay (in no event later than 5 days) after the interception. The original INV Form 71 will be filed in the case file.

5. *Documentation of the Conversation*: For recorded intercepts, it is generally sufficient to report the substance of a consensual intercept in a MOA, without having to transcribe the conversation. However, where the conversation is of particular significance to the investigation, it should be transcribed. When not transcribed, the case agent must listen to the recordings in their entirety to ensure recording quality and to verify the undercover agent's version of events. The original recording used in the interception should be dated, initialed by the seizing agent, and placed into evidence. Working copies of the original recording will be used for transcription and investigative purposes.

6. *Multiple Interceptions and Time Periods*: Approvals at the SAC level are made on the basis of single intercepts, and INV Form 71 **(Exhibit 15-1)** is submitted for each intercept. If it is anticipated that multiple intercepts will be directed against a suspect over a specified period not to exceed 90 days, SACs should receive prior approval from the DAIGI FOD. This should be done in a memorandum submitted by email, with a copy to the SAC DFAU. The memorandum should include all of the information required in INV Form 71, as well as an outline of the investigative plan for multiple interceptions and a justification for the period of time anticipated for the interceptions. If circumstances dictate that intercepts must be utilized over a period in excess of 90 days, then a new approval process must be initiated to extend the authorized period. When requesting an extension of an intercept, approval will follow the same procedures of the original authorization.

7. *Targets:* When any authorization is granted, it applies to only those target individuals and locations identified in the original request. If additional individuals become targets or other circumstances of the monitoring change a separate authorization must be obtained.

E. *Emergency Procedures for Obtaining Approval of Consensual Non-telephone Communications*: If an emergency request must be made during non-working hours and the AUSA/other appropriate prosecuting authority cannot be reached for authorization, the DAIGI or AIGI, if the DAIGI is not available, may authorize an interception. Emergency circumstances are defined as those in which the need arises within 48 hours before the intended intercept. Emergency procedures parallel non-emergency procedures, with the following differences:

1. In those cases where DOJ approval (under Section 15.11) is not required, the DAIGI may verbally authorize the intercept upon verbal receipt of the information called for in INV Form 71 **(Exhibit 15-1)** and the circumstances giving rise to the emergency.

2. The AUSA must be apprised of the circumstances involved as soon as practicable after the emergency approval.

3. Emergency request in cases in which DOJ approval is required may be made by telephone to the director or an associate director of the OEO or to the Assistant Attorney General or a Deputy Assistant Attorney General for the Criminal Division

and should later be reduced to writing and submitted to the appropriate officials as soon as practicable after authorization has been obtained. SACs should coordinate with the SAC DFAU in such cases.

15.10 INTERCEPTION/MONITORING WHEN SENSITIVE CIRCUMSTANCES ARE PRESENT AND WHERE PRIOR WRITTEN AUTHORIZATION FROM THE DEPARTMENT OF JUSTICE IS REQUIRED

A. *Sensitive Circumstances Where Prior Written DOJ Approval is Required*: A request for authorization to monitor an oral communication without the consent of all parties to the communication must be approved in writing by the Director or Associate Directors of the OEO, Criminal Division, DOJ, when it is known that one of the following sensitive circumstances is present:

1. The interception relates to an investigation of a member of Congress, a Federal judge, a member of the Executive Branch at Executive Level IV or above, or a person who has served in such capacity within the previous two years.

2. The monitoring relates to the investigation of the Governor, Lt. Governor, or Attorney General of any State, or Territory, or a Judge or Justice of the highest court of any State or Territory, and the offense investigated is one involving bribery, conflict of interest, or extortion relating to the performance of his official duties.

3. Any party to the communication is a member of the diplomatic corps of a foreign country.

4. Any party to the communication is or has been a member of the Witness Security Program and that fact is known to the agency involved or its officers.

5. The consenting or non-consenting person is in the custody of the Bureau of Prisons (BOP) or in the custody of the U.S. Marshals Service. [Note: See SAH Chapter 11.9 Special Approval Requirements regarding additional concerns.] In such cases, the memorandum requesting authorization will include the INV Form 74, Authorization for Use of a BOP Prisoner or Employee **(Exhibit 15-4)** and INV Form 65, Cooperating Individual Agreement for Persons in Custody **(Exhibit 15-5)** and contain the following additional information:

   a. the location of the prisoner;

   b. identifying data concerning the prisoner (Federal Bureau of Investigation (FBI) number, BOP number, sex, inmate identification number, Social Security number, and criminal history);

   c. charges for which the prisoner is incarcerated, including date and sentence;

   d. copy or summary of the prisoner's arrest record;

e. necessity of utilizing the prisoner in the investigation, and what other techniques have been tried and why they have failed;

f. name of target of the investigation and the target's role in the crime or organization under investigation;

g. the prisoner's relationship or association with the target;

h. whether the target is aware of the prisoner's incarceration status. If so, what is the prisoner's cover story to avoid jeopardizing his or her safety or the investigation;

i. explanation in detail of the nature of the activity being requested (for example, wearing a consensual monitoring device, furlough, or extraordinary transfer);

j. security measures to be taken to ensure the prisoner's safety, alleviate risk to the public, and prevent the prisoner's escape;

k. length of time the prisoner will be needed in the activity;

l. whether the prisoner will be needed as a witness or will be considered for the Witness Security Program;

m. whether a prison transfer will be necessary upon completion of the activity;

n. whether the prisoner will remain in the custody of the investigative agency, be housed in jails or similar facilities at certain times, or be unguarded except for protection;

o. the number of law enforcement agents assigned to the security detail;

p. whether the request been endorsed by the federal or state prosecutor directly involved in the matter (if another prosecutor is consulted, provide the name and contact information for that prosecutor and the reason for consulting the attorney);

q. an interim progress report if the intercept activity is a continuance (a detailed report should be submitted at the conclusion of activity); and

r. a sealed court order, obtained after a request has been approved, if the prisoner is un-sentenced or on writ status.

6. The Attorney General, Deputy Attorney General, Associate Attorney General, Assistant Attorney General, or the United States Attorney in the district where the investigation is being conducted has requested the investigating agency to obtain prior written consent before conducting consensual monitoring in a specific investigation.

B. *Exceptions:* Even if the interception falls within one of the six categories above, the procedures and rules in this Section do not apply to:

1. Extraterritorial interceptions;

2. Foreign intelligence interceptions, including interceptions pursuant to the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. §1801, et seq.);

3. Interceptions pursuant to the court-authorization procedures of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended (18 U.S.C. §2510, et seq.);

4. Routine BOP monitoring of oral communications that are not attended by a justifiable expectation of privacy;

5. Interceptions of radio communications; and

6. Interceptions of telephone communications.

C. *Application Requirements - Coordination with a Federal Prosecutor*: SAs, with prior SAC approval, must seek AUSA advice and assistance in drafting and submitting this request, and in conducting the monitoring. The AUSA should draft and submit the request to OEO. The following information must be set forth in any request to monitor an oral communication pursuant to Section 15.6 A, above:

1. *Reasons for the Monitoring*: The request must contain a reasonably detailed statement of the background and need for the monitoring.

2. *Offense*: If the monitoring is for investigative purposes, the request must include a citation to the principal criminal statute involved.

3. *Danger*: If the monitoring is intended to provide protection to the consenting party, the request must explain the nature of the danger to the consenting party.

4. *Location of Devices*: The request must state where the monitoring device will be hidden: on the person, in personal effects, or in a fixed location.

5. *Location of Monitoring*: The request must specify the location and primary judicial district where the monitoring will take place. A monitoring authorization is not restricted to the original district. However, if the location of monitoring changes, notice should be promptly given to the approving official. The record maintained on the request should reflect the location change.

6. *Time*: The request must state the length of time needed for the monitoring. Initially, an authorization may be granted for up to 90 days from the day the monitoring is scheduled to begin. If there is the need for continued monitoring, extensions for

additional periods of up to 90 days may be granted. In special cases (e.g., "fencing" operations run by law enforcement agents or long-term investigations that are closely supervised by the Department's Criminal Division), authorization for up to 180 days may be granted with similar extensions.

7. *Names*: The request must give the names of persons, if known, whose communications the department or agency expects to monitor and the relation of such persons to the matter under investigation or to the need for the monitoring.

8. *Attorney Advice*: The request must state that the facts of the surveillance have been discussed with the United States Attorney, an AUSA, or the previously designated DOJ attorney responsible for a particular investigation, and that such attorney advises that the use of consensual monitoring is appropriate under this Memorandum (including the date of such advice). The attorney must also advise that the use of consensual monitoring under the facts of the investigation does not raise the issue of entrapment. Such statements may be made orally. If the attorneys described above cannot provide the advice for reasons unrelated to the legality or propriety of the consensual monitoring, the advice must be sought and obtained from an attorney of the Criminal Division of the DOJ designated by the Assistant Attorney General in charge of that Division. Before providing such advice, a designated Criminal Division attorney shall notify the appropriate United States Attorney or other attorney who would otherwise be authorized to provide the required advice under this paragraph.

9. *Renewals*: A request for renewal authority to monitor oral communications must contain all the information required for an initial request. The renewal request must also refer to all previous authorizations and explain why an additional authorization is needed, as well as provide an updated statement that the attorney advice required under paragraph (8) has been obtained in connection with the proposed renewal.

D. *Oral Requests*: Unless a request is of an emergency nature, it must be in written form and contain all of the information set forth above. Emergency requests in cases in which written DOJ approval is required may be made by telephone to the Director or an Associate Director of the Criminal Division's OEO, or to the Assistant Attorney General, the Acting Assistant Attorney General, or a Deputy Assistant Attorney General for the Criminal Division, and should later be reduced to writing and submitted to the appropriate headquarters official as soon as practicable after authorization has been obtained. A copy of the written request and approval under this procedure must be submitted to the DAIGI and uploaded to the OIG Enterprise Data System (EDS) within five days of its submission to DOJ. Oral requests must include all the information required for written requests as set forth above.

E. *Emergency Monitoring*: If an emergency situation requires consensual monitoring at a time when one of the individuals identified in Section 15.6 D, above cannot be reached, the authorization may be given by the Inspector General. The SAC must then ensure that the DOJ, OEO is notified in writing as soon as practicable, but no later than 3 days of the

emergency approval. The notification shall explain the emergency and shall contain all other items required for a nonemergency request for authorization set forth in Section 15.6 C, above.

15.11 NON-CONSENSUAL INTERCEPTS

A. *General Terms and Provisions*: Non-consensual interception of communications is the act of intercepting verbal, wire or non-wire communications when no party to the communications has consented and when all parties have a reasonable expectation of privacy. These interceptions are sometimes referred to as "wiretaps," for telephone or wire intercepts, and "bugs," for non-wire intercepts. Interceptions of nonconsensual wire and non-wire communications that include the human voice are subject to the provisions of 18 U.S.C. § 2510 *et seq*., commonly referred to as Title III. Title III prohibits all such intercepts except where authorized by a court order. Deviation from the specified procedures may jeopardize the case and give rise to sanctions from civil lawsuits, contempt proceedings, and criminal actions against those responsible for unauthorized interceptions. Note that cellular telephone calls are protected as wire communications, and a court order is required to monitor the wire and radio portion of cellular telephone conversations.

B. *Statutory and Regulatory Approval Provisions*: SA requests for non-consensual intercepts are submitted to the assigned prosecutor in consultation with, and the prior written approval of, the SAC or ASAC. One of Title III's most restrictive provisions is the requirement that Federal investigative agencies submit requests for the non-consensual interception of wire and oral communications to the DOJ for review and approval before applications for such interception may be submitted to a court of competent jurisdiction for an order authorizing the interception. Specifically, in 18 U.S.C. § 2516(1), Title III explicitly assigns such review and approval powers to the Attorney General, but allows the Attorney General to delegate this review and approval authority to a limited number of high-level DOJ officials, including Deputy Assistant Attorneys General for the Criminal Division ("DAAGs"). The DAAGs review and approve or deny proposed applications to conduct "wiretaps" (to intercept wire [telephone] communications, 18 U.S.C. § 2510(1)) and to install and monitor "bugs" (the use of microphones to intercept oral [face-to-face] communications, 18 U.S.C. § 2510(2)). It should be noted that only those crimes enumerated in 18 U.S.C. § 2516(1) may be investigated through the interception of wire or oral communications. On those rare occasions when the government seeks to intercept oral or wire communications within premises or over a facility that cannot be identified with any particularity, and a "roving" interception of wire or oral communications is therefore being requested, the Assistant Attorney General or the Acting Assistant Attorney General for the Criminal Division must be the one to review and approve or deny the application. (See the roving interception provision at 18 U.S.C. § 2518(11)).

C. *Telephone versus Non-Telephone Intercepts*: Nonconsensual non-telephone intercepts are governed by the same statutes and policy controlling nonconsensual telephone intercepts. All provisions of Section 15.12 below apply equally, with the exception that

the "object" for non-wire intercepts is a place, and the "object" for a wire intercept is a telephone.

D. *Special Mandatory Application Provisions Applying to DHS OIG*: Non-consensual intercepts are governed by the Attorney General's Procedures for Lawful, Warrantless Monitoring of Verbal Communications, set forth by memorandum dated May 30, 2002 (**Exhibit 15-3**). Any investigation involving the interception of communications pursuant to 18 U.S.C. § 2510, *et seq*., and any other court-ordered electronic surveillance must be conducted only after consulting with the FBI and appropriate USAO or Criminal Division litigating section. Subsequent to such notification, the FBI may choose to join the investigation, but is not required to do so. However, if DHS OIG intends to engage in court-authorized electronic surveillance without the participation of the FBI, one of the following federal investigative agencies must participate in the investigation and supervise the application for and use of the surreptitious electronic surveillance: the Drug Enforcement Administration; Bureau of Alcohol, Tobacco, Firearms and Explosives; Homeland Security Investigations; United States Postal Inspection Service; United States Secret Service; or Internal Revenue Service.

15.12 APPLICATION AND PROCEDURES FOR NON-CONSENSUAL INTERCEPTION

A. *Preliminary Consultation and Selection of a Partnering Federal Agency*: In any investigation where a non-consensual interception of wire and/or oral communications is contemplated or where any investigative activity may implicate the wiretap provisions of Title III, SAs should first consult in detail with the FBI and determine whether the FBI will join the investigation, as provided above. If the FBI declines, the SAC should approach another appropriate federal agency, as detailed above, and determine whether the agency will join the investigation. This activity must be documented in an email to the DAIGI.

B. *Preliminary Evaluation and Planning Factors:* Once a partnering federal agency has been determined, the SAC and a representative from the partnering agency shall consult with the federal prosecutor assigned to the matter or, if no prosecutor is assigned, with an AUSA with jurisdiction over the offense. If the federal prosecutor consulted is satisfied that the investigative activity in question falls within the scope of the wiretap provisions of Title III, as described in Section 15.7 above, and interception is required, the SAC should work with the prosecutor to develop a plan for complying with the requirements of Title III, including the drafting and submission of an Authorization Request to the DOJ. The SAC should also inform their DAIGI in writing. The following preliminary evaluation and planning factors will be considered:

1. [redacted]

[redacted]

2. [redacted]

3. [redacted]

4. [redacted]

5. [redacted]

6. [redacted]

   a. [redacted]

   b. [redacted]

7. [redacted]

8. [redacted]

[redacted]

9. [redacted]

C. [redacted]

1. [redacted]

2. [redacted]

3. [redacted]

4. [redacted]

5. [redacted]

6. [redacted]

[redacted]

7. [redacted]

D. *Notification to DAIGI and AIGI Before Application for a Court Order to Conduct an Interception of Wire Communication*: When a Title III intercept is anticipated, the SAC must notify the AIGI by memorandum through their DAIGI as early as possible. The memorandum should include the following information:

1. Case number and identification information;

2. Telephone number and subscriber's name and address (wiretap) or specific location information (bug);

3. Supervising attorney;

4. Name and phone numbers (office and cell) of ASAC and SAC;

5. Affiant (case agent);

6. Anticipated date that affidavit/draft order package will be submitted to INV Headquarters;

7. Judicial district in which application will be made;

8. Brief statement substantiating that the telephone is being used to engage in unlawful activity as enumerated in 18 U.S.C. § 2516; and

9. Brief statement as to availability of necessary equipment and technical expertise and the need for technical assistance from the DFAU.

E. *Preparation of the Authorization Request*: The preparation of this package requires detailed technical knowledge of the pertinent laws, regulations, and DOJ requirements. It should be prepared by the SAC and the partnering federal agency in close coordination with the supervising DOJ attorney. Once the affidavit, application, and orders are drafted, copies of the paperwork will be distributed as follows:

1. The original set is retained by the originating office for subsequent presentation to the court; and

2. A copy of the set is submitted to the DAIGI, who after approval will forward to the AIGI.

F. *Format for the Authorization Request:* When DOJ review and approval of a proposed application for electronic surveillance is required, the Electronic Surveillance Unit (ESU) of the Criminal Division's OEO will conduct the initial review of the necessary pleadings, which include:

1. The affidavit of an "investigative or law enforcement officer" of the United States who is empowered by law to conduct investigations of, or to make arrests for, offenses enumerated in 18 U.S.C. § 2516(1) or (3) (which, for any application involving the interception of electronic communications, includes any Federal felony offense), with such affidavit setting forth the facts of the investigation that establish the basis for those probable cause (and other) statements required by Title III to be included in the application (the affiant should be from the partnering federal agency supervising the intercept);

2. The application by any United States Attorney or his/her Assistant, or any other attorney authorized by law to prosecute or participate in the prosecution of offenses enumerated in 18 U.S.C. § 2516(1) or (3) that provides the basis for the court's jurisdiction to sign an order authorizing the requested interception of wire, oral, and/or electronic communications;

3. The order to be signed by the court authorizing the government to intercept, or approving the interception of, the wire, oral, and/or electronic communications that are the subject of the application; and

4. A completed Title III cover sheet that includes the signature of a supervising attorney who reviewed and approved the Title III papers. The AIGI must sign the Title III cover sheet, demonstrating that he or she has reviewed the affidavit, application, and draft order included in the submission packet, and that, in light of the overall investigative plan for the matter, and taking into account applicable Department policies and procedures, he or she supports the request and approves of it.

G. *Submission to DOJ*: Upon completing a review and concurrence, the head of the supervising federal agency will submit a memorandum to the Assistant Attorney General, Criminal Division, requesting approval. As designated by the Attorney General, the Assistant Attorney General in charge of the Criminal Division, any Acting Assistant Attorney General in charge of the Criminal Division, and any Deputy Assistant Attorney General of the Criminal Division may authorize applications for interceptions of wire and oral communications. Upon the appropriate official's review and concurrence, that official will furnish written approval to the appropriate USAO. The original application, together with the written department approval, may then be presented to the appropriate court. Generally, about five working days are needed to obtain DOJ approval, unless significant changes are required. If necessary, expedited review can sometimes be arranged with adequate notice to OEO, Electronic Surveillance Unit. The statute requires sealing of applications and orders. Typically the title III order includes language providing for nondisclosure and sealing.

H. *After Obtaining the Authorization*: Upon the court granting the intercept order, the SAC will notify their DAIGI as to the dates of the order and the activation of the intercept.

I. *Ongoing Coordination by the DAIGI*: From the point of initial notification to the DAIGI that an application for a court ordered intercept is anticipated, the DAIGI will assume overall responsibility for coordinating the approval of the application and for providing technical assistance to the office conducting the intercept, including providing onsite technical personnel.

J. [redacted]

K. [redacted]

L. *Daily Reports and a Master Affidavit*: A daily report should be completed summarizing all pertinent calls for the benefit of communications between the personnel on [redacted], the personnel from one shift to the next, and management. [redacted]. Weekly progress reports can be easily compiled from the daily reports. The result is a chronological master affidavit incorporating all pertinent information from all sources. At the conclusion of the investigation, this master affidavit can be applied to all arrest and search warrants.

M. *Requesting Extensions to a Wire Intercept*. Extensions to a wire intercept may be granted for up to 30 days, and are processed in the same manner as the original application.

N. *Terminating the Wire Intercept*: The intercept must be terminated when the investigative objective for which it was approved has been achieved. Because determining this precise point can be difficult, the progress and usefulness of the intercept should be the subject of a daily discussion with the supervising DOJ attorney.

O. *Reporting Requirements for Wire Intercepts*: When the court grants the intercept order, it may require progress reports at specified intervals. The contents of these reports should reflect progress toward the objective (or reasons why progress has been hampered) and the need to continue the intercept. As stated in 18 U.S.C. § 2518(8)(d), within a reasonable time but not later than 90 days after terminating the intercept, all persons whose telephonic conversations were intercepted or who were named in the order and who are so designated by the court will be notified of these interceptions.

15.13 NON-VOICE ELECTRONIC COMMUNICATIONS OVER A NETWORK

A. *General Provisions*: In 1986, Congress amended Title III by enacting the Electronic Communications Privacy Act of 1986 (ECPA). Specifically, Congress added "electronic communications" as a new category of communications whose interception is covered by Title III. Electronic communications are non-voice communications made over a network in or affecting interstate commerce, and include text messages, electronic mail ("email"), facsimiles ("faxes"), other non-voice Internet traffic, and communications over digital-display pagers. See 18 U.S.C. § 2510(12).

B. *Other Protected Communications*: Radio communications that carry the human voice are protected as electronic communications if carried entirely over a radio communications system configured so the communications are not readily accessible to the general public. If a voice radio communication is carried in part over a wire telephone system, then the entire communication may be classified as a wire communication. Other examples of protected electronic communications are other computer transmissions and private nonverbal closed circuit television (CCTV) transmissions. Other similar transmissions are included if they are not readily accessible to the general public.

C. *Court Order Requirements*: In very general terms, in the absence of a specified exception, ECPA requires law enforcement to obtain a court order to intercept private electronic communications in real time. 18 U.S.C. §§ 2510 et seq. ECPA also generally requires law enforcement to obtain a search warrant to view the contents of unopened e-mail stored by electronic communications providers. 18 U.S.C. §§ 2701 et seq. For a discussion of ECPA, see Federal Guidelines for Searching and Seizing Computers, U.S. DOJ, Criminal Division (1994) and Supplement (1999), available online at ww.usdoj.gov/criminal/cybercrime.

D. *Department of Justice Approval Requirements*: With the exception of requests for the interception of electronic communications over digital-display paging devices, DOJ approval prior to application to the court is required for the interception of any type of electronic communications, including text messages, faxes, emails, and other non-voice communications over a computer. Applications to the court for authorization to intercept electronic communications over digital-display pagers may be made based solely upon the authorization of a United States Attorney. See 18 U.S.C. § 2516(3).

15.14 ACCESS TO STORED ELECTRONIC COMMUNICATIONS

A. *General Provisions Under the Electronic Communications Privacy Act*: The stored communication portion of ECPA, 18 U.S.C. §§ 2701-2712, creates statutory privacy rights for customers and subscribers of computer network service providers and regulates how the government can obtain stored account information from such providers. Whenever DHS OIG SAs seek stored e-mail, account records, or subscriber information from a network service provider, they must comply with ECPA.

B. *Providers of Electronic Communication Service vs. Remote Computing Service*: ECPA divides providers covered by the statute into "provider[s] of electronic communication service" and "provider[s] of remote computing service." An electronic communication service is "any service which provides to users thereof the ability to send or receive wire or electronic communications," according to 19 U.S.C. § 2510(15). For example, telephone companies and electronic mail companies generally act as providers of electronic communication services. The term remote computing service is defined by 18 U.S.C. § 2711(2) as "provision to the public of computer storage or processing services by means of an electronic communications system." An electronic communications system is "any wire, radio, electromagnetic, photo optical or photo electronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications," according to 18 U.S.C. § 2510(14). Roughly speaking, a remote computing service is provided by an off-site computer that stores or processes data for a customer. Whether an entity is a provider of electronic communication service, a provider of remote computing service, or neither depends on the nature of the particular communication sought. For example, a single provider can simultaneously provide electronic communication service with respect to one communication and remote computing service with respect to another communication.

C. *Electronic Storage*: 18 U.S.C. § 2510(17) defines electronic storage as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" or, in the alternative, as "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." Accordingly, electronic storage refers only to temporary storage, made in the course of transmission, by a provider of electronic communication service. As a practical matter, whether a communication is held in electronic storage by a provider governs whether that service provides electronic communication service with respect to the communication. The two concepts are coextensive: a service provides electronic communication service with respect to a communication if and only if the service holds the communication in electronic storage. Thus, it follows that if a communication is not in temporary, intermediate storage incidental to its electronic transmission, the service cannot provide electronic communication for that communication. Instead, the service must provide either "remote computing service" or else neither electronic communication service or remote computing service.

D. *Compelled Disclosure Under the ECPA*: 18 U.S.C. § 2703 provides the steps that the government must take to compel providers to disclose the contents of stored wire or electronic communications (including e-mail and voice mail) and other information, such as account records and basic subscriber information. Section 2703 offers five mechanisms that the government may use to compel a provider to disclose information: (1) subpoena; (2) subpoena with notice to the subscriber or customer; (3) § 2703(d) court order; (4) § 2703(d) court order with prior notice to the subscriber or customer; and (5) search warrant.

E. *Subpoena*: ECPA permits the government to compel two kinds of information using a subpoena (grand jury or administrative). The first type of information is the basic subscriber information listed in 18 U.S.C. § 2703(c)(2): (1) name; (2) address; (3) local and long distance telephone connection records or records of session times and durations; (4) length of service (including start date) and types of service utilized; (5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (6) means and source of payment for such service (including any credit card or bank account number). SAs can also use a subpoena to obtain information that is outside the scope of ECPA, for example information that is held by an entity other than a remote computing service or electronic communication service, such as an employer who retains e-mail records on an internal system.

F. *Subpoena With Notice*: SAs who obtain a subpoena and either give prior notice to the subscriber or comply with the delayed notice provisions of § 2705(a) may obtain: (1) everything that can be obtained using a subpoena without notice; (2) "the contents of any wire or electronic communication" held by a provider of remote computing service "on behalf of . . . a subscriber or customer of such remote computing service," according to 18 U.S.C. § 2703(b)(1)(B)(i), § 2703(b)(2); and (3) "the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days," according to 18 U.S.C. § 2703(a). As a practical matter, DOJ has been requiring a warrant for the retrieval of any stored communications, opened or unopened, following the decision in United States v. Warshak (*US v. Warshak*, 631 F.3d 266 (6th Cir. 2010)).

G. *Court Orders and Warrants*: In order to obtain information beyond that described above, including account logs and transactional records and the content of unopened e-mail and voicemail which has been in electronic storage 180 days or less, an agent must obtain either a court order or a warrant. If a particular investigation warrants the collection of such information, consult with the Counsel or the assigned federal prosecutor.

H. *Cost Reimbursement*: ECPA generally obligates government entities to reimburse the disclosing person or entity for the reasonable costs incurred in providing ECPA information. Any bills received in connection with the provision of ECPA material should be directed to the attention of the SAC DFAU, who will consult with the DAIGI and Office of Counsel as necessary.

15.15 VIDEO SURVEILLANCE

A. *General Provisions*: Video cameras and related viewing and recording equipment are valuable investigative tools available to DHS OIG. However, where a reasonable expectation of privacy exists, the use of video surveillance requires a court order and DHS OIG and DOJ authorization. SAs should consult the prosecutor with case-specific questions regarding reasonable expectation of privacy. All recordings made during video surveillance should be considered evidence and handled according to DHS OIG's evidence storage and handling procedures. Pursuant to DOJ Order No. 985-82, dated

August 6, 1982, certain officials of the DOJ Criminal Division have been delegated authority to review requests to use video surveillance for law enforcement purposes when there is a constitutionally protected expectation of privacy requiring judicial authorization. This authority was delegated to the Assistant Attorney General, any Deputy Assistant Attorney General, and the Director and Associate Directors of the OEO. Accordingly, DHS OIG use of video is restricted as indicated below:

1. [redacted]

2. [redacted]

B. *Video Installation and Viewing in Public Places*: Public places include such areas as open fields, public streets, public parking lots, and other places to which the public has continuous access. No prior court order or DOJ approval is required to install video in public places or to view places that remain continuously public. However, whether the place of installation is completely and continuously "public" requires legal analysis. Accordingly, installation of video monitoring equipment in public places requires consultation with an AUSA, DFAU and final DAIGI approval.

1. *Specific Approval Procedures*: Prior to installation, SAs must consult with an AUSA regarding the propriety of video installation in the place purported to be public. After obtaining concurrence from the AUSA, SAs will submit a request for installation by memorandum through their ASACs, field SACs and SAC DFAU to the appropriate DAIGI. If the SAC approves the installation, he/she must forward the approved memorandum to the DAIGI through the SAC DFAU for final approval. The SAC DFAU will provide consultation and comment to their DAIGI upon forwarding the request to the DAIGI. The DAIGI will also consult with OIG Counsel as appropriate before deciding whether to approve the request and authorize the installation. The memorandum to the DAIGI should contain the following information:

   a. Case identification information;

   b. Reason for the monitoring;

c. Steps taken to review privacy implications of the installation;

d. Type/description/locations of equipment used;

e. Descriptions of how monitoring and review of the material will be conducted; and date of SAC approval.

C. *Consensual Video Installation and Viewing in Private Areas*: The procedures for installing and viewing consensually obtained video surveillance in private areas are generally the same as for consensual monitoring of oral communication, provided in Section 15.9, above. Consultation with and approval from an AUSA or DOJ Trial Attorney and subsequent DAIGI approval is required before conducting consensual video surveillance, and the surveillance can only be conducted in the presence of the consenting party. Surveillance must be stopped whenever the consenting party is absent from the viewing area. Properly obtained consent must cover the entire period of video installation in a private area and be documented on INV Form 72/72S **(Exhibit 15-2 and 15-2S Spanish Version)**.

1. *Specific Approval Procedures*: SAs will seek the necessary advice and approval from an AUSA or Trial Attorney and, if prosecutor approval is obtained, request approval by memorandum through the ASAC, SAC and SAC DFAU to the appropriate DAIGI. If upon review of the memorandum the SAC concurs with the request and is satisfied with prosecutor approval, he/she should forward the approved request to their DAIGI through the SAC DFAU for final approval. The SAC DFAU will provide consultation and comment to the DAIGI upon forwarding the request to the DAIGI. The DAIGI will also consult with OIG Counsel as appropriate before deciding whether to approve the request and authorize the installation. The memorandum to the DAIGI should contain the following information:

   a. Case identification information

   b. Reason for the monitoring

   c. Steps taken to review privacy implications of the installation

   d. Type/description/locations of equipment used

   e. Descriptions of how monitoring and review of the material will be conducted

   f. Date of SAC approval

D. [redacted]

[redacted]

1. *Specific Approval Procedures*: The specific procedures to be followed are set forth in Sections 15.12, above. These procedures should be followed closely, and notification to and consultation with the DAIGI and AIGI should occur as early as possible. The DAIGI and AIGI will consult with the SAC DFAU and OIG Counsel before determining whether the application package is technically and legally sufficient for the AIGI to forward to the DOJ Criminal Division. The AIGI will forward the application and supporting affidavit to the Criminal Division for approval prior to submission to the court.

15.16 [redacted]

[redacted]

15.17 [redacted]

A. [redacted]

[redacted]

B. [redacted]

2. [redacted]

C. *When a Court Order is Required*: As discussed in SAH Section 15.13 (C), SAs should be mindful that, in the absence of a specified exception, ECPA requires law enforcement to obtain a court order to intercept private electronic communications in real time. 18 U.S.C. §§ 2510 et seq. ECPA also generally requires law enforcement to obtain a search warrant to view the contents of unopened e-mail stored by electronic communications providers. 18 U.S.C. §§ 2701 et seq.

D. *Obtaining Information from Unrestricted Sources*: SAs may obtain information from publicly accessible online sources and facilities under the same conditions as they may obtain information from other sources generally open to the public. This principle applies to publicly accessible sources, such as Facebook or Twitter profiles, located in foreign jurisdictions as well as those in the United States.

E. [redacted]

F. *Observing and Logging Real-Time Communications*: SAs may passively observe and log real-time electronic communications open to the public under the same circumstances in which the agent could attend a public meeting. SAs may not access restricted online sources or facilities absent legal authority permitting entry into private space.

1. Facilities such as *Internet Relay Chat* (IRC), and its analogues within individual service providers (such as "chat rooms"), permit online users to engage in real-time discussions. Participants can normally make these discussions private (i.e., prevent access by the general public) in which case the protections and requirements of ECPA apply.

2. SAs can passively observe and log only at those online discussions to which public access has not been restricted; in such cases, ECPA affords no statutory protection to the communications (see 18 U.S.C. § 2511(2)(g)), and the absence of any reasonable expectation of privacy means that the agent's observing or recording of such communications would not violate the Fourth Amendment.

3. When an agent's activity in a real-time forum crosses from mere monitoring into active participation, it raises issues addressed in Subsection (I) below regarding communications online.

G. *Accessing Restricted Sources*: SAs may not access restricted online sources or facilities absent legal authority permitting entry into a private space.

1. In the online world, as in the physical world, some individuals, resources, or facilities may choose not to make their information or services available to all, but instead may place restrictions on who may access their services. Some may open their sites only to persons of a particular group. Others may decide to open their facilities to everyone except law enforcement personnel. Online technology permits such restrictions through the use of such things as passwords, allowing only persons authorized by the system operator to access them. Similarly, most real-time "chat" programs also permit private conversations that are not open to the general public. Even sites that are otherwise open to the public may attempt to exclude law enforcement through either passive measures (such a banner saying "police not welcome") or active measures (such as requiring a negative response to the question "Are you a police officer?" before allowing access). SAs should consult the

prosecutor with case-specific questions regarding reasonable expectation of privacy, to include whether such banners create a reasonable expectation of privacy.

2. When encountering an online facility, resource, group, forum or other such online area where access has been restricted like this, SAs must respect those restrictions to the extent they create recognizable expectations of privacy. Law enforcement may access such places only if they have authority to enter similarly restricted places in the physical world. The Fourth Amendment allows law enforcement agents to access private places only when they have consent of the owner or user, a warrant authorizing them to enter, or a legally recognized exception to the warrant requirement.

3. As in the physical world, consent is valid even if based on a false self-identification by law enforcement. For example, an agent using a fictitious online identity may invite a suspect to connect via social media (e.g., "friend"). Consent is given when the suspect accepts the agent's invitation. This consent allows the agent to look at social media content even though the agent used a false identity.

H. *Online Communication Generally*: SAs may use online services to communicate as they may use other types of communication devices, such as the telephone and the mail. SAs should retain the contents of a stored electronic message, such as an e-mail, if they would have retained that message had it been written on paper. The contents should be preserved in a manner authorized by the procedures governing the preservation of electronic communications set forth in SAH Chapters 8 and 16.

I. *Online Undercover Activities*:

1. *General Considerations*: Online undercover activities and operations are to be generally guided by the provisions of SAH Chapter 13.

2. [redacted]

3. [redacted]

[redacted]

4. [redacted]

5. *Online Communication Restrictions*: For safety and security reasons, agents who are, or who may reasonably be expected to work in undercover operations, shall not post, transmit, or disseminate via social media any form of visual or personal identification. Furthermore, agents must avoid using a username or password that can be traced back to, or may provide any clues as to the identity of, the user or OIG.

6. [redacted]

J. [redacted]

1. [redacted]

[redacted]

2. *DAIGI Approval*: The SAC DFAU will review the request and forward it to the requesting SAC's DAIGI with a recommendation to approve or disapprove the request. The DAIGI will consider the request and the SAC DFAU recommendation and approve or disapprove the request as provided below in paragraph K. Once the DAIGI has approved or disapproved the request, he or she will provide notification to both the requesting SAC and the SAC DFAU. [redacted]

3. [redacted]

4. [redacted]

K. [redacted]:

1. [redacted]

2. Requests to communicate in an undercover capacity should be drafted by the SA via email or memorandum on a case-specific basis, following consultation with DFAU. The requests must be routed through the SAC, and must be approved by the DAIGI FOD or the AIGI. The requests should include the following:

[redacted]

L. [redacted]:

[redacted]

M. *Documentation, Storage, Retention and Dissemination*:

1. DHS OIG policies regarding recordkeeping also apply to online investigations. [redacted]

2. Requests for online queries and resulting records will be documented in an MOA and included in the original casefile.

3. Information obtained online that is evidentiary in nature and obtained in the course of an investigation must be collected and retained using screen shots, printouts of communication logs, copying URLs for subpoena or investigatory purposes, and/or storing the information via secure digital means.

N. *Authentication of Evidence Obtained Online*: Information and data obtained online is not necessarily reliable, and may not be appropriate as a primary or sole source for information and verification. Because sources of evidence found online can be difficult if not impossible to verify, information found online must be thoroughly checked and evaluated to ensure that it is accurate and online sources must be authenticated. This usually requires the use of other investigative techniques. For example, to authenticate the source of a YouTube video showing individuals engaging in visa fraud, SAs should obtain a subpoena to determine the IP address used to upload the video and to identify to whom the IP address was registered at the time of upload.

1. Like any other type of evidence, evidence deriving from online sources needs to be properly preserved and authenticated to be admissible in a court of law. In other words, online evidence must be collected and secured in a form that is admissible and persuasive at trial. Evidence found online has been ruled admissible, for instance, where the content of the evidence contained sufficient indicia that it is the authentic creation of the purported user. Accordingly, a large part of any investigative activity conducted online is proving the source; effectively establishing that the evidence is what it purports to be and has the probative value it purports to have. Failure to authenticate electronic evidence can result in exclusion from trial. For the highest level of authenticity, SAs will typically obtain content and identifying data directly from internet service and social media providers with a subpoena.

2. ECPA governs DHS OIG's ability to compel production of content (e.g., posts, Tweets) and non-content customer records (e.g., name, email address). In some circumstances, DHS OIG may compel social media providers to produce social media evidence with an IG subpoena. SAs may consult with OIG Counsel to determine whether an IG subpoena would be appropriate for gathering information from social media accounts. Such IG subpoenas should be discussed with the prosecutor before they are issued.

O. *International Investigations Online*: When conducting an online investigation it is often difficult to discern whether the investigative activity has engaged a computer system or platform, data, witnesses, or subjects located outside of the United States. However, initiating personal contact with residents of a foreign country, accessing the non-public social media sites of a foreign national, or using an online forum or platform hosted in another country may: (1) be regarded as a violation of the other nation's sovereignty; (2) violate that country's laws or a treaty; and (3) harm diplomatic affairs with the United States. Furthermore, depending on the jurisdiction, such contact may expose the agent to personal criminal liability. Accordingly, before conducting online undercover activities SAs must make reasonable efforts to ascertain whether such foreign elements may be involved in the activity and, where such a condition is possible, seek guidance from the

USAO with venue over the investigation or Office of Counsel if no such venue has been determined. For help discerning the possibility that foreign elements will be involved in the activity planned, SAs should consult with the SAC DFAU and feel free to consult with DOJ's Computer Crimes and Intellectual Property Section, the Criminal Division Section with expertise in such legal issues. Because each country has its own laws and requirements, AUSAs may also have to consult DOJ's Office of International Affairs before giving guidance to the SA. In the Republic of Mexico, law enforcement activity is governed by the Brownsville-Merida Protocols (BMP). See the Special Agent Handbook, 11.14, for more guidance relating to Mexico.

P. *Privacy Act Restrictions and Considerations*: To comply with the *Privacy Act of 1974*, 5 U.S.C. § 552a, and other privacy laws, SAs will not use social media or other online facilities to maintain, collect, use, or disseminate information about the following topics, unless records are within the scope of an authorized law enforcement activity:

1. Individuals' or organizations' religious, political, or social views, or associations and activities;

2. An individual's participation in a particular non-criminal organization or lawful event;

3. An individual's race, ethnicity, citizenship, place of origin, disability, gender, or sexual orientation; or

4. An individual's age (other than to determine if someone is a minor).

Q. *Contact with Minors*: SAs should take all reasonable precautions to establish that the persons with whom they interact on social media are not minors. SAs should not intentionally contact minors via social media.

15.18 MOBILE TRACKING DEVICES

A. *General Provisions*: A Mobile Tracking Device (MTD) is a device designed for automatically determining and transmitting the geographic location of a vehicle, person or other item. Such devices typically have a built in memory capacity that enables the storage of location data until it is collected or downloaded by the SA. When location data is collected in this way, it provides a complete depiction of travel over a period of time. Among other things, such devices attached covertly can be used to track journeys made by individuals who are under surveillance, particularly when they are using vehicles. In many more recent devices, the location is determined using a Global Positioning System (GPS) and/or ground based, cellular tower location data. In some devices, location data can be transmitted in real-time via satellite or terrestrial radio signals to a radio receiver for surveillance purposes.

B. *Request for Equipment from Headquarters*: SAs contemplating the use of an MTD should be mindful that a field office may not have an MTD on hand. If an MTD is not

locally available, the equipment will have to be requested from the EISPM at HOD and shipped to the field office. SAs should be sure to make this request in a timely manner in order to ensure that any critical investigative timing requirements are met. MTD requests must be directed to the EISPM, who reports to the SAC DFAU, after receiving approval under the procedures below.

C. *Approval Procedures*: A search warrant is required to install and use such devices to monitor the movements of an object or vehicle. The SA must consult with the local USAO prior to proceeding with any implementation of this investigative tool. This warrant requirement was decided by the Supreme Court in *U.S. v. Jones*, 132 S. Ct. 945, 949 (2012), which held that the installation of a GPS on a suspect's vehicle, and use of that device to monitor the vehicle's movements, constitutes a "search" under the Fourth Amendment. A search warrant is not required where the consent of the vehicle owner/operator is obtained, and where the device is placed on a DHS OIG government vehicle to protect the agent and those working with DHS OIG. Other unique circumstances should be discussed with the relevant USAO. Other specific procedures are as follows:

1. Use of an MTD requires appropriate legal and managerial approvals. The case agent must discuss the use of MTDs with the ASAC as well as with an AUSA or other assigned local prosecutor. The case agent is responsible for complying with all legal requirements deemed necessary by the assigned prosecutor (i.e., search warrant affidavits and an installation plan, etc.). Once approval is obtained from the relevant USAO, the case agent will submit a written request for approval to the SAC, including the following information:

    a. Case identification

    b. Subject identification.

    c. Information on the vehicle to be tracked, including make/model and license plate numbers.

    d. Method and duration of the tracking.

    e. Method and location where the installation will occur.

    f. Investigative goals of the tracking.

    g. Date and person approving from the USAO.

2. The approving SAC will submit a copy of the written request to the DAIGI FOD with a copy to the SAC DFAU, and maintain the original in the case file. Once the approval is received, the EISPM will coordinate the delivery of the equipment to the local TEC.

3. Preserve all tapes, computer disks or other electronic data produced by the GPS mapping software or other collected data as evidence. Maintain appropriate surveillance logs in the case file.

D. *MTD Authorizations for Consensual Use*: In cases where the property owner has given permission for the installation of an MTD, SAs will:

1. Follow all the requirements for requesting the MTD as noted above in Section 15.18 (B) above;

2. Consult with the appropriate AUSA or other assigned prosecutor prior to installing a tracking device on a Government Owned Vehicle (GOV) since in certain circumstances a search warrant may be required;

3. Document the owner's consent in writing, using INV Form 72 **(Exhibit 15-2 and 15-2S Spanish Version)**, and ensure that the consenting party is lawfully authorized to give consent. Documentation must be included in the case file;

4. When conducting undercover activities using a vehicle, consider using a tracking device on undercover vehicles for safety and protection. This is considered a consensual use of an MTD and requires no court order.

E. *Storage and Inventory Requirements*: TECs will ensure that MTDs are maintained with other technical investigative equipment and stored in a safe, cabinet, closet, or secured room and that the MTD equipment is inventoried using established inventory procedures.

15.19 USE OF ELECTRONIC SURVEILLANCE TECHNIQUES IN JOINT INVESTIGATIONS

A. *Domestic*:

1. The use of electronic surveillance equipment in any investigation controlled by the DHS OIG will be done in full accord with the requirements of this chapter, regardless of the agency affiliation of involved personnel.

2. The applicability of DHS OIG requirements to an investigation not controlled by DHS OIG will depend on the circumstances. [redacted] these requirements shall apply. If a case is ultimately prosecuted in federal court, the admissibility of evidence gained through the use of this equipment will be measured against compliance with federal law. If federal prosecution is anticipated, at the time the equipment is used, all requirements of this chapter will apply.

B. *Foreign*: Any electronic surveillance activities in a foreign country can have serious diplomatic consequences. "Foreign Investigations," must be reviewed and approval

obtained from the AIGI before any contact is made with foreign entities concerning using electronic surveillance operations.

15.20 AIRCRAFT TRANSPONDERS

A. Use of a transponder, a special type of transmitter used for tracking aircraft, requires very close coordination with the Federal Aviation Administration (FAA). All coordination between FAA and the DHS OIG will be handled by a DAIGI.

B. With as much lead time as possible, the SAC must notify their DAIGI by memorandum with the following items of information:

1. case title and file number;

2. name of case agent (and alternate); office, home, and cellular telephone numbers;

3. type, color, and identification number of aircraft;

4. name of the owner and/or operator (if known);

5. present location of aircraft and the approximate areas of travel;

6. whether the transponder will be installed on a consensual basis or under a court order; and

7. approximate date of installation and length of time to remain in operation.

C. In exigent circumstances, this notification may be via telephone, followed by a memorandum.

D. Immediately upon installing the transponder and before the aircraft becomes airborne, it is important that El Paso Intelligence Center (EPIC) be notified via telephone that the transponder is operational if operating along the southwest border.

E. The FAA will notify EPIC of all flight activity of the aircraft. EPIC will in turn notify the case agent of all FAA contacts.

F. EPIC must be notified immediately of termination, disablement, or removal of the transponder if operating along the southwest border.

15.21 AIRCRAFT LOOKOUTS

A. *Requests for Federal Aviation Administration (FAA) Aircraft Lookouts*: At the request of the DHS OIG, the FAA will place a lookout for aircraft of interest to the DHS OIG. To place an FAA lookout, the DAIGI should be contacted. Lookouts may be requested for a period of time not exceeding 7 days; however, they may be extended by calling the

DAIGI. If the need for a lookout ceases before its cancellation date, EPIC should be notified immediately.

B. *Requests for DHS Aircraft Lookouts*: The Air and Marine Operations Center (AMOC), a facility within U.S. Customs and Border Protection (CBP), Office of Air and Marine (OAM) is an international multi-domain federal law enforcement center located in Riverside, California. The AMOC is a state-of-the-art law enforcement operations and domain awareness center, which focuses on suspicious general aviation and non-commercial maritime activities in the Western Hemisphere. The AMOC conducts air and marine surveillance operations, providing direct coordination and support to OAM; CBP law enforcement officers performing interdiction missions; and other federal, state and local law enforcement agencies conducting criminal investigations. AMOC coordinates operations with the North American Aerospace Defense Command, and the governments of Mexico, Canada and the Bahamas. The AMOC maintains integrated data from hundreds of additional domestic and international radar, optical and acoustical sensors to provide surveillance of critical national infrastructure throughout the United States and to support disaster response. A SAC may contact the Director of the AMOC, Riverside, CA, to request tracking services for aircraft and vessels as appropriate during investigations.

CHAPTER 15 - EXHIBITS

15-1 INV Form 71, Authorization and Report of Consensual Intercept

15-2 INV Form 72, Consent to Intercept, Monitor and Record Communications.

15-2S INV Form 72S, Consent to Intercept, Monitor and Record Communications – Spanish.

15-3 Attorney General Procedures for Lawful, Warrantless Interceptions of Verbal Communications, dated May 30, 2002.

15-4 INV Form 74, Authorization to Use BOP Prisoner or Employee

15-5 INV Form 65, Cooperating Individual Agreement for Persons in Custody

Exhibit 15-1, INV Form 71, Report of Consensual Intercept

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

AUTHORIZATION & REPORT OF CONSENSUAL INTERCEPT

Case Number:
Case Title:
Case Agent: Planned Date of Intercept:

AUTHORIZATION FOR CONSENSUAL INTERCEPT

Type of Consensual Intercept
☐ Telephonic ☐ Non Telephonic
☐ Consensual ☐ Non-Consensual

Are the consenting or non-consenting persons in custody? ☐Yes ☐No

Are any sensitive circumstances as identified in the DOJ Attorney General Guidelines, specified in SAH Section 15.10 present? ☐Yes ☐No [If "No", all boxes below should be checked]

☐ Does not relate to an investigation of a member of Congress, a Federal judge, a member of the Executive Branch at Executive Level IV or above, or a person who has served in such capacity within the previous two years.
☐ Does not relate to an investigation of the Governor, Lt. Governor, or Attorney General of any State, or Territory, or a Judge or Justice of the highest court of any State or Territory, and the offense investigated is one involving bribery, conflict of interest, or extortion relating to the performance of his official duties.
☐ No party to the communication is or has been a member of the Witness Security Program and that fact is known to the agency involved or its officers.
☐ No party to the communication is or has been a member of the Witness Security Program and that fact is known to the agency involved or its officers.
☐ The consenting or non-consenting person is **not** in the custody of the Bureau of Prisons (BOP) or in the custody of the U.S. Marshals Service.

Summary of Investigation and Allegations/Violations:

Investigative benefits expected from intercept:

☐ AUSA Advice Obtained AUSA: _____ Date: _____

☐ Approved _____ ☐ Disapproved _____
SAC Signature/Date SAC Signature/Date

INV Form 71

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

REPORT OF CONSENSUAL INTERCEPT

Date of Intercept:

Type of Equipment Used:

Description & Property # of Equipment Used:

Installation Method:

Recording Made: ☐ Yes ☐ No

Duration of Intercept: _____

Location Where Equipment Was Used: _____
(Street, City, State)

Telephone # Called:

Telephone # From Which Call Was Placed:

Consenting Party:

Name(s) of Individual(s) Intercepted:

Special Agents involved:

Investigative Benefits Derived:

☐ Reviewed _____
SAC (or designee)

INV Form 71

Exhibit 15-2, INV Form 72, Consent to Intercept, Monitor and Record Communications

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

CONSENT TO INTERCEPT, MONITOR AND RECORD COMMUNICATIONS

I, _____, hereby give Special
(Name)

Agent(s)_____ of the Department of

Homeland Security, Office of Inspector General, my consent to intercept, monitor, and record

Non-Telephone, Telephone or video communications to which I am a party

on _____.
(Date or Dates)

I have given this consent freely and voluntarily without threats or promises of any kind.

Signature: _____

Date: _____

Witness: _____

Witness: _____

INV FORM 72

Exhibit 15-2S, INV Form 72S, Consent to Intercept, Monitor and Record Communications – Spanish

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

CONSENTIMIENTO PARA INTERCEPTAR, MONITORIAR Y GRAVAR COMMUNICACCIONES

Yo, _____ le doy al Agente Especial(s)
(Nombre)

_____ del Departamento de Seguridad de la

Patria, Oficina de Inspector General, mi consentimiento para interceptor, monitoriar, y

graver communicaciones no-telefonicas, telefonicas, y de video donde yo soy parte de en

_____.
(fecha o fechas)

Yo he dado consentimiento libre y volunrariamente sin amenazas o promesas de cualquier modo.

Firma: _____

Fecha: _____

Testigo: _____

Testigo: _____

INV FORM 72S

Exhibit 15-3, Procedures for Lawful, Warrantless Interceptions of Verbal Communications

Office of the Attorney General
Washington, D.C. 20530

May 30, 2002

MEMORANDUM FOR THE HEADS AND INSPECTORS GENERAL
OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM THE ATTORNEY GENERAL

SUBJECT: Procedures for Lawful, Warrantless Monitoring of Verbal Communications

By Memorandum dated October 16, 1972, the Attorney General directed all federal departments and agencies to obtain Department of Justice authorization before intercepting verbal communications without the consent of all parties to the communication. This directive was clarified and continued in force by the Attorney General's Memorandum of September 22, 1980, to Heads and Inspectors General of Executive Departments and Agencies. It was then superseded, with new authorization procedures and relevant rules and guidelines, including limitations on the types of investigations requiring prior written approval by the Department of Justice, in the Attorney General's Memorandum of November 7, 1983.[1]

The Attorney General's Memorandum of January 20, 1998, superseded the aforementioned directives. It continued most of the authorization procedures established in the November 7, 1983, Memorandum, but reduced the sensitive circumstances under which prior written approval of senior officials of the Department of Justice's Criminal Division is required. At the same time, it continued to require oral authorization from Department of Justice attorneys, ordinarily local Assistant United States Attorneys, before the initiation of the use of consensual monitoring in all investigations not requiring prior written approval. In addition, that Memorandum reduced and eventually eliminated the reporting requirement imposed on departments and agencies. These changes reflected the results of the exercise of the Department's review function over many years, which showed that the departments and agencies had uniformly been applying the required procedures with great care, consistency, and good judgment, and that the number of requests for consensual monitoring that were not approved had been negligible.

---

[1]As in all of the prior memoranda except for the one dated October 16, 1972, this memorandum only applies to the consensual monitoring of oral, nonwire communications, as discussed below. "Verbal" communications will hereinafter be referred to as oral.

This Memorandum updates and in some limited respects modifies the Memorandum of January 20, 1998. The changes are as follows:

First, Parts III.A.(8) and V. of the January 20, 1998, Memorandum required concurrence or authorization for consensual monitoring by the United States Attorney, an Assistant United States Attorney, or the previously designated Department of Justice attorney responsible for a particular investigation (for short, a "trial attorney"). This Memorandum provides instead that a trial attorney must advise that the monitoring is legal and appropriate. This continues to limit monitoring to cases in which an appropriate attorney agrees to the monitoring, but makes it clear that this function does not establish a supervisory role or require any involvement by the attorney in the conduct of the monitoring. In addition, for cases in which this advice cannot be obtained from a trial attorney for reasons unrelated to the legality or propriety of the monitoring, this Memorandum provides a fallback procedure to obtain the required advice from a designated attorney of the Criminal Division of the Department of Justice. Where there is an issue as to whether providing the advice would be consistent with applicable attorney conduct rules, the trial attorney or the designated Criminal Division attorney should consult with the Department's Professional Responsibility Advisory Office.

Second, Part V. of the Memorandum of January 20, 1998, required that an agency head or his or her designee give oral authorization for consensual monitoring, and stated that "[a]ny designee should be a high-ranking supervisory official at headquarters level." This rule was qualified by Attorney General Order No. 1623-92 of August 31, 1992, which, in relation to the Federal Bureau of Investigation (FBI), authorized delegation of this approval function to Special Agents in Charge. Experience has shown that the requirement of Special Agent in Charge approval can result in a loss of investigative opportunities because of an overly long approval process, and indicates that allowing approval by Assistant Special Agents in Charge would facilitate FBI investigative operations. Assistant Special Agents in Charge are management personnel to whom a variety of supervisory and oversight responsibilities are routinely given; generally, they are directly involved and familiar with the circumstances relating to the propriety of proposed uses of the consensual monitoring technique. Part V. is accordingly revised in this Memorandum to provide that the FBI Director's designees for purposes of oral authorization of consensual monitoring may include both Special Agents in Charge and Assistant Special Agents in Charge. This supersedes Attorney General Order No. 1623-92, which did not allow delegation of this function below the level of Special Agent in Charge.

Third, this Memorandum omits as obsolete Part VI. of the Memorandum of January 20, 1998. Part VI. imposed a reporting requirement by agencies concerning consensual monitoring but rescinded that reporting requirement after one year.

The Fourth Amendment to the United States Constitution, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended (18 U.S.C. §2510, et seq.), and the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. §1801, et seq.) permit government agents,

acting with the consent of a party to a communication, to engage in warrantless monitoring of wire (telephone) communications and oral, nonwire communications. See United States v. White, 401 U.S. 745 (1971); United States v. Caceres, 440 U.S. 741 (1979). Similarly, the Constitution and federal statutes permit federal agents to engage in warrantless monitoring of oral, nonwire communications when the communicating parties have no justifiable expectation of privacy.[2] Because such monitoring techniques are particularly effective and reliable, the Department of Justice encourages their use by federal agents for the purpose of gathering evidence of violations of federal law, protecting informants or undercover law enforcement agents, or fulfilling other, similarly compelling needs. While these techniques are lawful and helpful, their use in investigations is frequently sensitive, so they must remain the subject of careful, self-regulation by the agencies employing them.

The sources of authority for this Memorandum are Executive Order No. 11396 ("Providing for the Coordination by the Attorney General of Federal Law Enforcement and Crime Prevention Programs"); Presidential Memorandum ("Federal Law Enforcement Coordination, Policy and Priorities") of September 11, 1979; Presidential Memorandum (untitled) of June 30, 1965, on, inter alia, the utilization of mechanical or electronic devices to overhear nontelephone conversations; the Paperwork Reduction Act of 1980 and the Paperwork Reduction Reauthorization Act of 1986, as amended; and the inherent authority of the Attorney General as the chief law enforcement officer of the United States.

I. DEFINITIONS

As used in this Memorandum, the term "agency" means all of the Executive Branch departments and agencies, and specifically includes United States Attorneys' Offices which utilize their own investigators, and the Offices of the Inspectors General.

As used in this Memorandum, the terms "interception" and "monitoring" mean the aural acquisition of oral communications by use of an electronic, mechanical, or other device. Cf. 18 U.S.C. § 2510(4).

As used in this Memorandum, the term "public official" means an official of any public entity of government, including special districts, as well as all federal, state, county, and municipal governmental units.

---

[2]As a general rule, nonconsensual interceptions of wire communications violate 18 U.S.C. § 2511 regardless of the communicating parties' expectation of privacy, unless the interceptor complies with the court-authorization procedures of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C. § 2510, et seq.) or with the provisions of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801 et seq.).

II. NEED FOR WRITTEN AUTHORIZATION

A. Investigations Where Written Department of Justice Approval is Required

A request for authorization to monitor an oral communication without the consent of all parties to the communication must be approved in writing by the Director or Associate Director of the Office of Enforcement Operations, Criminal Division, U.S. Department of Justice, when it is known that:

(1) the monitoring relates to an investigation of a member of Congress, a federal judge, a member of the Executive Branch at Executive Level IV or above, or a person who has served in such capacity within the previous two years;

(2) the monitoring relates to an investigation of the Governor, Lieutenant Governor, or Attorney General of any State or Territory, or a judge or justice of the highest court of any State or Territory, and the offense investigated is one involving bribery, conflict of interest, or extortion relating to the performance of his or her official duties;

(3) any party to the communication is a member of the diplomatic corps of a foreign country;

(4) any party to the communication is or has been a member of the Witness Security Program and that fact is known to the agency involved or its officers;

(5) the consenting or nonconsenting person is in the custody of the Bureau of Prisons or the United States Marshals Service; or

(6) the Attorney General, Deputy Attorney General, Associate Attorney General, any Assistant Attorney General, or the United States Attorney in the district where an investigation is being conducted has requested the investigating agency to obtain prior written consent before conducting consensual monitoring in a specific investigation.

In all other cases, approval of consensual monitoring will be in accordance with the procedures set forth in part V. below.

B. Monitoring Not Within Scope of Memorandum

Even if the interception falls within one of the six categories above, the procedures and rules in this Memorandum do not apply to:

(1) extraterritorial interceptions;

(2) foreign intelligence interceptions, including interceptions pursuant to the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801, et seq.);

(3) interceptions pursuant to the court-authorization procedures of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended (18 U.S.C. § 2510, et seq.);

(4) routine Bureau of Prisons monitoring of oral communications that are not attended by a justifiable expectation of privacy;

(5) interceptions of radio communications; and

(6) interceptions of telephone communications.

III. AUTHORIZATION PROCEDURES AND RULES

A. Required Information

The following information must be set forth in any request to monitor an oral communication pursuant to part II.A.:

(1) Reasons for the Monitoring. The request must contain a reasonably detailed statement of the background and need for the monitoring.

(2) Offense. If the monitoring is for investigative purposes, the request must include a citation to the principal criminal statute involved.

(3) Danger. If the monitoring is intended to provide protection to the consenting party, the request must explain the nature of the danger to the consenting party.

(4) Location of Devices. The request must state where the monitoring device will be hidden: on the person, in personal effects, or in a fixed location.

(5) Location of Monitoring. The request must specify the location and primary judicial district where the monitoring will take place. A monitoring authorization is not restricted to the original district. However, if the location of monitoring changes, notice should be promptly given to the approving official. The record maintained on the request should reflect the location change.

(6) Time. The request must state the length of time needed for the monitoring. Initially, an authorization may be granted for up to 90 days from the day the monitoring is scheduled to begin. If there is the need for continued monitoring, extensions for additional periods of up to 90 days may be granted. In special cases (e.g., "fencing" operations run by law enforcement agents or long-term investigations that are closely supervised by the Department's Criminal Division) authorization for up to 180 days may be granted with similar extensions.

(7) Names. The request must give the names of persons, if known, whose communications the department or agency expects to monitor and the relation of such persons to the matter under investigation or to the need for the monitoring.

(8) Attorney Advice. The request must state that the facts of the surveillance have been discussed with the United States Attorney, an Assistant United States Attorney, or the previously designated Department of Justice attorney responsible for a particular investigation, and that such attorney advises that the use of consensual monitoring is appropriate under this Memorandum (including the date of such advice). The attorney must also advise that the use of consensual monitoring under the facts of the investigation does not raise the issue of entrapment. Such statements may be made orally. If the attorneys described above cannot provide the advice for reasons unrelated to the legality or propriety of the consensual monitoring, the advice must be sought and obtained from an attorney of the Criminal Division of the Department of Justice designated by the Assistant Attorney General in charge of that Division. Before providing such advice, a designated Criminal Division Attorney shall notify the appropriate United States Attorney or other attorney who would otherwise be authorized to provide the required advice under this paragraph.

(9) Renewals. A request for renewal authority to monitor oral communications must contain all the information required for an initial request. The renewal request must also refer to all previous authorizations and explain why an additional authorization is needed, as well as provide

an updated statement that the attorney advice required under paragraph (8) has been obtained in connection with the proposed renewal.

B. Oral Requests

Unless a request is of an emergency nature, it must be in written form and contain all of the information set forth above. Emergency requests in cases in which written Department of Justice approval is required may be made by telephone to the Director or an Associate Director of the Criminal Division's Office of Enforcement Operations, or to the Assistant Attorney General, the Acting Assistant Attorney General, or a Deputy Assistant Attorney General for the Criminal Division, and should later be reduced to writing and submitted to the appropriate headquarters official as soon as practicable after authorization has been obtained. An appropriate headquarters filing system is to be maintained for consensual monitoring requests that have been received and approved in this manner. Oral requests must include all the information required for written requests as set forth above.

C. Authorization

Authority to engage in consensual monitoring in situations set forth in part II.A. of this Memorandum may be given by the Attorney General, the Deputy Attorney General, the Associate Attorney General, the Assistant Attorney General or Acting Assistant Attorney General in charge of the Criminal Division, a Deputy Assistant Attorney General in the Criminal Division, or the Director or an Associate Director of the Criminal Division's Office of Enforcement Operations. Requests for authorization will normally be submitted by the headquarters of the department or agency requesting the consensual monitoring to the Office of Enforcement Operations for review.

D. Emergency Monitoring

If an emergency situation requires consensual monitoring at a time when one of the individuals identified in part III.B. above cannot be reached, the authorization may be given by the head of the responsible department or agency, or his or her designee. Such department or agency must then notify the Office of Enforcement Operations as soon as practicable after the emergency monitoring is authorized, but not later than three working days after the emergency authorization.

The notification shall explain the emergency and shall contain all other items required for a nonemergency request for authorization set forth in part III.A. above.

IV. SPECIAL LIMITATIONS

When a communicating party consents to the monitoring of his or her oral communications, the monitoring device may be concealed on his or her person, in personal effects, or in a fixed location. Each department and agency engaging in such consensual monitoring must ensure that the consenting party will be present at all times when the device is operating. In addition, each department and agency must ensure: (1) that no agent or person cooperating with the department or agency trespasses while installing a device in a fixed location, unless that agent or person is acting pursuant to a court order that authorizes the entry and/or trespass, and (2) that as long as the device is installed in the fixed location, the premises remain under the control of the government or of the consenting party. See United States v. Yonn, 702 F.2d 1341, 1347 (11th Cir.), cert. denied, 464 U.S. 917 (1983) (rejecting the First Circuit's holding in United States v. Padilla, 520 F.2d 526 (1st Cir. 1975), and approving use of fixed monitoring devices that are activated only when the consenting party is present). But see United States v. Shabazz, 883 F. Supp. 422 (D. Minn. 1995).

Outside the scope of this Memorandum are interceptions of oral, nonwire communications when no party to the communication has consented. To be lawful, such interceptions generally may take place only when no party to the communication has a justifiable expectation of privacy,[3] or when authorization to intercept such communications has been obtained pursuant to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C. § 2510, et seq.) or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801 et seq.). Each department or agency must ensure that no communication of any party who has a justifiable expectation of privacy is intercepted unless proper authorization has been obtained.

V. PROCEDURES FOR CONSENSUAL MONITORING WHERE NO WRITTEN APPROVAL IS REQUIRED

Prior to receiving approval for consensual monitoring from the head of the department or agency or his or her designee, a representative of the department or agency must obtain advice that the consensual monitoring is both legal and appropriate from the United States Attorney, an Assistant United States Attorney, or the Department of Justice attorney responsible for a particular investigation. The advice may be obtained orally from the attorney. If the attorneys described above cannot provide this advice for reasons unrelated to the legality or propriety of the consensual monitoring, the advice must be

---

[3]For example, burglars, while committing a burglary, have no justifiable expectation of privacy. Cf. United States v. Pui Kan Lam, 483 F.2d 1202 (2d. Cir. 1973), cert. denied, 415 U.S. 984 (1974).

sought and obtained from an attorney of the Criminal Division of the Department of Justice designated by the Assistant Attorney General in charge of that Division. Before providing such advice, a designated Criminal Division Attorney shall notify the appropriate United States Attorney or other attorney who would otherwise be authorized to provide the required advice under this paragraph.

Even in cases in which no written authorization is required because they do not involve the sensitive circumstances discussed above, each agency must continue to maintain internal procedures for supervising, monitoring, and approving all consensual monitoring of oral communications. Approval for consensual monitoring must come from the head of the agency or his or her designee. Any designee should be a high-ranking supervisory official at headquarters level, but in the case of the FBI may be a Special Agent in Charge or Assistant Special Agent in Charge.

Similarly, each department or agency shall establish procedures for emergency authorizations in cases involving non-sensitive circumstances similar to those that apply with regard to cases that involve the sensitive circumstances described in part III.D., including obtaining follow-up oral advice of an appropriate attorney as set forth above concerning the legality and propriety of the consensual monitoring.

Records are to be maintained by the involved departments or agencies for each consensual monitoring that they have conducted. These records are to include the information set forth in part III.A. above.

VI. GENERAL LIMITATIONS

This Memorandum relates solely to the subject of consensual monitoring of oral communications except where otherwise indicated. This Memorandum does not alter or supersede any current policies or directives relating to the subject of obtaining necessary approval for engaging in nonconsensual electronic surveillance or any other form of nonconsensual interception.

Exhibit 15-4, INV Form 74, Authorization to Use BOP Prisoner or Employee

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

AUTHORIZATION TO USE BOP PRISONER OR EMPLOYEE

DATE PREPARED	CASE NUMBER	REQUEST NUMBER *(Original, 1st, 2nd, 3rd submission)*
PREPARED BY	TITLE OF PREPARER *(SA, ISA, etc.)*	APPROVING SUPERVISOR

ALSO INCLUDE THE APPROPRIATE FORM OR MEMO IF ELECTRONIC SURVEILLANCE IS USED

TYPE OF AUTHORIZATION REQUEST:	☐ BOP Prisoner ☐ USMS Prisoner ☐ BOP Employee
1. FEDERAL PRISONER/BOP EMPLOYEE INFORMATION *a. Full Name and Job Title*	*b. Identifying Data (DOB, SSN, and BOP #, if applicable)*
c. Charge(s) and Sentence	*d. Date of Scheduled Release*
2. DURATION OF PROPOSED USE *(Dates. Not to exceed 90 days)*	3. LOCATION WHERE FEDERAL PRISONER/BOP EMPLOYEE WILL BE USED *(Include Title and Address)*
4. ANTICIPATED TARGET(S)	5. ASSOCIATION WITH ANTICIPATED TARGET(S)
6. BOP OR USMS PERSONNEL PERSONALLY BRIEFED BY THE CASE AGENT AND IN AGREEMENT WITH PLAN *(Include names, Titles, Phone #, and Locations)*	

7. NAME OF CONCURRING PROSECUTOR	8. JUDICIAL DISTRICT	9. TELEPHONE NUMBER

10. LEGAL ISSUES DISCUSSED WITH PROSECUTOR BY DATE					11. REQUIREMENTS AFTER USE *(Check all that apply)*	
Violation Code(s)		Entrapment (Date)			☐ Witness Security	☐ Need As Witness
McDade 28 USC 530B (Date)		Concurrence of Private Attorney (Issues Asked)		☐ Yes ☐ Has None	☐ Prison Reassignment and/or Job Transfer	

12. JUSTIFICATION *(Allegation, Reliability, Operational Plan, Safety Issues, Motive for Cooperation, and Other Concerns* Continue on separate sheet)

See Continuation Page

13. RESULT OF USE
(Concise narrative - Must be returned to HQ when use of prisoner or employee is complete and electronic surveillance is NOT involved)

OIG INV FORM 74

Exhibit 15-5, INV Form 65, Cooperating Individual Agreement for Persons in Custody

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Cooperating Individual Agreement for Persons in Custody

I, _____ by my signature below, indicate that I have read (or had read to me), understand, and agree to the following statements:

1. I voluntarily, and without threats or promises of any kind, agree to assist the U.S. Department of Homeland Security (DHS) Office of the Inspector General (OIG) in an ongoing investigation of criminal and/or administrative misconduct. My assistance may include the provision of information to the OIG as well as assistance in gathering evidence, including my possible participation in undercover operations. I understand that if I am requested and agree to participate in recorded telephone conversations to have my conversations and/or movements videotaped or agree to wear a monitoring/transmitter device on my person, I will be asked to sign an additional consent form. I understand that I may withdraw my agreement to provide assistance to the OIG at any time and that I will not be penalized for doing so.

2. I have been advised that although the OIG will make all reasonable efforts to prevent the fact of my cooperation from becoming known to the subject(s) of the investigation, other inmates, or other U.S. Government employees not involved in the investigation, this cannot be guaranteed. I understand that to help maintain confidentiality, I should not discuss the investigation or my role in it with anyone not involved in the investigation.

3. I understand that I may be called to testify in a court of law regarding any information or services I may provide to the OIG.

4. I have also been advised that it is a federal offense to threaten, harass, or mislead anyone who provides information about a federal crime to a federal law enforcement agency such as the OIG. I understand that there is a possibility that I may experience such conduct as a result of my cooperation with the OIG. If this occurs, I will contact one of the undersigned OIG agents immediately. I also understand that if I experience such conduct, it is possible that for my protection, I may be transferred to a more secure section of the institution or to another federal institution.

5. I will not violate criminal laws in furtherance of gathering information or providing services to the OIG. I understand that any evidence of such a violation will be reported by the OIG to the appropriate law enforcement agency.

6. I understand that I have no official status, implied or otherwise, as an agent or employee of the OIG.

WITNESSED BY:

_____
(Signature, Date and Title)

_____
(Signature, Date, and Title)

_____
(Agent's Signature, Date, and Title)

OIG INV Form 65

16.0 ACQUISITION, PRESERVATION, AND MANAGEMENT OF EVIDENCE

16.1 EVIDENCE GENERAL

Evidence is the means by which any alleged action is proved or disproved.

SAs should develop an understanding of the "Federal Rules of Evidence" (FRE) and the "Federal Rules of Criminal Procedure." Both sets of rules may be found in West Publishing Company's Federal Criminal Code and Rules. Questions regarding the admissibility of evidence should be discussed with the prosecuting attorney.

16.2 TYPES OF EVIDENCE

Evidence may be classified as direct or circumstantial. Evidence may also be classified as oral, physical, and documentary.

Oral testimony consists of statements made by witnesses under oath or affirmation.

Physical evidence may be defined as any article or material found during an investigation that may assist in the solution of the case. It relates to tangible objects or property that are admitted in court or inspected by a trier of facts.

Documentary evidence consists of writings such as judicial and official records, contracts, deeds, and less formal writings such as letters, memoranda, and books and records of private persons and organizations.

16.3 BEST EVIDENCE RULE

The "Best Evidence Rule" (Rule 1002) requires original documents except as otherwise provided in the FRE. Rule 1003 provides that a duplicate is admissible to the same extent as an original unless a question is raised as to the authenticity of the original, or in circumstances where it would be unfair to admit the duplicate in lieu of the original.

The "Admissibility of Other Evidence of Contents," (Rule 1004) provides that other evidence of the contents of a writing, recording, or photograph is admissible if:

> All originals are lost or have been destroyed (unless the proponent lost or destroyed them in bad faith): or
>
> No original can be obtained by judicial process; or

The original is under the control of the party against whom evidence would be offered, and who, after being notified that the contents would be a subject of proof, does not produce the original; or

The writing, recording, or photograph is not closely related to a controlling issue.

16.4 EVIDENCE OBTAINED THROUGH THE GRAND JURY

Rule 6(e) of the "Federal Rules of Criminal Procedure" imposes strict obligations upon SAs who are duly appointed agents of the grand jury to protect the secrecy of matters occurring before the grand jury. Grand jury material should be handled in such a manner that it does not become misplaced or available to unauthorized personnel. Access must be strictly on a need-to-know basis. Materials obtained through the Grand Jury and entered into evidence should be secured as all other evidence. (Chapter 17.1)

16.5 OBTAINING AND SECURING EVIDENCE AND/OR PERSONAL PROPERTY

SAs will document receipt of evidence or personal property and chain of custody on an INV Form 30/30A, "Evidence/Personal Property Inventory Form." **(Exhibits 16-1 and 16-2).** Each INV Form 30 will contain a serial number composed of the numeric characters from the case number and a sequential number for the specific INV Form 30, i.e. 08-12345-001, 002, etc. An SA may use the INV Form 30A "Evidence/Personal Property Inventory Continuation Form."

Evidence and personal property should be inventoried on separate INV Form 30 upon receipt.

Completion of INV Form 30

INV Form 30 will be signed by the SA completing the form and the reviewing supervisor.

Column 1 – Item Number: Each inventoried item will be numbered.

Column 2 – Date Received: The date the item was received or seized.

Column 3 – Quantity: Total number of the items to be described.

Column 4 - Description of Evidence: Brief description of the item, including any identifying make, model, and/or number.

Column 5 – Value: Approximate dollar value of the item being inventoried, if unknown or item has no value use N/V. Total value for all items inventoried should be entered at the bottom of this column.

After the final item on INV Form 30/30A is listed, the SA completing the inventory will conclude the form with the following in order to identify the agent who obtained the evidence/property and where or from whom it was obtained:

"Item(s) _____(e.g. 1 – 4) were seized/received by SA_____ (name) from _____(location/source) and are marked for identification _____(initials and date)."

Each change in the custody of the evidence will be documented in the chain of custody portion on the reverse of the original and Copy No.1 of the INV Form 30.

Distribution of INV Form 30

The original INV Form 30 will remain with the evidence at all times along with the chain of custody which will be documented on the reverse.

Copy No. 1 will be maintained by the Evidence Custodian and the chain of custody will also be documented on the reverse. The Evidence Custodian will maintain this copy in an Evidence Log Book (a three ring binder) in the evidence vault.

Copy No. 2 will be maintained in the office case file.

Copy No. 3 will be maintained by the case agent.

Handling Evidence

When large quantities of cash are seized, the monies should be counted and individually verified by two SAs as soon as possible. The monies should be re-counted by the evidence custodian and at least one witness for verification prior to being placed in the evidence vault.

Whenever possible, two SAs should transport large quantities of controlled substances and/or large quantities of cash.

SAs should mark any evidence received with their initials and date, in a manner that does not alter the value or integrity of the seized item. When dealing with large quantities of documents, it may be acceptable to initial and date the first and last document.

SAs should consider "Bates Stamping" (a sequential numbering stamp) large quantities of documents gathered by search warrant or subpoena. Stamping in red allows for later identification of the original document obtained.

Evidence tags and labels are available to mark and identify evidence as needed.

The evidence will be placed in a plain envelope, evidence bag, or other sealable container applicable to the size and construction of the item(s). The container will be identified as evidence with the original Evidence Inventory Form attached on the outside.
If the evidence container must be opened for any reason, a new evidence container will be used. The old evidence container will be saved inside the new container to preserve the "Chain of Custody."

16.6 EVIDENCE CUSTODIAN

SACs will designate an evidence custodian and alternates for each investigative office. The evidence custodian will assure that case SAs properly enter, maintain, transfer, document, and dispose of evidence. The evidence custodian will maintain in a log book in order to control and track evidence.

The evidence custodian will assign a sequential serial number, as previously described, to each INV Form 30 affiliated with a specific case. The custodian will maintain a record of these numbers in the "Evidence Log," INV Form 31. **(Exhibit 16-3)** Only evidence custodian and alternates will make entries in the evidence log. A separate evidence log will be maintained for each case.

16.7 EVIDENCE STORAGE

All evidence will be maintained in a designated, secure storage area. Safes, lockers, cabinets, and/or rooms should be of such weight, size, construction, or installation so as to minimize the possibility of unauthorized access to or theft of evidence. The evidence storage area will be secured by a locking device. Cash and narcotics should be stored in a safe whenever possible. Access will be limited to the SAC, evidence custodian(s), alternate(s) and other personnel as designated by the SAC.

16.8 TRANSFER OF EVIDENCE

Evidence transferred from the control of an INV office to any other authorized recipient will be hand-carried or sent by registered mail return receipt. All transfers of evidence will be documented utilizing the "Chain of Custody" portion of the original and Copy No. 1 of the INV Form 30. If mailed, the registered mail and the return receipt will be affixed to Copy No. 1 of the INV Form 30 to document the transfer.

16.9 ANNUAL EVIDENCE VERIFICATION

Each office will conduct an annual verification of inventoried evidence. This verification must be completed in January of each year. The verification will be documented by a Memorandum from the Evidence Custodian to the SAC that will be filed in the Evidence Log Book and the office administrative file (5600).

In addition, the SAC will be responsible for conducting a complete inventory of evidence when there is a personnel change in the evidence custodian.

16.10 DISPOSITION OF EVIDENCE AND PERSONAL PROPERTY

Instructions for return, destruction, or other disposition of evidence will be sought from the AUSA, when applicable. In cases where no prosecution is accepted disposition of evidence may be authorized by the field office SAC.

The final disposition of the evidence will be documented in the chain of custody section of the INV Form 30 and will include the date and manner/method of disposition/destruction. The SA and one witness will sign this entry. Any receipts obtained for the return of evidence or personal property will be maintained with the original INV Form 30, which will be made a part of the case file. All other copies of the INV Form 30 should be destroyed.

28 U.S.C. § 2042 and 18 U.S.C. § 3612 provide that monies received or tendered as evidence in any United States court should be disposed of by the court. The case agent should ensure that the prosecuting AUSA prepares a motion requesting disposition of any monies as part of sentencing.

Monies seized during the course of an investigation will only be retained as evidence at the request of the USAO. Seized monies no longer needed as evidence should be converted to a certified bank check made payable to the "Department of Homeland Security" and forwarded to the SAC of Operations and Planning via memorandum. The memorandum will include the following information: 1) the case number; 2) a brief description of the circumstances surrounding the seizure, 3) the USAO authorized disposition of evidence in the case, 4) the fiscal year of the seizure, and 5) whether the seizure is from INV Confidential Funds. A copy of the bank check and memorandum will be attached to the INV Form 30.

Monies determined not to be forfeitable evidence will be returned to the rightful owner. A receipt will be obtained and will be maintained with the original INV Form 30, which will be made a part of the case file.

Paper and documents may be disposed of when all avenues of appeal have been exhausted. Original documents should be returned to the source. Original affidavits, forensic reports, schedules, and similar materials should be retained in the permanent case file.

Weapons must be destroyed or, when applicable, returned to the owner. Offices are not authorized to keep confiscated weapons after the conclusion of the investigation.

Controlled Substances will be disposed of through the Drug Enforcement Agency or through state or local law enforcement. Minimal amounts of controlled substances can be disposed of locally at the SAC's discretion.

Personal property should be returned to the proper owner unless otherwise directed by the USAO. Personal property subject to claims of ownership or other rights shall be disposed of as directed by the USAO.

In cases where the owner of personal property is unknown, the item will be declared lost, abandoned, or unclaimed property. Disposition will be decided by the SAC in accordance with abandoned property procedures outlined in Section 16.11.

In cases where the owner of the property elects to forfeit his/her proprietary rights the field office SAC will decide on the final disposition of the property. The forfeiture should be documented on an MOA and the Chain of Custody section of INV Form 30.

16.11 PROCEDURES TO DECLARE PROPERTY ABANDONED

If the property in question is valued at $500 or less, and if contact with the known owner has been attempted without result or if the owner is unknown, the property may be summarily abandoned with the approval of the SAC. In these cases, all attempts to contact the rightful owner must be documented in the case file.

Where the property is valued in excess of $500 and where exhaustive efforts fail to establish the whereabouts of the owner, or where the identity of the owner remains unknown, or where the owner refuses to answer, then before the property may be declared abandoned, it must be advertised in a periodical of general circulation within the Federal judicial district where the property was recovered. These advertisements are to appear once a week for three consecutive weeks and contain a description of the property, the location where the property was recovered, a statement advising that anyone wishing to file a claim as lawful owner must do so within thirty days, and complete mailing address of the office where a claim may be filed or additional information concerning the property obtained. A sample advertisement is appended. **(Exhibit 16-4)**

If no claim is made for property, title will vest to the United States upon expiration of the thirty-day claim period. If a claim is received, it must be in the form of a sworn statement by the claimant describing his vested interest in the property. This statement should be supported by acceptable documentation and a summary of facts that would justify granting a claim. SACs are directed to review such claims and make determinations of validity based on investigation of the merits of the claim. The information will be forwarded to the DAIGI Field Operations via memorandum for determination. When appropriate, Counsel will be consulted prior to a final determination.

If a claim is denied, the SAC will provide written notification to the claimant outlining reasons for the denial. A sample letter is appended. **(Exhibit 16-5)** The claimant may submit a written request for reconsideration of the denial within ten days. This request should be addressed to the SAC Field Operations. The basis for granting or denying a claim will be the claimant's proof of a valid, good faith interest in the property.

After conformance to all the steps outlined above, if the owner has not been located or identified, the property may be declared abandoned and disposed of in consultation with the SAC Field Operations will determine if the property should be converted to government use, donated, or destroyed.

CHAPTER 16.0 - EXHIBITS

16-1 INV Form 30, Evidence/ Personal Property Inventory Form.

16-2 INV Form 30A, Evidence/Personal Property Inventory Continuation.

16-3 INV Form 31, Evidence Log.

16-4 Sample advertisement.

16-5 Sample letter to claimant.

Exhibit 16-1, INV Form 30, Evidence/ Personal Property Inventory Form

Office of Inspector General - Investigations
U.S. Department of Homeland Security

Homeland Security

EVIDENCE PERSONAL PROPERTY INVENTORY FORM

CERTIFIED INVENTORY OF ☐ EVIDENCE ☐ PERSONAL PROPERTY	SERIAL NUMBER
ITEM(S) ___Taken From ___Received From ___ Found At ___Other (Describe Person or Location)	CASE NO.
ITEM(S) INVENTORIED BY _____ SIGNATURE – SPECIAL AGENT DATE	OFFICE
_____ SIGNATURE – REVIEWING SUPERVISOR DATE	Page ____ of ____

ITEM #	DATE RECEIVED & RECEIVED BY	QUANTITY	DESCRIPTION OF EVIDENCE or PERSONAL PROPERTY	VALUE
			Total	

INV FORM-30

Page ____ of ____

Exhibit 16-1, **INV Form 30, Evidence/ Personal Property Inventory Form - page 2**

CHAIN OF CUSTODY

If this inventory consists of more than one page, document the Chain of Custody Log on the reverse of the FINAL CONTINUATION SHEET.

ITEM NO.	DATE	ACTION	REGISTRY NUMBER(S)	SIGNATURE

INV FORM-30

Page _____ of _____

Exhibit 16-2, INV Form 30A, Evidence/Personal Property Inventory Continuation

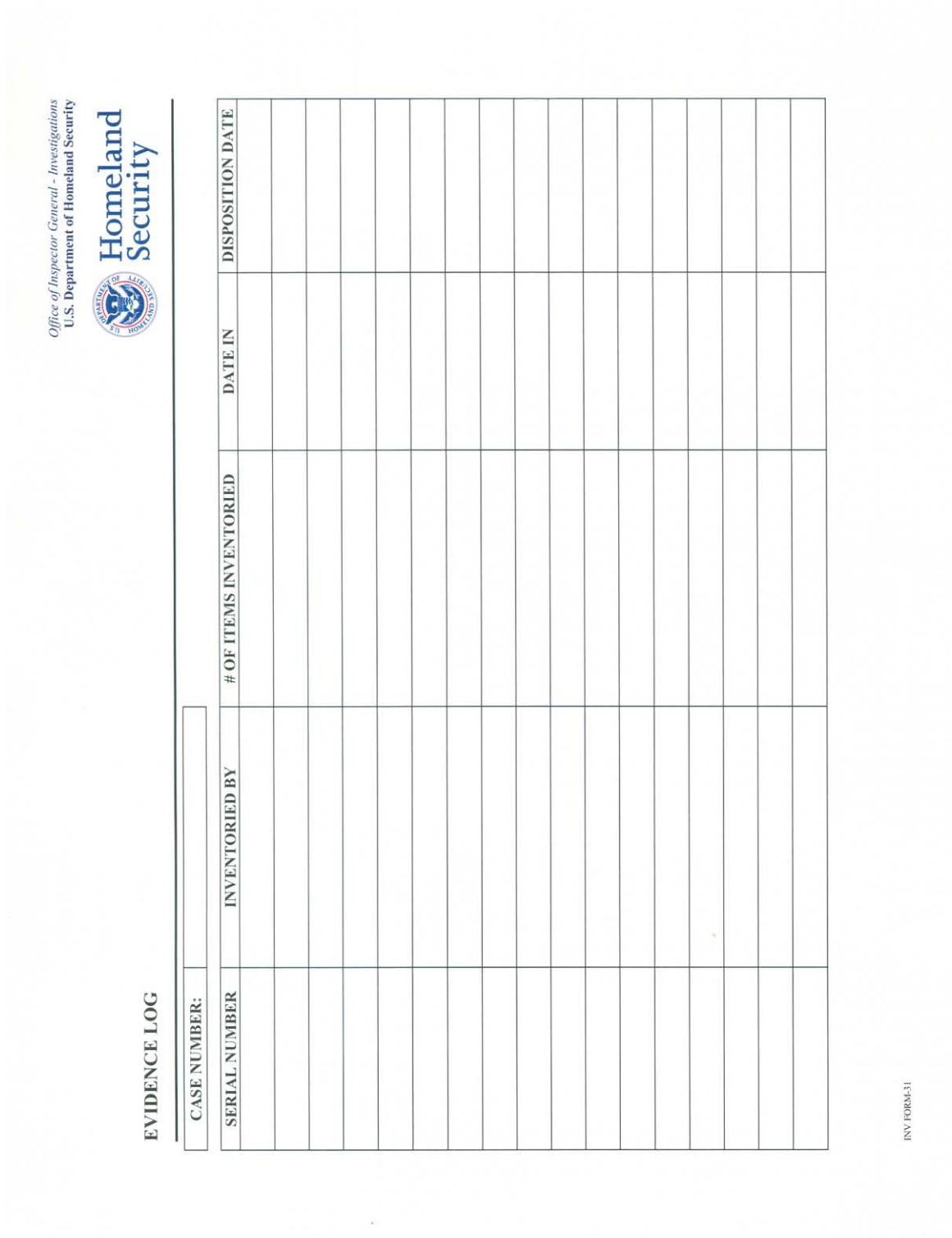
CERTIFIED INVENTORY OF ☐ EVIDENCE ☐ PERSONAL PROPERTY *(CONTINUATION SHEET)*

SERIAL NUMBER (FROM INV FORM-30)	CASE Number	PAGE OF PAGES

ITEM #	DATE RECEIVED & RECEIVED BY	QUANTITY	DESCRIPTION OF EVIDENCE or PERSONAL PROPERTY	VALUE
			BROUGHT FORWARD	
			TOTAL →	

INV FORM-30A

Exhibit 16-3, INV Form 31, Evidence Log



Office of Inspector General - Investigations
U.S. Department of Homeland Security

Homeland Security

EVIDENCE LOG

CASE NUMBER:				
SERIAL NUMBER	INVENTORIED BY	# OF ITEMS INVENTORIED	DATE IN	DISPOSITION DATE

INV FORM 31

Exhibit 16-4, Sample Advertisement

Sample Newspaper Advertisement

Abandoned Property

On (date of seizure) the Department of Homeland Security, Office of Inspector General, seized the property described as follows:

(Describe property)

The property was seized on (date) at (exact location) and remains in the custody of the Department of Homeland Security, Office of Inspector General, (city) Field Office.

Parties having legal claim to this property are hereby advised that you must file your claim for the above described property on or about (insert date 30 days from first publication date) and may do so by contacting the Special Agent in Charge, (field office), Department of Homeland Security, (address & telephone number). Refer to case number xxx-xxx-xxxx when making inquiry.

Exhibit 16-5, Sample Letter to Claimant

Office of Inspector General
Office of Investigations
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

Sample Letter to Known Owner to Claim Property

Date
File No.
Certified, Return Receipt Requested

Name
Address
Dear(name);

On (date) the Department of Homeland Security Office of Inspector General seized the property described as follows:

(List Items)

You are hereby advised that you have thirty days from the date postmarked on this letter to claim the above described property. If the property is not claimed by that date, title vest to the United States Government, Department of Homeland Security.

This property may be claimed by you or your authorized representative by contacting (name of person to be contacted) located at (address of field office or resident agency), telephone (number).

The property is currently (held as evidence, awaiting release to you, etc.) and upon conclusion of this case will be released to you or your authorized agent. If you do not wish to reclaim this property, please provide written instructions naming which private, charitable, or governmental agency to whom you wish to donate this property, if such is the case.

You are advised this property will only be released to you, your agent, or designee, in person, upon proper receipt.

Sincerely yours,

(Name)
Special Agent in Charge

17.0 CRIMINAL PROCEDURES

17.1 GRAND JURY INFORMATION (RULE 6(E))

Rule 6(e) of the "Federal Rules of Criminal Procedure" imposes strict obligations upon SAs to protect the secrecy of matters occurring before the Grand Jury. SAs handling Grand Jury materials may not disclose the material or their contents to any third party unless he or she is certain that the disclosure meets the applicable legal standards. SAs must seek clearance from the appropriate Assistant United States Attorney (AUSA) before disclosing Grand Jury material.

A knowing violation of Rule 6(e) may be punished as contempt of court. Breaches of Grand Jury secrecy may result in motions to dismiss indictments against defendants. Breaches of Grand Jury secrecy committed by IG personnel can result in agency disciplinary action against the offending employee.

SAs assisting a Grand Jury investigation should make certain that the AUSA has placed the SA's name on the Grand Jury access list. This list sets forth the names of all persons to whom disclosure of Grand Jury material has or will be made. The SA should also ensure that the name of the SAC and all other IG employees needing access to this file or the Grand Jury information are placed on the 6(e) list.

Grand Jury materials must be kept in a "limited access" storage file area. The official case file will be marked on the outside "Grand Jury Material." Only authorized personnel may have access to this area. During non-duty hours, all areas where Grand Jury material is present should be locked.

Rule 6(e) does not apply to information obtained through an IG subpoena. Therefore, SAs should consider using IG subpoenas in lieu of Grand Jury subpoenas in cases involving administrative actions (such as adverse personnel proceedings against employees) and civil fraud litigation (such as false claims cases). (Section 18.0)

17.2 INDICTMENT AND INFORMATION

Indictments and Informations are means by which individuals are prosecuted in the Federal Criminal Justice System.

Indictment

An indictment is a formal written accusation charging a person(s) with the commission of a crime. It is presented by a Grand Jury to the court after the examination of the evidence reveals that there is a probable cause to believe the defendant has committed the offense charged. A Grand Jury may return a True Bill, resulting in an indictment upon

concurrence of 12 or more jurors.

Federal Grand Juries are composed of 16 to 23 jurors who serve an appointed term not to exceed 18 months.

The only persons permitted to be present during Grand Jury proceedings are attorneys for the government, the witness under examination, interpreters when needed, and a stenographer or operator of a recording device. No person other than the jurors may be present when the Grand Jury is deliberating or voting.

Upon indictment, an arrest warrant or summons is issued.

Information

The Information, brought by the U.S. Attorney's Office (USAO), is a plain, concise, and definite statement of the essential facts constituting the offense charged and generally agreed to by the defendant.

The use of an Information is a decision within the purview of the USAO.

17.3 DECLINATIONS OF PROSECUTION

The date of and the reason for the decision must be documented in an MOA in each case in which prosecution has been declined by the USAO.

In some jurisdictions, the USAO may prefer to exercise prosecutorial discretion by issuing "blanket declinations" in certain types of cases. Otherwise, SAs should obtain a letter from the USAO outlining the reasons for the declination. In lieu of a letter from the USAO, SAs can send a letter to the USAO confirming that the matter has been presented to the USAO and declined for prosecution. A sample letter is included. **(Exhibit 17-1)**

Documents pertaining to declinations will be filed in the case file and appropriate office administrative file (6400).

All declinations will be entered into EDS by the investigating office.

17.4 ARRESTS

Arrest by Warrant

Arrest Warrants are issued by the Court, typically by a Magistrate, based upon a Criminal Complaint outlining the charges and supported by a sworn affidavit documenting the essential facts of the offense(s) charged. The Court will issue a warrant based upon determination of probable cause. **(Exhibit 17-2)**

The Criminal Complaint contains the following information: **(Exhibit 17-3)**

Name of the defendant (if name unknown, a complete description by which the defendant can be identified with reasonable certainty);

Statutory language of the offense charged;

Details of complainant's charge, and

A brief synopsis of the investigation explaining how the facts of the case became known to the agent. An affidavit may be used if the synopsis is lengthy.

Arrests Without a Warrant

It is OIG policy that arrests will not be affected without an arrest warrant unless extraordinary circumstances exist. Whenever possible, the SAC of the investigating office, in consultation with the DAIGI, will determine the circumstances under which arrests will be affected without a warrant.

When making an arrest without a warrant, the arrestee must be taken without unnecessary delay before the nearest federal magistrate judge, or if none is available, before a state or local judicial officer (as authorized and defined by 18 U.S.C. § 3041). At that time, a complaint has to be filed with the magistrate judge. If time allows, the complaint should be reviewed by the appropriate AUSA prior to presentation.

Arrest Warrant Execution

The arrest warrant may be executed any place within the jurisdiction of the United States by a United States Marshal or any other officer authorized by law. OIG SAs have the authority to execute arrest warrants. (Section 1.5)

Unexecuted warrants are returned to the issuing magistrate judge. The USAO may also request that the warrant be given to the United States Marshals Service for execution.

No arrest warrant will be executed on DHS property without prior notification to the AIGI.

The SA is not required to have the warrant in hand when making the arrest, but the defendant must be advised that a warrant has been issued and the offense(s) charged. The SA must also read the contents of the warrant to the defendant as soon as practicable after the physical arrest and show the defendant, upon request, a copy of the warrant.

INV policy provides that generally, a "Tactical Plan," INV Form 39 **(Exhibit 13-1)** will be prepared and approved by the investigating office SAC before the arrest warrant is executed. (Section 13.11)

Ideally a minimum of two SAs should be present to affect an arrest. If a second agent is not available, attempts should be made to enlist the cooperation of state or local law

enforcement, or the U.S. Marshals Service. In all cases, the arrestee will be handcuffed (double-locked) and thoroughly searched for the agent's safety, for the safety of those in contact with the arrestee and to secure items in the arrestee's possession. It is preferred that arrestees be handcuffed behind their back whenever possible. SAs will inform all arrestees of their constitutional rights per Miranda at the earliest possible opportunity. (Chapter 10.4)

The agent executing the warrant shall bring the defendant (along with a copy of the warrant) before the nearest federal magistrate judge, or state or local judicial officer if a magistrate judge is unavailable.

INV policy provides that generally, arrest warrants for defendants who are outside of the geographical boundaries of the investigating office will be forwarded to the field office where the defendant is currently located.

17.5 SUMMONS

A summons is used at the discretion of the USAO and orders the defendant to appear before a United States magistrate judge at a stated time and place. To obtain a summons, the SA should use the same procedures and forms used in obtaining an arrest warrant.

The summons is served by personally delivering a copy to the defendant or by leaving it at the defendant's dwelling or place of employment with a person of suitable age or discretion. An agent may also mail a copy of the summons to the defendant's last known address.

If the defendant fails to appear in response to the summons, an arrest warrant will be issued.

17.6 PROCESSING ARRESTEES

Generally, arrested individuals should be photographed and fingerprinted before being transported to a detention facility. If necessary, arrestees may be photographed and fingerprinted at the detention facility. Arrestees should execute a Miranda Rights Advisement and Waiver Form. (Chapter 10.4)

Fingerprints will be recorded on at least two Criminal Fingerprint Cards (FD-249). One of the criminal fingerprint cards will be mailed to the FBI for classification and storage. The other copy of the criminal fingerprint card will remain in the INV case file. An R-84 will be mailed to the FBI to report the final judicial disposition.

INV personnel must exercise care to ensure that an acceptable set of fingerprints is obtained at the time of arrest. Fingerprints which are unreadable or otherwise improperly recorded will not be accepted by FBI classification personnel.

Fingerprint cards must reflect the assigned originating agency (ORI) number. The

following ORI numbers have been assigned to DHS OIG:

[redacted]

Atlanta Field Office (ATL)
Chicago Field Office (CHI)
Dallas Field Office (DAL)
Detroit Field Office (DET)
Houston Field Office (HOU)
De Rio Sub Office (DRT)
Laredo Sub Office (LAR)
El Paso Field Office (ELP)
McAllen Field Office (MCA)
Miami Field Office (MIA)
Orlando Sub Office (ORL)
San Juan Resident Office (SNJ)
Philadelphia Field Office (PHL)
New York Resident Office (NYC)
Boston Sub Office (BOS)
Buffalo Sub Office (BUF)
San Diego Field Office (SND)
El Centro Resident Office (ELC)
Los Angeles Resident Office (LAX)
Tucson Field Office (TUC)
San Francisco Field Office (SFO)
Seattle Field Office (SEA)
Washington Field Office (WFO)
Special Investigations Division (SID)

Mug shots of arrestees should consist of two full-faced photographs. All mug shots will have the following information placed on the reverse side of the photograph: name of the offender, date of photograph, and the case number.

17.7 INITIAL APPEARANCE (RULE OF CRIMINAL PROCEDURE - RULE 5(A))

An arrestee must be brought before a U.S. magistrate judge for an initial appearance. During the initial appearance, the arrestee is informed of the complaint against them, provided an opportunity to consult with counsel, advised of their right to a preliminary hearing, and admitted to bail.

A defendant who waives preliminary examination is held to answer in the district court. If the defendant does not waive preliminary examination, a date is set for one during the initial appearance before the magistrate judge.

17.8 PRELIMINARY HEARING (RULE OF CRIMINAL PROCEDURE – RULE 5(C))

The preliminary examination is a probable cause hearing. The U.S. magistrate judge shall hold the defendant to answer in the district court if, from the evidence, it appears there is probable cause to believe that an offense has been committed and the defendant committed the offense.

If no probable cause is found to believe that an offense has been committed and that the defendant has committed the offense, the magistrate shall dismiss the complaint and discharge the defendant.

If charges are brought by indictment, the Grand Jury determines probable cause and a Preliminary Hearing is not held.

17.9 THE ARRAIGNMENT (RULE OF CRIMINAL PROCEDURE - RULE 10)

Arraignments are conducted in open court and consist of reading the indictment or information to the defendant, or stating to him the substance of the charge and calling on the defendant to enter a plea to the charges.

If the defendant pleads not guilty, the case is remanded for trial.

If the defendant pleads guilty and the court accepts the defendant's plea, the court sets a sentencing date and orders the U. S. Probation Office (USPO) to conduct a pre-sentencing investigation.

17.10 PRETRIAL DIVERSION

The USAO uses pretrial diversion as an alternative to prosecution in certain situations favorable to the government. The pretrial diversion program is an alternative to prosecution that seeks to divert certain offenders from traditional criminal justice processing into a program of supervision and services administered by the USPO. The diversion is finalized by a written contract agreed to by prosecution, defendant, and defendant's counsel. Only certain offenders meeting established criterion are eligible for Pretrial Diversion. Pretrial Diversions will be documented in an MOA and entered into the IDMS. Offenders receiving Pretrial Diversion will be fingerprinted and photographed in accordance with INV Arrest Procedures.

CHAPTER 17.0 - EXHIBITS

Exhibit 17-1, Sample USAO Declination Letter

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

United States Attorney
District of [XXXXXXXXX]
Address:

Attention: AUSA [Name]

Subject: [Name and Title of Subject]

Dear Sir (or Madam):

This letter is to confirm your [date], telephone conversation with Special Agent [Name] of my staff, wherein you declined criminal prosecution of [name of subject]. This office presented the [Doe] matter to your office for determination of possible violations of [cite federal statute e.g. 18 U.S.C. 641 (Theft of Government Property)] by the captioned subject.

[Provide a brief description of the subject's actions relative to this alleged violation.]

You declined prosecution in this matter citing [state reason, e.g. the lack of criminal intent.]

Thank you for your prompt attention to this matter, and if you have any questions concerning this letter please contact me, at [Telephone Number], or Assistant Special Agent in Charge [Name], at [Telephone Number].

Sincerely,

[Name]
Special Agent in Charge
[Field Office]

Exhibit 17-2, Sample Warrant for Arrest an Complaint

AO 442 (Rev. 5/85) Warrant for Arrest

United States District Court

_____DISTRICT OF_____

UNITED STATES OF AMERICA
V.

WARRANT FOR ARREST ON COMPLAINT

(Name and Address)

CASE NUMBER:

To: The United States Marshal or any Authorized United States Officer

YOU ARE HEREBY COMMANDED to arrest _____
Name
and bring him or her forthwith to the nearest Judge/Magistrate to answer a complaint charging him or her with (brief description of offense)

in violation of Title _____ United States Code, Section _____.

with Bail fixed at $_____

Approved to Form_____,[Name], AUSA

Date:_____ _____
Name of Judge/Magistrate

_____
Signature of Judge/Magistrate

RETURN		
This warrant was received and executed with the arrest of the above-names defendant at_____		
DATE RECEIVED _____ DATE OF ARREST	NAME AND TITLE OF ARRESTING OFFICER	SIGNATURE OF ARRESTING OFFICER

Exhibit 17-3, Sample Criminal Complaint

AO 91 (Rev. 5/85) Criminal Complaint

United States District Court

_____DISTRICT OF_____

UNITED STATES OF AMERICA
V.

CRIMINAL COMPLAINT

CASE NUMBER:

(Name and Address of Defendant)

I, the undersigned complainant being duly sworn state the following is true and correct to the best of my knowledge and belief. On or about_____[Date]_____ in_____ county, in the _____District of _____ defendants(s) did, (Track Statutory Language of Offense)

Violation of Title _____ United States Code, Section(s) _____.
I further state that I am a(n) _____[Official Title]_____ and that this complaint is based on the following facts:

Approved to Form_____,[Name], AUSA

Continued on the attached sheet and made part of hereof: ☐ Yes ☐ No

_____
Signature of Complaint

Sworn to before me and subscribed in my presence,

_____ at _____
Date City and State

_____ _____
Name & Title of Judicial Officer Signature of Judicial Officer

18.0 INSPECTOR GENERAL SUBPOENAS

18.1 IG SUBPOENA AUTHORITY

The Inspector General Act and Homeland Security Act of 2002, provide DHS OIG with broad authority to subpoena documentary evidence necessary to the performance of the IG's responsibilities. The Inspector General or designee signs IG subpoenas. Special procedures covering subpoenas issued to financial institutions for records controlled by the Right to Financial Privacy Act, 12 U.S.C. §§ 3401-3422 (RFPA), are covered by Chapter 21, Sections 5 through 11.

IG subpoenas are usually preferred to grand jury subpoenas because records obtained by grand jury subpoena cannot be used in administrative actions and are difficult to obtain in civil fraud litigation. (Chapter 17.1)

Once an investigation is the subject of federal grand jury proceedings, it is still possible to use IG subpoenas; however, courts will more closely scrutinize the subpoena to prevent improper expansion of criminal discovery or violation of grand jury secrecy rules. If there is a related ongoing criminal investigation or prior referral of a possible criminal violation to the Attorney General, consult with the Office of Counsel and with the U.S. Department of Justice/U.S. attorney's office on all such subpoena requests.

IG subpoenas may be used where the related audit, investigation, or other OIG inquiry is legitimate and within the lawful jurisdiction of the OIG. When there is reason to believe the documents sought are relevant to the inquiry, and the subpoena demands are not so broad or indefinite so as to make compliance unduly burdensome.

Restrictions

IG subpoenas may not be issued to another federal agency. IG subpoenas cannot be used to collect records on behalf of another Federal or state agency, although subpoenas may be issued in joint inquiries worked with other agencies as long as there is a legitimate OIG purpose.

IG subpoenas to compel production of records located outside the United States are not enforceable in U.S. district courts and whether they are enforceable in a foreign court depends on the country. Contact OIG Counsel if you require a subpoena to be issued to an entity outside the United States.

Subpoena Alternatives.

Audit Access Clauses: Consider whether OIG already has access to the needed records through a contract or agreement that includes an "audit access clause" requiring a contractor or other party to provide OIG with records upon request.

General Release: If a custodian of records requires a written release from the person to whom the records pertain before the custodian will release the records, SAs should use INV Form 04, "Authority for Release of non-RFPA Financial Records." **(Exhibit 18-1)** **NOTE**: **This form may be used to obtain records from a bank only when the records sought are NOT protected by the RFPA**. (Chapter 21, Sections 5 through 7)

18.2 TYPES AND CATEGORIES OF RECORDS SUBJECT TO SUBPOENA

IG subpoena authority applies to all information, documents, reports, records, accounts, papers, and other data and documentary evidence necessary to carry out the statutory functions of the IG Act, including audits, investigations, evaluations, and inspections. Generally, the subpoena power applies to four categories of records.

Corporate and other non-personal records: The IG Act enables the OIG to require production of records from corporations, subcontractors, grantees, and other third parties, even those not required to be made available under provisions of a particular contract.

Personal records: Individuals can be required to produce records within their personal possession, responsibility, or control, including tax returns, bank statements, and employment records unless the individual asserts a Fifth Amendment privilege and proves that the act of production is equivalent to compelling a statement against him or herself. This Fifth Amendment privilege is not available under certain circumstances, including, for example, where the subpoenaed records are required by law to be maintained.

Government records: A State or municipal government body or agency can be required to produce documents, but IG subpoenas cannot be used to obtain records and information from other Federal agencies. NOTE: When requesting records or documents from a State or municipal government body or agency, use an IG subpoena or other appropriate legal process. Failure to do so may raise questions regarding OIG's obligation to reimburse the government body or agency. Contact Counsel for further information.

Records held by financial institutions: Financial institutions, such as banks, credit unions, loan companies, and credit card companies, can be required to produce financial records of customers. However, OIG must comply with the RFPA when seeking customer financial records of individuals or partnerships of five or fewer individuals.

18.21 RIGHT TO FINANCIAL PRIVACY ACT (RFPA)

The RFPA of 1978, 12 U.S.C. §§ 3401-3422, generally prohibits the disclosure to the government of the "financial records" of the "customers" of "financial institutions," except in accordance with specified access procedures.

18.22 RFPA DEFINITIONS

The term "financial record" is broadly defined to mean an "original of, a copy of, or information known to have been derived from, any record held by a financial institution pertaining to a customer's relationship with the financial institution." Accordingly, the RFPA expressly exempts any financial record or information not identifiable with a particular customer. The RFPA, therefore, does not directly protect:

> Records pertaining to a person who appears in the account of another customer (e.g., check endorsements); or,
>
> Items drawn by an individual and deposited into the account of a corporation, if the item is obtained through a search of the corporation's account.

The term "customer" is narrowly defined to include any person or authorized representative of that person or partnerships of five or fewer individuals that use a financial institution in connection with an account maintained under the person's or partnership's name. The RFPA does not pertain to the customer records of corporations, associations, larger partnerships, or other legal entities.

The term "financial institution" includes banks and consumer finance businesses, as well as credit unions and companies issuing credit cards, located in any state or territory of the United States, the District of Columbia, Puerto Rico, Guam, American Samoa, or the Virgin Islands. Court decisions have extended interpretation of this term to include all institutions that extend credit, such as telephone companies, department stores, or gas companies, with regard to charges made to their credit cards.

The term "law enforcement inquiry" means "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."

18.23 ACCESS TO FINANCIAL RECORDS

The RFPA prohibits any agency or department of the United States from obtaining financial records from financial institutions (and any financial institution from disclosing such records to the government) unless access is permitted by one of the enumerated exceptions to the RFPA, or is accomplished through one of the RFPA's five access mechanisms:

> Customer Consent and Authorization for Access to Financial Records, INV Form 04A **(Exhibit 18-3)**

Administrative summons or IG subpoena

Search warrant

Judicial subpoena

Formal written request (Formal written request is available only to agencies that do not have administrative subpoena authority.)

Financial institutions are permitted to notify government authorities when they have information relevant to any possible violation of law or regulation reflected in a customer's financial records. Such information may include only the name or other identifying information concerning any individual, corporation, or account involved in and the nature of the suspected illegal activity.

All requests for financial records should be coordinated through Counsel's office.

18.24 DELAYED NOTIFICATION

In situations where any notice to the customer that his/her records are being (or were) sought or obtained under the RFPA would seriously jeopardize a law enforcement inquiry or some related law enforcement interest, the government may apply to a court for a delay of its notification obligation of up to 90 days (180 days under 12 U.S.C. § 3406(c) for an initial delay of search warrant notification).

Pursuant to 12 U.S.C. §3409(a), to obtain such a delay of notice order, the government must make a showing to a judge or magistrate sufficient to support findings that:

The pertinent investigation is within the agency's lawful jurisdiction;

There is reason to believe the records sought are relevant to a legitimate law enforcement inquiry; and,

There is reason to believe that notice would result in:

Danger to the life or physical safety of any person;

Flight from prosecution;

Destruction of or tampering with evidence;

Intimidation of a potential witness; or,

Otherwise seriously jeopardize an investigation or official proceeding, or unduly delay a trial or ongoing official proceeding.

Further delays may be granted for periods not exceeding 90 days upon the same showing of necessity.

Any court order delaying notice under the Act not only relieves the government of its notification responsibility, but also expressly prohibits the financial institution from disclosing, during the delay period, that records were sought or obtained.

After expiration of the period of delay, the customer must be served with or mailed a copy of the process or request together with the following notice which shall state with reasonable specificity the nature of the law enforcement inquiry:

18.25 TRANSFER OF FINANCIAL RECORDS

12 U.S.C. §3412 contains special restrictions on the government's transfer of any records originally obtained under the RFPA.

Transfer of financial records obtained under RFPA should be coordinated through Counsel's office. Such records may be transferred to "another agency or department" only if an official of the transferring agency certifies in writing that there is reason to believe that the records are relevant to a legitimate law enforcement inquiry within the jurisdiction of the receiving agency or department.

Additionally, the customer must be notified of any such transfer within 14 days unless the government first obtains a court order delaying such notice.

The requirement for customer notice does not apply when financial records obtained by INV are disclosed or transferred to a USAO upon the certification by a SAC or his/her supervisor that:

There is reason to believe that the records may be relevant to a violation of federal criminal law and,

The records were obtained in the exercise of INV's lawful authority to conduct investigations relating to the programs and operations of the Department of Homeland Security.

18.26 RFPA EXCEPTIONS

RFPA does not apply to subpoenas issued by federal grand juries. Reference 12 U.S.C. § 3420. However, financial records (or a description of voluminous records) so obtained must be actually presented to the grand jury and the records must be destroyed or returned to the financial institution if they are not used in connection with a criminal proceeding.

18.27 RFPA COST REIMBURSEMENT

12 U.S.C. § 3415 of the RFPA requires generally that a financial institution be reimbursed for the costs incurred in assembling or providing financial records. Reimbursement rules are set forth in 12 C.F.R. Part 219.

Pursuant to 12 C.F.R. § 219.4 (c) government entities, including the OIG, are not required to reimburse a financial institution for the costs of complying with a subpoena when the records sought do not belong to a particular "customer."

While OIG could choose to reimburse the institution, it is not required by law to do so.

The USAO reimburses costs incurred as a result of grand jury subpoenas.

All requests for financial records for which reimbursement is required will be coordinated with Counsel.

18.3 SUBPOENA PROCEDURES

SAs will complete the following subpoena forms online by clicking on "My Computer", then "Groups on Dc1clu01 (O:)", then "OIG Wide", then "OC Forms". Choose "Standard Subpoena" or "RFPA Subpoena."

Requests for Standard Subpoenas:

> Request Memo: Provide a description of the case and alleged violations, explaining why the requested records are relevant and how these records will advance a legitimate purpose of the investigation.
>
> Additional Required Forms: Cover Letter, Subpoena, and Attachment A must be prepared for each subpoena. **(Exhibit 18-2)**
>
> SAs are only required to submit one Subpoena Request Memo for multiple accounts from the same service provider with an explanation in the background section of the Request Memo.

SAs will forward a copy of the completed subpoena request and associated forms via email to the SAC for approval. The SAC will forward the approved request to the DAIGI and the Office of Counsel concurrently for processing.

Counsel prepares the subpoena (and related documents); tracks it in the OIG Subpoena Log; signs off and submits it to the AIGI for approval.

The AIGI forwards the signed subpoena to the requesting office.

Requests for RFPA Subpoenas:

Customer Authorization: Utilize INV Form 04A, "Customer Consent for Access to Financial Records" **(Exhibit 18-3),** if the bank customer authorizes OIG access. Therefore, a subpoena is not required.

Request Memo: Provide a description of the case and alleged violations, explaining why the requested records are relevant and how these records will advance a legitimate purpose of the investigation. Ensure that the "yes" block in Item 11 is checked.

RFPA Cover Letter to Bank: Fill in the recipient bank's name and address, and special agent's name and office location. Insert the suggested text into the cover letter, where an investigation requires that the subpoenaed party not further disclose the existence of the subpoena.

RFPA Subpoena: Fill in recipient's name and address, and compliance date (usually 2 weeks from the date you request the subpoena) and location (Counsel fills in the subpoena number).

RFPA Attachment A: Utilized when request is for financial records.

Subpoena Service

SAs should serve the subpoena on the financial institution and the customer concurrently as soon as possible after issuance, and will not serve a subpoena after the indicated compliance date. The subpoena should be served personally during normal business hours, if possible.

Refusal to accept service: If a person refuses to physically accept service, the SA may leave the subpoena in the immediate vicinity of the person, e.g., on the individual's desk in an office or reception area when the individual is physically present and has notice that the subpoena is being left.

Service upon attorney: Service on a person's attorney is acceptable only if attorney has been authorized to accept service of the subpoena.

Service on business entities: Serve a corporation, partnership, or other business entity by serving the entity's resident agent or custodian of records.

Service by certified or registered mail: Where circumstances warrant (e.g., when the subpoenaed party cannot be located), an SA may serve subpoenas by registered mail or by certified mail, return receipt requested, to the subpoena addressee's last known address.

Service by facsimile or express mail: Subpoenas may be served by facsimile or express mail, only where the subpoena recipient has agreed in advance to accept service by this alternative method.

Proof of service: Serve a copy of the subpoena and the original cover letter on the addressee. Complete the "Return of Service" and maintain it, along with a copy of the subpoena and all other subpoena-related documents in the office case file. Document the subpoena compliance date on an MOA, INV Form-09.

Subpoena Compliance

Certificate of Compliance: This certificate authorizes the financial institution to comply with the subpoena as no challenge has been filed. It should be served on the financial institution after the respective dates for a challenge by the customer have expired (10 days if personal service or 14 days if mailed).

Limited initial production: Recipients may be asked to provide a limited and specific sub-set of subpoenaed documents first, and the remaining documents on a rolling basis. This is often desirable when requesting voluminous documents from, for example, a financial institution. Ensure that OIG's right to review all subpoenaed materials is preserved and contact the Office of Counsel if questions arise.

Time for production: Allow a reasonable time frame to allow for production of records -- usually 10 working days (can be a longer time period for RFPA subpoenas).

Extensions: Grant time extensions on compliance where reasonable, but officially record the extension in a letter to the addressee with a copy to the case file. Contact OIG Counsel if questions arise regarding the appropriateness of an extension.

Place of production: The usual place of production is the nearest OIG office. Other locations may be appropriate, depending on the circumstances and where the records are located. OIG may authorize subpoena addressees to produce records by courier, or express or certified mail, return receipt requested, where appropriate.

Non-compliance: Notify Counsel regarding questions about time extensions or if an addressee does not comply with the terms of the subpoena. Counsel will work with the U.S. Attorney's Office to enforce the subpoena in United States District Court if the addressee does not comply with the subpoena.

Retention and Disclosure of Documents

Retention: Maintain documents securely in case files.

Disclosure: Subpoenaed records are not disclosed except as required by law (e.g., by court order), and as necessary in performance of IG responsibilities. Records obtained under the RFPA cannot be disclosed except as authorized by the RFPA (Chapter 21.9).

Reimbursement: Generally, costs resulting from production of records in response to a standard IG subpoena are borne by the subpoena recipient. There are exceptions to this general rule. For example, OIG is required to reimburse costs in certain circumstances such as subpoenas issued under the RFPA for bank records (Chapter 21.11), and subpoenas issued under the Electronic Communications Privacy Act, 18 U.S.C. §§ 2701-2712, for the content or text of electronically-stored messages. Do not agree or promise to reimburse for compliance costs of any non-RFPA subpoena without first consulting Counsel. Forward any subpoena reimbursement requests to Counsel for review.

CHAPTER 18.0 - EXHIBITS

18-1 INV Form 04, Authority for Release of non-RFPA Financial Records.

18-2 INV Form 41, Office of Counsel IG Subpoena Request Templates.

18-3 INV Form 04A, Customer Consent for Access to Financial Records.

Exhibit 18-1, INV Form 04, Authority for Release of non-RFPA Financial Records

Office of Inspector General - Investigations
U.S. Department of Homeland Security

Homeland Security

AUTHORITY FOR RELEASE OF NON-RFPA FINANCIAL RECORDS

To Whom It May Concern

I, _____, _____(Title), hereby authorize any Special Agent of the Department of Homeland Security, Office of the Inspector General (OIG), bearing this release, or a copy thereof, within one year of its date, to obtain any information from any bank or other financial institution.

I hereby direct you to release such information directly to the bearer of this authorization. I understand that the information released is for official use by the OIG and, pursuant to the Inspector General Act of 1978 (Public Law 95-452) may be disclosed to such third parties as necessary in the fulfillment of the OIG's responsibilities.

I hereby release any individual, including record custodians, from any and all liability for damages of whatever kind or nature, which may at any time result to me on account of compliance, or any attempts to comply, with this authorization. Should there be any question as to the validity of this release, you may contact me as indicated below.

Signature *(Full Name)* _____

Full Name *(Printed)* _____

Other Names Used _____

Date _____

Current Address _____

_____

_____

Telephone Number _____

INV FORM-04 (Revised Sep 2008)

Exhibit 18-2, IG Subpoena Templates

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

MEMORANDUM FOR: Assistant Inspector General for Investigations

THROUGH: Deputy Assistant Inspector General for Investigations

FROM: [ ]
Special Agent in Charge

SUBJECT: Request for Issuance of Subpoena

I request that you issue a subpoena in the matter described below:

1. Authority: IG Act of 1978, as amended, 5 U.S.C.A. App. 3.
2. OIG File No.:
3. Nature of inquiry: [ ] Audit [ ] Investigation
   [ ] Joint Audit/Investigation [ ] Inspection [ ] Other
4. Homeland Security agency and program:
5. Subject(s) of inquiry:
6. Name of person (and title, if person is to be subpoenaed in representative capacity) or entity to be subpoenaed:
7. Relationship of person/entity to be subpoenaed to subject of inquiry:
8. Background: [Agent describes nature of case and need for the particular documents sought either here or in an attachment.]
9. Purpose(s) of subpoena:
10. Description of records sought: See Attachment A appended to subpoena.

11. Does the Right to Financial Privacy Act, 12 U.S.C. §§ 3401-3422, cover the records being subpoenaed? [ ] Yes [ ] No

    If so, special procedures must be followed per manual chapter on OIG Subpoena Authority.

12. Have efforts been made to obtain records by means other than subpoena? [ ] Yes [ ] No If so, how and with what results:

13. Is the subject of this investigation or the person/entity to be subpoenaed the subject of any non-OIG investigation or any civil, criminal or administrative proceedings? [ ] Yes [ ] Unknown [ ] If so, describe:

14. Has the subject of this inquiry been discussed with a United States Attorney's Office, or the Department of Justice in Washington? [ ] Yes [ ] No If so, provide name and telephone number.

15. Recommendation for requiring production of records in person:

    [ ] Yes [ ] No If yes, explain:

16. Date and time for production, if no court challenge:

FIELD OFFICE REVIEW

17. Cleared by Special Agent in Charge: [ ] Yes [ ] No

    Initials and date:

    Comments, if any:

FOR HEADQUARTERS USE

18. Cleared by Desk Officer: [ ] Yes [ ] No

    Initials and date:

    Comments, if any:

19. Cleared by Office of Counsel: [ ] Yes [ ] No

Initials and date:

Comments, if any:

20. Cleared by IG, Acting IG, DIG or AIG: [ ] Yes [ ] No

Initials and date:

Comments, if any:

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

[Address]

Dear Sir or Madam:

Pursuant to the Inspector General Act of 1978, as amended, 5 U.S.C.A. App. 3, Section 6(a)(4), the enclosed Subpoena Duces Tecum has been issued. The materials identified should be produced for the Office of Inspector General by the date and time indicated on the subpoena. You may elect to deliver the documents in person or via registered mail to Special Agent [ ], U.S. Department of Homeland Security, Office of Inspector General, Office of Investigations, [Street, City, Zip].

Fully legible and complete copies of the records called for will be accepted in response to the subpoena, provided that the original records will be made available to employees of the Office of Inspector General, upon request, during normal business hours. It would also be helpful for you to provide us with a list identifying each document or other material furnished and the item or items of the subpoena to which it relates.

The enclosed Statement of Production must be executed by you or another individual holding full legal authority to attest to the accuracy, authenticity and completeness of the documents produced. If any of the required materials are not furnished for any reason, you are required to list and indicate the location of such materials and the reason for nonproduction. Failure of the documents to arrive by the time and date set forth in the subpoena will be considered a failure on your part to comply with the subpoena, and may result in an enforcement action.

[NOTE: Either pick one of the bracketed choices or delete the second or both of these bolded sentences.] [Please do not disclose the existence of this subpoena. Any such disclosure could impede [this investigation] [or] [a criminal investigation (if there is criminal potential)] and interfere with the enforcement of law. You should bear in mind that you have the right to consult with and be represented by an attorney in connection with this matter.

Should you wish to discuss any matter pertaining to the execution of this subpoena, please feel free to call Special Agent [ ], at (XXX) XXX-XXXX, or Ric Doery, Office of Counsel at (202) 254-4209.

Sincerely,

Thomas M. Frost
Assistant Inspector General for Investigations

Enclosures

No. XX

United States of America
DEPARTMENT OF HOMELAND SECURITY
OFFICE OF INSPECTOR GENERAL
SUBPOENA DUCES TECUM

To: [Name]
[Address]

PURSUANT TO TITLE 5 U.S.C.A. APP. 3, SECTION 6(a)(4), YOU ARE HEREBY COMMANDED TO DELIVER the materials listed at Attachment A, to Special Agent [ ], United States Department of Homeland Security, Office of Inspector General, Office of Investigations, X Street, Suite X, City, ST Zip, on or before the ___ day of _____, 2008, at 10 o'clock a.m.

This material is necessary to carry out a legitimate law enforcement inquiry under the authority of the Inspector General Act of 1978, as amended, 5 U.S.C.A. App. 3. Under this Act, the Inspector General has the duty and responsibility to conduct and supervise audits and investigations, to promote economy, efficiency and effectiveness in the administration of, and to prevent and detect fraud and abuse in and relating to, the programs and operations of the Department of Homeland Security.

IN TESTIMONY WHEREOF, the undersigned
Assistant Inspector General for Investigations
of said DEPARTMENT OF HOMELAND SECURITY,
has hereunto set his hand at Washington, D.C.
this_____day of [month], 2008.

Thomas M. Frost

ATTACHMENT A

The following documents, as that term is defined in Attachment B, in the custody or control of (Company Name). from (date) to (date) regarding telephone number .....

1. All business and subscriber records to include the subscriber's full name and account information. Also include address, telephone number(s), date account created, length of service, account number(s), and detailed billing records and types of services utilized by the account holder for the above mentioned dates.

2. Billing information to include method of payment and payment history.

18-3 INV Form 04A, Customer Consent for Access to Financial Records

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528

[If the bank customer authorizes OIG access, use this form. A subpoena will not be necessary.]

Homeland Security

Customer Consent and Authorization for Access to Financial Records
Right to Financial Privacy Act, Sec. 1104(a), 12 U.S.C. § 3404(a)

CUSTOMER CONSENT AND AUTHORIZATION
FOR ACCESS TO FINANCIAL RECORDS

I, _____ , having read the explanation
(Name of Customer)

of my rights which is attached to this form, hereby authorize the

_____
(Name and Address of Financial Institution)

to disclose the financial records it maintains on any accounts relating to me to any Special Agent of the Department of Homeland Security, Office of Inspector General, bearing this authorization, or a copy thereof, to carry out a legitimate law enforcement inquiry under the authority of the Inspector General Act of 1978, as amended, 5 U.S.C.A. App. 3. The records will be used for the following purpose(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 three months from the date of my signature.

_____ , 20__ _____
(Date) (Signature of Customer)

_____

_____

_____
(Address of Customer)

INV Form-04A (Revised Sept 08)

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

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 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 three months, and your financial institution must keep a record of the instances in which it discloses 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

INV Form-04A (Revised Sept 08)

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 or write to:

DHS/Office of Inspector General/STOP 2600
Attn: Ric Doery 202-254-(b)
245 Murray Drive, S.W., Bldg 410
Washington, D.C. 20528

Sec. 1104(a) of the Right To Financial Privacy Act, 12 U.S.C. § 3404(a)

INV Form-04A (Revised Sept 08)

19.0 CIVIL RIGHTS INVESTIGATIONS

19.1 CIVIL RIGHTS STATUTES

Title 18 USC Section 242, Deprivation of Rights Under Color of Law, is the most common Civil Rights statute violated by employees of the Department. This statute prohibits an employee from willfully depriving any person of rights secured by the constitution. In order to substantiate such a violation the following elements must be proven:

the subject must have been acting under color of law, statute, ordinance, regulation, or custom;

the right, privilege or immunities granted the victim must have been secured or protected by the Constitution of the United States; and

the subject must have willfully deprived, or caused to be deprived, such a right from any person in any State, Territory, or District of the United States.

A violation of 18 USC § 242 is punishable by fine and imprisonment up to ten (10) years when bodily injury or use of a dangerous weapon is involved; life imprisonment if there was an attempt to kill, kidnap, or commit aggravated sexual abuse; and life imprisonment or capital punishment in cases of death.

Additionally, violations of other Civil Rights statutes that may be considered and applicable in OIG investigations would include 18 U.S.C. § 241 (Civil Rights Conspiracy), 18 U.S.C. § 1001 (False Statements), 18 U.S.C. § 1512 (Witness Tampering), and 18 U.S.C. Section 1519 (Destruction, alteration, or falsification of records in Federal investigations and bankruptcy).

19.2 NOTIFICATION OF COMPLAINTS TO THE DEPARTMENT OF JUSTICE (DOJ)

A Memorandum of Understanding with DOJ outlines procedures for handling allegations of Civil Rights violations. **(Exhibit 2-7)**

Within 24 hours, or the next business day, of receiving a complaint involving an allegation of a civil rights violation against a DHS employee, the SAC/ASAC will send via fax a copy of the complaint and any supporting documents to the Department of

Justice, Civil Rights Division, Criminal Section (CRD). CRD can be reached at 202-514-3789, FAX 202-514-8336.
The supporting documents will include the results of a review of EDS to determine if the subject or victim have had a past record of any complaints or proven civil rights violations. Additional supporting documents might include any victim/witness statements, photographs, police reports, medical records, etc.

CRD attorneys will review the matter and contact the OIG with a decision to initiate or decline an investigation, or to request more information. CRD may request the FBI to investigate the allegations due to concurrent jurisdiction. The DHS OIG and the FBI Civil Rights Unit will determine the composition of the investigative team.

The United States Attorney's Office (USAO) in the district where the violation occurred should also be notified at the same time CRD is notified. The USAO may confer with the CRD. In certain judicial districts a civil rights task force may have been established with a designated AUSA. The complaint and other supporting documents should also be faxed to the USAO. If directed by the USAO or CRD, a copy of the complaint will also be sent to the FBI.

19.3 DOCUMENTING CIVIL RIGHTS COMPLAINTS IN EDS

At the time the allegation is entered into EDS, the term "Civil Rights" will be selected from the
"Investigative Type" drop-down menu on the EDS Investigative/Complaint Data page.

The "Remarks" field of the complaint will be used to document contact with CRD and the USAO. When a decision is received from the CRD and the USAO, the response, the date it is received, and the name of the deciding official will be recorded.

19.4 PROCESSING THE ALLEGATION

Generally, the complaint will not be reclassified in EDS until a prosecutorial decision is rendered.

When CRD requests an investigation by the OIG, or requests a joint investigation by the OIG and FBI, the complaint will be classified as an Investigation in EDS.

If it is determined that the FBI will be the sole investigative agency, CRD will forward the complaint to the FBI. The Desk Officer (DO) will inform the component that the FBI will conduct the civil rights investigation.

If the CRD and the USAO decline prosecution, the complaint will not be opened as an investigation by the OIG unless it is determined that it is necessary for the OIG to conduct an administrative investigation. Generally, the complaint will be designated as a referral ("R") and forwarded to the DO for referral to the DHS component. This should be annotated in EDS.

If the allegation had been initially opened as an investigation and subsequently determined that the FBI should be the sole investigating agency or prosecution was declined, the investigation will be closed with the submission of an AROI.

19.5 JOINT INTAKE CENTER CR COMPLAINT REFERRALS

As stated in Chapter 7.4, DHS components are required to refer CR allegations to the OIG. These complaints will be processed as follows:

Complaints received from the JIC will be reviewed and processed by ISD.

DOs will review complaints to determine if quantifiable physical injury (stitches, gunshot wound, or physical contact that occurred after handcuffing, such as slap across the face or flashlight to back of head, etc.). Those meeting this standard will be referred to the respective SAC for review. For all other complaints not meeting this standard, (alleged verbal assault, pinched wrist while handcuffing, hard arrests etc.), these will be returned to the JIC classified as a Box 1.

In the case of a complaint, which is referred to the field by the DO, the DOs will advise the JIC within 24 hours that a preliminary inquiry is being conducted.

The SAC to whom the complaint is referred will conduct a preliminary inquiry, and consult with CRD and local AUSA.

If upon completion of the preliminary inquiry, CRD and, if applicable the local USAO, decline prosecution, the SAC may close the referral by forwarding record of the declination along with any documents received from the JIC (initial referral), and any Memoranda of Activities (MOAs) generated during the preliminary inquiry will be emailed to the DOs. The SAC still has the option of continuing the investigation.

Should preliminary inquiries result in the CRD, or the local USAO, accepting the case for prosecution, the SAC will inform the DO and an investigation will be opened in EDS.

19.6 FIELD ORIGINATED CIVIL RIGHTS COMPLAINTS

Complaints received in the field that do not warrant investigation will be emailed to ISD with all relevant documents for entry into EDS. ISD will notify the JIC.

Upon receipt of a complaint, which merits further inquiry, the reporting office will notify ISD by email of the nature of the complaint and the identity of the subject. ISD will forward an email advising the JIC that a preliminary inquiry is being conducted.

Upon completion of the preliminary inquiry, if the SAC determines that an investigation is warranted, the reporting office will forward predicate documents to ISD by email so that an investigation will be opened in EDS.

19.7 INVESTIGATIVE PROCEDURES

The initial investigation of a Civil Rights allegation shall be conducted as though it is to be prosecuted criminally. If CRD decides to initiate a criminal investigation, any administrative proceedings shall be suspended pending the outcome of the criminal investigation. If the CRD declines to proceed with a criminal investigation, the OIG may immediately initiate an administrative investigation or take whatever action is deemed appropriate.

The following investigative steps will be completed to the fullest extent possible in each civil rights investigation:

Medical Treatment:

If the victim is injured, the first task should be to get any necessary medical treatment. SAs should be cautioned that payment of medical costs by the OIG is not an authorized expense. Refer to Article IV of the Attorney General Guidelines for Victim and Witness Assistance for further guidance. (Chapter 20.4)

Photographs:

Observe, describe and photograph in color any complaint-related injuries visible on each victim at the time of the interview. It is very important to photograph the victim as soon as possible after the incident occurs. If the victim was photographed when he first made a complaint, obtain the photographs, the date and time they were taken, and the name and title of the person who took them.

If the victim's injuries are bandaged, determine whether the bandages can be removed so that the injuries can be photographed. If the bandages can be safely removed, photograph the uncovered injuries. Because of liability issues, only medical personnel should be employed to remove bandages. If the bandages cannot be safely removed, photograph the bandaged injuries.

If the victim is in custody of another agency and cannot be interviewed immediately by OIG, SAs should ask the other agency to photograph the victim. Photographs should be taken of the victim’s face to identify him, and any areas where the victim claimed to be injured.

Photographs should be taken of the injured area with the victim wearing whatever clothing he was wearing at the time of the incident. The clothing should then be removed, and photographs should be taken of the same area. If appropriate hold a

ruler next to the injury in some of the photographs to act as a scale. Record the date and time each photograph was taken, and who took them.

Arrangements should be made to re-photograph the victim in 24 hours, even if there are no visible marks. This will reveal the presence or absence of any bruising. If possible, preserve any clothing that covered the injured area as evidence. This is especially important if the skin was broken.

If the victim was not photographed at the time he first complained, the victim should be photographed as soon as possible thereafter, even if there are no visible marks. It is just as important to document the absence of an injury.

Interview of the alleged victim.

If the alleged victim is medically cleared to be interviewed, then he/she should be interviewed as soon as possible. If the victim is in custody, all necessary legal precautions should be taken before interviewing him/her. Determine the particulars of the allegation and the DHS employee's involvement.

If it appears the situation would likely meet guidelines to be prosecuted criminally, an affidavit, taken under oath, should be taken during this initial interview only after consultation with an AUSA. If, however, the case is unlikely to meet such guidelines, the agent should take an affidavit for possible use in administrative proceedings by the employee's component. If medical treatment was received, obtain a signed "Release of Medical Information" INV Form 5, at the time of the interview. **(Exhibits 19-1 or 19-2)**

Agents may provide direction to assault victims for filing a police report. (Chapter 20.4)

Interview of witnesses

Interview witnesses whose identities are furnished by the alleged victim or are obtained in police or other reports of the incident.

Identify and interview the subject(s) alleged by the victim(s) to have violated his/her civil rights.

Medical Evidence

Obtain copies of any medical records relating to treatment received by each victim for injuries allegedly sustained at the hands of the subject. The medical release obtained from the victim will be needed for such copies. If treatment was received at a hospital and it is determined later that the original records are required, identify the appropriate individual to receive a subpoena.

Identify and interview all physicians and other medical and paramedical personnel who treated each victim for injuries allegedly sustained at the hands of the subject; including the ambulance attendants who treated the victim. The medical release will be needed for such interviews. In the interviews with physicians and other medical personnel, determine the following information:

How severe were the victim's injuries;

What statements were made by the victim concerning how the injuries were received;

What statements were made to them by arresting officers as to how the victim's injuries were sustained or whether they heard any conversations between the officers about the incident;

Is it possible the injuries occurred the way the victim claimed they were received;

Did the victim appear to be intoxicated or under the influence of drugs; if so, were any alcohol or drug screens done, and;

Was the victim belligerent or in any way disorderly?

Collection of Other Evidence and Records:

Describe the scene of the incident; where appropriate, and supplement the description with photographs and diagrams.

Package, mark, and preserve any physical evidence obtained for submission to a forensics laboratory for examination if deemed appropriate. Obtain and photograph any objects that might have been used to injure the victim (flashlight, gun, baton, etc.). Establish a chain of custody for each item. Obtain copies of all reports or memoranda relevant to the incident. Investigating agents should be aware that if management compels an employee to submit a memorandum,
that may be considered Garrity material which cannot be used against an employee in a criminal prosecution. Accordingly, great care must be taken to determine the circumstances under which a subject officer's report was written prior to reviewing the report. If there is any question about a report being Garrity material, do not look at the report. Have someone from the contributing agency put a copy of the report in a sealed envelope. Label the envelope with the date and author of the report, and "Possible Garrity material." Consult with CRD or the AUSA on how to handle the report.

Review the Official Personnel File (OPF) of the subject(s) for information that may be relevant
to the incident. Agents are again cautioned that personnel files need to be reviewed for Garrity material prior to being examined for substantive information.

Obtain copies of any previous arrest reports and/or criminal history record of the victim.

Obtain copies of all agency logs and any audio and video recordings that are relevant to the incident.

Describe the scene of the incident; where appropriate, and supplement the description with photographs and diagrams.

CHAPTER 19 - EXHIBITS

19-1 INV Form 5, Release of Medical Information.

19-2 INV Form 5(S), Release of Medical Information (Spanish version).

Exhibit 19-1, INV Form 5, Release of Medical Information

Office of Inspector General - Investigations
U.S. Department of Homeland Security

AUTHORITY FOR RELEASE OF MEDICAL INFORMATION

Homeland Security

AUTHORITY FOR RELEASE OF MEDICAL INFORMATION

To Whom It May Concern

I hereby authorize any Special Agent of the Department of Homeland Security, Office of the Inspector General (OIG), bearing this release, or a copy thereof, within one year of its date, to obtain any information from any physician or other person who has attended, examined, or treated me, or from any clinic, hospital, instruction, company, or Federal, state, or municipal agency, office or bureau which may have information concerning my medical history. I also authorize the release of psychiatric, medicine, and alcohol records that are contained in my medical files. I hereby direct you to release such information directly to the bearer of this authorization. I understand that the information released is for official use by the OIG and, pursuant to the Inspector General Act of 1978 (Public Law 95-452) may be disclosed to such third parties as necessary in the fulfillment of the OIG's responsibilities.

I hereby release any individual, including record custodians, from any and all liability for damages of whatever kind or nature which may at any time result to me on account of compliance, or any attempts to comply, with this authorization. Should there be any question as to the validity of this release, you may contact me as indicated below.

Signature *(Full Name)* _____

Full Name *(Printed)* _____

Other Names Used _____

Date _____

Current Address _____

_____

_____

Telephone Number _____

INV FORM-05

Exhibit 19-2, INV Form 5S, Release of Medical Information (Spanish)

Oficina del Inspector General – Investigations
Departamento de Seguridad De La Patria

Homeland Security

AUTORIZACION PARA LA ENTREGA DE INFORMACION MEDICA

AUTORIZACION PARA LA ENTREGA DE INFORMACION MEDICA

A Quien Pueda Interesar:

Por la presente autorizo a cualquier Agente Especial del Departamento de Seguridad De La Patria, Oficina del Inspector General (OIG), portador de esta autorización, o de una copia de la misma, en el plazo de un año a partir de su fecha, para que obtenga cualquier dato de cualquier medico u otra persona que me haya asistido, examinado o tratado, o de cualquier clínica, hospital, academia, empresa, u organismo, oficina o departamento federal, estatal o municipal que pueda tener información concerniente a mis antecedentes médicos. Asimismo, autorizo la entrega de las constancias psiquiátricas, medicas y de bebidas alcohólicas que figuren en mis antecedentes médicos. Por la presente ordeno que entregue dicha información al portador de esta autorización. Tengo entendido que la información entregada será utilizada de manera oficial por la Oficina del Inspector General y, de conformidad con la Ley del Inspector General de 1978 (Ley Publica 95-452), puede ser entregada a terceros en la medida en que sea necesario para el cumplimiento de las funciones de la Oficina del Inspector General.

Por la presente eximo a toda persona, incluidos los custodios de las constancias, de toda responsabilidad por los perjuicios de cualquier clase o naturaleza que en cualquier momento pueda causarme el cumplimiento o cualquier tentativa de cumplimiento de esta autorización. En caso de que haya dudas acerca de la validez de esta autorización, se puede comunicar conmigo según se indica a continuación.

Firma *(nombre completo)* _____

Nombre completo *(con letra de imprenta)* _____

Otros nombres utilizados _____

Fecha _____

Dirección actual _____

_____

_____

Número de teléfono _____

INV FORM-05S

20.0 VICTIM AND WITNESS ASSISTANCE PROGRAM

20.1 OVERVIEW OF VICTIM AND WITNESS ASSISTANCE PROGRAM

All INV criminal investigator personnel must be aware of OIG procedures when responding to the needs of crime victims and witnesses.

These procedures have been established to ensure conformance with *the Victims' Rights and Restitution Act of 1990, as amended (VRRA), 42 U.S.C. § 10607, and the Crime Victims' Rights Act, as amended (CVRA), 18 U.S.C. § 3771,* and other applicable laws as well as the Attorney General Guidelines for Victim and Witness Assistance (AG Guidelines).

The Attorney General developed and implemented guidelines for the Department of Justice, consistent with the various federal victim's rights statutes beginning with the *Victim and Witness Protection Act of 1992*. These are to be followed in the treatment of victims and witnesses to crime by officers and employees of the Department of Justice engaged in investigative, prosecutorial, correctional or parole functions within the criminal justice system. The AG Guidelines are also intended to serve as a model for guidelines on the fair treatment of crime victims and witnesses by other Federal law enforcement agencies. The AG guidelines are periodically updated by the Department of Justice's Office of Justice Programs, Office for Victims of Crime. The AG Guidelines were revised in October 2011 and are available at **www.ojp.usdoj.gov/ovc**.

The guidelines are intended to apply in all cases when individual victims are adversely affected by criminal conduct or in which witnesses provide information regarding criminal activity. The guidelines do not apply to individuals who are culpable for or accused of the crime being investigated or prosecuted.

20.2 VICTIM AND WITNESS PROTECTION POLICY

All victims and witnesses of federal crimes who have suffered physical, financial, and/or emotional harm shall receive the rights and services to which they are entitled under the law. A victim is covered by the following "Bill of Rights" codified in 18 U.S.C. § 3771(a):

> The right to be treated with fairness and with respect for dignity and privacy.
>
> The right to be reasonably protected from the accused offender.
>
> The right to reasonable, accurate, and timely notice of court proceedings and parole proceedings involving the crime or of any release or escape of the accused.

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

The reasonable right to confer with the attorney(s) for the government in the case.

The right to full and timely restitution as provided by law.

The right to be reasonably heard at any public proceeding in district court involving release, plea, sentencing, or any parole proceeding.

The right to proceedings free from unreasonable delay.

20.3 VICTIM AND WITNESS DEFINITIONS

A. Victim

A person that has suffered direct physical, emotional, or pecuniary harm as a result of the commission of a crime, including in the case of a victim that is an institutional entity, an authorized representative of the entity. Neither the Federal government nor any state, local, tribal, or foreign government or agency falls within the definition of crime victim for mandatory services or enforceable rights; however, they may qualify for restitution. Even if a particular person does not qualify as a victim under the law or AG Guidelines, in their discretion OIG personnel may provide services, such as referrals or notices, as they deem appropriate.

B. Witness

A person who has information or evidence concerning a crime, and provides information regarding his/her knowledge to a law enforcement agency. Where the witness is a minor, the term "witness" includes an appropriate family member or legal guardian. The term "witness" does not include a defense witness or an individual involved in the crime as a perpetrator or accomplice.

C. Victim Witness Coordinator (VWC)

The person in the OIG and U.S. Attorney's offices assigned as the point of contact with the victims and witnesses and the liaison with law enforcement agencies. Each U.S. Attorney's office has a designated VWC. Contact with the U.S. Attorney's VWC is encouraged, as it might be useful in the discharge of the responsibilities described in this chapter.

D. Emotional Harm

The term emotional harm means harm to a person's psychological or intellectual functioning which may be exhibited by severe anxiety, depression, withdrawal or outward aggressive behavior, or a combination of these behaviors, which may be demonstrated by a change in behavior, emotional response, or cognition.

E. Financial Harm

The term financial or pecuniary harm shall not be defined or limited by a dollar amount, and the degree of assistance must be determined on a case-by-case basis.

20.4 RESPONSIBILITIES

The AIGI is responsible for developing policies and procedures to assure the proper exercise of law enforcement authority by SAs in identifying the victims and witnesses of crime and providing the required rights and services.

The DAIGI Inspection Operations Division (IOD) is responsible for general oversight of compliance with this chapter through the National Victim Witness Coordinator (VWC) and the field office SACs.

A National VWC is established within IOD and is the SAC of the Financial Crimes Evaluation Unit. The National VWC will provide assistance to the field in carrying out the provisions of victims' rights and services laws and DHS OIG policy and will maintain liaison with the DOJ, Office of Justice Programs, Office of Victims of Crime and disseminate additional information as appropriate to field office VWCs. The National VWC will maintain a roster of the field cadre of VWCs.

SACs are responsible for ensuring that SAs comply with the INV policy and procedures when dealing with victims and witnesses of crime. SACs are to perform the following:

> Designate an SA in their office as a field office VWC to provide assistance to victims and/or witnesses.
>
> Establish internal procedures to ensure the proper oversight of providing services to victims and witnesses, tracking and recording the procedures used in providing these services, and training all office personnel in their victim/witness responsibilities under the law.

Case agents and/or field office VWCs are responsible for providing victims and witnesses information regarding the AG guidelines as outlined in a brochure on victims' rights. **(Exhibit 20-1)** SAs will document distribution of this brochure by preparing an MOA, a copy of which will be forwarded to the National VWC.

SAs have the responsibility of providing services and information to victims and witnesses of a crime until criminal proceedings are initiated by complaint, information, or indictment, at which time the responsibility shifts to the USAO VWC.

In the event intimidation and/or harassment of a victim/witness occurs, take immediate action to notify the AUSA and assist in making arrangements for the reasonable protection of the victim/witness.

SAs will provide the victim/witness with information regarding the status of the investigation (to the extent no compromises affecting the investigation will occur), the arrest of the individual, and developments and scheduling of court appearances.

Ensure that property of victims (held as evidence) is maintained in good condition and returned as quickly as possible.

Upon request of a victim/witness, notify the employer or creditor of the victim/witness of the cause of the victim's/witness's absence from work or nonpayment of debt.

Ensure that all information in the investigative file pertinent to the defendant's sentencing is brought to the attention of the AUSA handling the matter or the United States Probation Office (USPO). This information is needed for the preparation of the "Victim Impact Statement" portion of the pre-sentence report, which is presented to the presiding federal judge.

Providing all victim/witness information to the VWC at the local USAO after the case has been officially accepted by the DOJ.

SAs shall perform the following:

> Identify victims/witnesses and inform them of their right to receive services mandated by law at the earliest opportunity at which it may be done without interfering with an investigation and distribute the pamphlet entitled "OIG Victims and Witnesses of Crime" [which should include notification to victims of their right to receive, on request, the services listed in 42 U.S.C. § 10607(c) as well as the name, title, and address and telephone number of the VWC to whom a request for such service should be addressed].
>
> Refer victims/witnesses for medical or social services as needed.
>
> Ensure that victims/witnesses routinely receive information concerning the prohibition against intimidation and harassment, and the appropriate remedies available. Immediately notify the office SAC and VWC concerning instances of threat, intimidation, or harassment of any victim or witness.

When interviewing a victim or witness at his or her place of employment or in other public areas, explain (if so requested) to the employer the status of the individual as a victim or witness and the necessity for conducting the interview at that time.

Provide the victim the earliest possible notice of the status of the investigation of the crime, to the extent it is appropriate to inform the victim and will not interfere with the investigation, the arrest, or filing of charges against a suspected offender.

Assist the VWC from the OIG field office, the Victim Witness Coordinator in the U.S. Attorney's Office, and the AUSA as necessary in carrying out the provisions of law regarding victims and witnesses.

Ensure that any property of a victim that is being held for evidentiary purposes be maintained in good condition and returned to the victim as soon as it is no longer needed for evidentiary purposes.

Document all contacts with victims or witnesses and maintain the record in the official case file.

Prior to filing of criminal charges, provide the responsible prosecuting official with a list containing the names of and available contact information for known victims and witnesses.

Reporting Suspected Child Abuse

State child abuse reporting laws determine the scope of the reporting obligation in cases of suspected child abuse and vary substantially by state. SAs are responsible for knowing, understanding, and complying with obligations in the states in which they work. Reports of suspected child abuse required by state or local law will be made to the agency or entity identified in that law.

The federal child abuse reporting law requires certain professionals, including law enforcement personnel, working on federal land or in a federally operated or contracted facility in which children are cared for or reside, to report suspected child abuse to an investigative agency designated by the Attorney General to receive and investigate such reports. 42 U.S.C. § 13031(a). The Attorney General has directed that such reports be made to the local law enforcement agency or local child protective services agency that has jurisdiction to investigate reports of child abuse or to protect child abuse victims in the area or facility in question. When no such agency has entered into a formal written agreement with the Attorney General to investigate such reports, the FBI shall receive and investigate such reports. 28 CFR § 81.3. Failing to timely report shall be fined or imprisoned not more than one year or both.

Reporting child abuse in Indian country is governed by 18 U.S.C. § 1169 and 25 U.S.C. § 3203. SAs shall report suspected cases of child abuse to the federal, state, or tribal agency with primary responsibility for child protection or investigation of child abuse within the Indian country involved. If the report involves a potential crime and either

involves an Indian child or an Indian suspect, the local law enforcement agency is required to make an immediate report to the FBI.

Reporting of suspected child abuse will be documented on an MOA and retained in the case file. A copy of the MOA will be forwarded to the National VWC.

Information Disclosure

Disclosure laws, including the Privacy Act, define the information that may be disclosed regarding an ongoing investigation. No information should be provided about the status of an open investigation if it could reveal investigative techniques and procedures or otherwise interfere with the progress of an investigation. When any information about the progress of an investigation is disclosed to a victim or witness, such information should be limited to general information regarding the progress and projected duration of the investigation, and not consist of any information regarding the facts developed. Information regarding the estimated time or completion of an investigation can be provided. A victim or witness also may be informed of a decision not to seek an indictment or otherwise commence prosecution. The consideration that shaped a prosecution or declination should never be disclosed except by the prosecutor.

20.5 CONFIDENTIAL INFORMANTS (CI)

No action should be taken pursuant to this chapter that could jeopardize the safety of a CI or compromise their identity. (Chapter 11.1)

20.6 VICTIM OR WITNESS VISAS

Several types of visas may be useful in ensuring that aliens are available to aid in successful investigations or prosecutions.

The U Visa was created to strengthen the ability of law enforcement agencies to investigate and prosecute cases of domestic violence, sexual assault, trafficking of aliens and other crimes while offering protection to victims of such crimes (Victims of Trafficking and Violence Protection Act) who are willing to assist in the investigation or prosecution of the criminal activity. The U Visa provides a mechanism for the alien to remain in the U.S. or to return to the U.S. from their country of origin to assist in an investigation of those who have perpetrated a crime against them.

The program is generally utilized for aliens who have entered the U.S. legally but are subject to deportation due to expiration or cancelation of their entry visas. An alien identified as a possible victim eligible for the U Visa is not subject to removal from the U.S. until he or she has the opportunity to avail themselves of the provisions of this program.

Four following conditions must be satisfied to classify an alien as a U Visa nonimmigrant:

1. The alien has suffered substantial physical or mental abuse as a result of having been a victim of certain criminal activity.

2. The alien possesses information concerning the above criminal activity.

3. The alien has been helpful or is likely to be helpful to law enforcement officials investigating or prosecuting the criminal activities.

4. The criminal activity violated the laws of the U.S. or occurred within the U.S. See Exhibit 20-2 for a list of qualifying criminal activity.

U Visa applications are submitted to U.S. Citizenship and Immigration Services (CIS), Vermont Service Center for their review and approval. The U Visa Certification, CIS Form I-918, Supplement B is mandatory and is to be completed by the requesting Field Office and submitted to Headquarters for approval and signature by the AIGI. The alien petitioner or his representative will complete the I-918 Petition for U Nonimmigrant Status and the two forms will be submitted together to CIS for their review. The maximum length of time a U Visa can be issued for is four years.
(Exhibit 20-2)

The U Visa program differs from the parole system utilized by the agency which allows a cooperating illegal alien to remain in the country while assisting with the prosecution of a crime. The parole program, deferred action and stays of removal are most commonly used for an undocumented alien who has illegally entered the U.S. and needs to remain in country to assist in the investigation or prosecution of an OIG investigation. Parole applications are approved by Immigration and Customs Enforcement (ICE).

The S-5 visa is available for alien witnesses or informants who supply critical, reliable information concerning a criminal organization or enterprise and whose presence in the U.S. is required for the successful investigation or prosecution of the criminal organization. The witness or informant may be admitted for three years and this status may not be extended. Form I-854 must be submitted.

Victims of severe forms of human trafficking, defined at 22 U.S.C. § 7102, who are already physically present in the U.S. may remain in the U.S. to assist in investigations or prosecutions of human trafficking violators under a nonimmigrant T visa. Principal T visas are limited to 5000 per year.

20.7 VICTIM AND WITNESS AWARENESS TRAINING

SAs who attend CITP at FLETC receive training in Victim and Witness Awareness. DHS does not coordinate additional VWC training for Organizational Elements. VWCs should avail themselves of any periodic training as provided by the local USAO.

SACs will periodically review victim/witness requirements during office training.

20.8 REPORTING REQUIREMENTS

By the 5th day after the end of each quarter of the calendar year, the VWC will provide a report concerning victim witness assistance to the National VWC. Negative responses are not required.

CHAPTER 20.0 - EXHIBITS

U.S. Department of Homeland Security

Victim and Witness Assistance Program

U.S. Department of Homeland Security Office of Inspector General

IMPORTANT CONTACT NUMBERS

OIG SPECIAL AGENT

_____
Name

_____
Phone

OIG VICTIM/WITNESS COORDINATOR

_____
Name

_____
Phone

U.S. ATTORNEY
VICTIM/WITNESS COORDINATOR

_____
Name

_____
Phone

ADDITIONAL PROGRAMS

_____

_____

TO REPORT FRAUD, WASTE, AND MISMANAGEMENT

HOMELAND SECURITY OIG HOTLINE
1-800-323-8603

THE EMOTIONAL IMPACT OF CRIME

Many victims and witnesses are emotionally affected by crime. Although everyone reacts differently, victims and witnesses report some common behaviors, such as:

- Anger.
- Feelings of panic and anxiety.
- Increased concern for their personal safety and that of their family.
- Nightmares and a change in sleep patterns.
- Depression, difficulty in handling everyday problems, trouble concentrating, and feeling overwhelmed.
- Feelings of self-doubt, shame, and guilt.
- Reliving what happened.

Everyone copes with emergencies and tragedy differently and all of these responses are normal reactions to a very abnormal event. Many people continue to have these responses for some time after the crime. You may want to talk about what happened with a counselor, clergy member, friend, family member, or other victims. The OIG Victim/Witness Coordinator can assist you in finding appropriate support services.

We encourage you to contact the OIG Victim/Witness coordinator listed on the back page.

We are here to serve you.

INFORMATION FOR VICTIMS AND WITNESSES OF CRIME

As a Federal Law Enforcement agency, the U.S. Department of Homeland Security Office of Inspector General (OIG), is concerned about the problems often experienced by victims and witnesses of crime. We know that as a victim or witness you may experience anger, confusion, frustration or fear as a result of your experience.

This brochure provides information that will help you deal with the problems and questions that often surface during an investigation and to provide you with a better understanding of how the Federal criminal justice system works. We have included a description of victims' rights under Federal law, as well as information and services available to you as a federal victim and/or witness. We encourage you to contact your OIG Victim/Witness Coordinator if you have any questions. The coordinator's name and number are on the back of this brochure.

We know that days and months ahead may be difficult for you and your family. We hope the resources described in this brochure can help you. At the same time, we need your cooperation throughout the investigation, your OIG Victim/Witness Coordinator is the person you should contact.

IF YOU ARE THREATENED OR HARASSED

If anyone threatens you or you feel that you are being harassed because of your cooperation with the investigation, contact your OIG Victim/Witness Coordinator immediately. He/She is available to discuss additional protective measures, which can be taken, if necessary.

IF YOUR PROPERTY WAS STOLEN

If your property was stolen, we hope to recover it as part of our investigation. If we do, we will notify you and make every effort to see that it is returned.

IF YOU NEED ASSISTANCE WITH YOUR EMPLOYER OR CREDITORS

During the course of the investigation, we will contact your employer if cooperation in the investigation causes absences from work and we will contact any creditors if cooperation in the investigation affects your ability to make timely payments.

IF YOU NEED FINANCIAL HELP OR SUPPORT SERVICES

States have crime victim compensation programs to help cover some expenses resulting from violent crimes. Your state program may pay for medical health care costs, lost wages and support, and funeral and burial expenses not covered by insurance other benefits. Contact your state compensation program to find out if you are eligible for benefits. For more information, contact the OIG Victim/Witness Coordinator.

The OIG Victim/Witness Coordinator can also tell you about available victim assistance programs. These programs offer a variety of services to help crime victims, such as crisis intervention, counseling, and emotional support.

IF AN ARREST IS MADE

If you request, you will be notified if a defendant is apprehended. Following the arrest, the OIG Victim/Witness Coordinator will make every effort to keep you informed of the status of your case.

(Cont.)

Once we have filed your case with the U.S. Attorney's Office, the Assistant U.S. Attorney assigned to handle your case will contact you. Each U.S. Attorney's Office has a Victim/Witness Coordinator to help answer your questions and deal with your concerns during the prosecution of your case.

YOUR RIGHTS AS A VICTIM

As a Federal crime victim you have the following rights:

- The right to be treated with fairness and with respect for your dignity and privacy.
- The right to be reasonably protected from the accused offender.
- The right to be notified of court proceedings.
- The right to be present at all public court proceedings related to the offense, unless the court determines that your testimony would be materially affected if you heard other testimony at trial.
- The right to confer with the attorney for the Government in the case.
- The right to restitution.
- The right to information about the conviction, sentencing, imprisonment, and release of the offender.

Victims who are children, or victims of sex offenses, domestic violence, or telemarketing crimes, have additional rights. For further information, contact your OIG Victim/Witness Coordinator.

Exhibit 20-2, Form I-918 Supplement B, U Nonimmigrant Status Certification

Office of Communications
U.S. Citizenship and Immigration Services

September 5, 2007

Fact Sheet

CERTIFYING U NONIMMIGRANT STATUS

U Nonimmigrant Status Certification (Form I-918, Supplement B)

An alien victim of criminal activity may file for U Nonimmigrant Status – status set aside for victims of crimes who have suffered substantial mental or physical abuse because of the activity and who also are willing to assist law enforcement agencies or government officials in the investigation of that activity.

In order to file for that status, the alien must provide a certification from a federal, state, or local law enforcement official certifying the following:

- The alien has been a victim of qualifying criminal activity;
- The alien possesses information about the qualifying criminal activity; and
- The alien has been, is being or is likely to be helpful to the investigation and/or prosecution of that qualifying criminal activity.

This certification must be executed using the U Nonimmigrant Status Certification (Form I-918, Supplement B). USCIS will give the certification significant weight during adjudication; however, it alone will not be the sole evidence that a petitioner meets eligibility requirements. USCIS will look at the totality of the circumstances surrounding the petition before rendering a decision.

It is important to note that a certifying agency is under no legal obligation to complete this certification. However, the alien petitioner will be ineligible for U nonimmigrant status without one. **The petitioner is responsible for filing the completed certification with his/her initial Petition for U Nonimmigrant Status (Form I-918).**

Certifications shall be prepared by the certifying agency and should provide specific details about the nature of the crime being investigated and/or prosecuted and describe the petitioner's helpfulness in the case. Form I-918 Supplement B must be prepared by a certifying agency, and signed by a qualifying official within six months immediately preceding the alien's submission of Form I-918.

U NONIMMIGRANT STATUS CERTIFICATION SPECIFICATIONS

Qualified certifying agencies include:

- Federal, State or local law enforcement agencies; or
- Other agencies that have criminal investigative jurisdiction in their respective areas of expertise such as child protective services, the Equal Opportunity Commission and the Department of Labor.

www.uscis.gov

Certifying officials include:

- The head of a qualifying certifying agency;
- Any person in a supervisory role in a qualifying agency who is specifically designated by the head of that agency to issue U nonimmigrant certifications; or
- Federal, State or local judges

Certification must contain an affirmation of the following:

- The official signing the certificate is authorized to do so;
- The agency is a federal, state, or local law enforcement agency, prosecutor, judge, or other authority having responsibility for the detection, investigation, prosecution, conviction, or sentencing of a qualifying criminal activity;
- The petitioner has been a victim of a qualifying criminal activity;
- The petitioner possesses information regarding that activity;
- The petitioner has been, is being, or will likely be helpful to the investigation; and
- The criminal activity violated U.S. law, or occurred within the United States, or its territories and possessions.

Qualifying criminal activity includes:

Abduction	Incest	Rape
Abusive Sexual Contact	Involuntary Servitude	Sexual Assault
Blackmail	Kidnapping	Sexual Exploitation
Domestic Violence	Manslaughter	Slave Trade
Extortion	Murder	Torture
False Imprisonment	Obstruction of Justice	Trafficking
Felonious Assault	Peonage	Unlawful Criminal Restraint
Female Genital Mutilation	Perjury	Witness Tampering
Hostage	Prostitution	Other Related Crimes

Note: Certifying agencies must notify USCIS in writing if, at any time, the petitioner unreasonably refuses to assist in the investigation of the criminal activity, or if the agency wishes to withdraw its certification for any other reason. Send that notice (including the alien's name, date of birth and A-file number (if available) along with the reason for the withdrawal of the certification to:

U.S. Citizenship and Immigration Services
Vermont Service Center—U-visa Unit
75 Lower Welden St.
St. Albans, Vermont 05479-0001

Page 2

OMB No. 1615-0104; Expires 08/31/2010

Department of Homeland Security
U.S. Citizenship and Immigration Services

Instructions for I-918, Supplement B, U Nonimmigrant Status Certification

Instructions

Please read these instructions carefully to properly complete this form. If you need more space to complete an answer, use a separate sheet(s) of paper. Write your name and Alien Registration Number (A #), if any, at the top of each sheet of paper and indicate the part and number of the item to which the answer refers.

What Is the Purpose of This Form?

You should use Form I-918, Supplement B, to certify that an individual submitting a Form I-918, Petition for U Nonimmigrant Status, is a victim of certain qualifying criminal activity and is, has been, or is likely to be helpful in the investigation or prosection of that activity.

When Should I Use Form I-918, Supplement B?

If you, the certifying official, determine that this individual (better known as the petitioner) is, has been, or is likely to be helpful in your investigation or prosecution, you may complete this supplement form. The **petitioner** must then submit the supplement to USCIS with his or her petition for U nonimmigrant status.

NOTE: An agency's decision to provide a certification is entirely discretionary; the agency is under no legal obligation to complete a Form I-918, Supplement B, for any particular alien. However, without a completed Form I-918, Supplement B, the alien will be ineligible for U nonimmigrant status.

To be eligible for U nonimmigrant status, the alien must be a victim of qualifying criminal activity. The term "victim" generally means an alien who has suffered direct and proximate harm as a result of the commission of qualifying criminal activity.

The alien spouse, unmarried children under 21 years of age and, if the victim is under 21 years of age, parents and unmarried siblings under 18 years of age, will be considered victims of qualifying criminal activity where:

1. The direct victim is deceased due to murder or manslaughter, or
2. Where a violent qualifying criminal activity has caused the direct victim physical harm of a kind and degree that makes the direct victim incompetent or incapacitated, and, therefore, unable to provide information concerning the criminal activity or to be helpful in the investigation or prosecution of the criminal activity.

An alien may be considered a victim of witness tampering, obstruction of justice, or perjury, including any attempt, conspiracy, or solicitation to commit one or more of those offenses if:

1. The victim has been directly and proximately harmed by the perpetrator of the witness tampering, obstruction of justice, or perjury; **and**
2. There are reasonable grounds to conclude that the perpetrator committed the witness tampering, obstruction of justice, or perjury offense, at least in principal part, as a means:
   - **A.** To avoid or frustrate efforts to investigate, arrest, prosecute, or otherwise bring to justice the perpetrator for other criminal activity; or
   - **B.** To further the perpetrator's abuse or exploitation of or undue control over the petitioner through manipulation of the legal system.

A person who is culpable for the qualifying criminal activity being investigated or prosecuted is excluded from being recognized as a victim.

A victim of qualifying criminal activity must provide evidence that he or she (or in the case of an alien under the age of 16 years or who is incapacitated or incompetent, the parent, guardian, or next friend of the alien) has been, is being, or is likely to be helpful to a certifying official in the investigation or prosecution of the qualifying criminal activity as listed in **Part 3** of this form. Being "helpful" means assisting law enforcement authorities in the investigation or prosecution of the qualifying criminal activity of which he or she is a victim.

General Instructions

Fill Out the Form I-918, Supplement B

1. Type or print legibly in black ink.
2. If extra space is needed to complete any item, attach a continuation sheet, indicate the item number, and date and sign each sheet.

3. Answer all questions fully and accurately. State that an item is not applicable with "N/A." If the answer is none, write "none."

This form is divided into **Parts 1** through 7. The following information should help you fill out the form.

Part 1 - Victim information.

A. **Family Name** (Last Name) - Give victim's legal name.

B. **Given Name** (First name) - Give victim's full first name, do not use "nicknames." (Example: If victim's name is Albert, do not use Al.)

C. **Other Names Used** - Provide all the names the victim has used that you are aware of, including maiden name if applicable, married names, nicknames, etc.

D. **Date of Birth** - Use eight numbers to show his or her date of birth (example: May 1, 1979, should be written 05/01/1979).

E. **Gender** - Check the appropriate box.

Part 2 - Agency information.

A. **Name of certifying agency** - The certifying agency must be a Federal, State, or local law enforcement agency, prosecutor, or authority, or Federal or State judge, that has responsibility for the investigation or prosecution, conviction or sentencing of the qualifying criminal activity of which the petitioner was a victim.

This includes traditional law enforcement branches within the criminal justice system, and other agencies that have criminal investigative jurisdiction in their respective areas of expertise, such as the child protective services, Equal Employment Opportunity Commission, and Department of Labor.

B. **Name of certifying official** - A certifying official is:

1. The head of the certifying agency or any person in a supervisory role, who has been specifically designated by the head of the certifying agency to issue a U Nonimmigrant Status Certification on behalf of that agency; **or**

2. A Federal, state or local judge.

If the certification is not signed by the head of the certifying agency, please attach evidence of the agency head's written designation of the certifying official for this specific purpose.

C. **Agency address** - Give the agency's mailing address.

Part 3 - Criminal acts.

A. **Check all of the crimes of which the petitioner is a victim that your agency is investigating, prosecuting, or sentencing** - If the crime(s) of which the petitioner is a victim is not listed, please list the crime(s) and provide a written explanation regarding how it is similar to one of the listed crimes. Similar activity refers to criminal offenses in which the nature and elements of the offenses are substantially similar to the list of criminal activity found on the certification form itself.

B. **Indicate whether the qualifying criminal activity violated the laws of the United States or occurred within the United States (including in Indian country and military installations) or the territories and possessions of the United States** - Qualifying criminal activity of which the applicant is a victim had to violate U.S. law or occur within the United States.

Please indicate whether the qualifying criminal activity occurred within the United States (including in Indian country and military installations) or the territories and possessions of the United States.

1. **United States** means the continental United States, Alaska, Hawaii, Puerto Rico, Guam, and the U.S. Virgin Islands.

2. **Indian country** refers to all land within the limits of any Indian reservation under the jurisdiction of the United States Government, notwithstanding the issuance of any patent, and including rights-of-way running through the reservation; all dependent Indian communities within the borders of the United States whether within the original or subsequently acquired territory thereof, and whether within or without the limits of a state; and all Indian allotments, the Indian titles to which have not been extinguished, including rights-of-way running through such allotments.

3. **Military installation** means any facility, base, camp, post, encampment, station, yard, center, port, aircraft, vehicle, or vessel under the jurisdiction of the Department of Defense, including any leased facility, or any other location under military control.

4. **Territories and possessions of the United States** means American Samoa, Bajo Nuevo (the Petrel Islands), Baker Island, Howland Island, Jarvis Island, Johnston Atoll, Kingman Reef, Midway Atoll, Navassa Island, Northern Mariana Islands, Palmyra Atoll, Serranilla Bank, and Wake Atoll.

If the qualifying criminal activity did not occur within the United States as discussed above, but was in violation of U.S. law, it must violate a Federal extraterritorial jurisdiction statute. There is no requirement that a prosecution actually occur. Please provide the statutory citation for the extraterritorial jurisdiction.

Part 4 - Helpfulness of the victim.

A. **Indicate whether the victim possesses information about the crime(s).** A petitioner must be in possession of information about the qualifying criminal activity of which he or she is a victim. A petitioner is considered to possess information concerning qualifying criminal activity of which he or she is a victim if he or she has knowledge of details concerning that criminal activity that would assist in the investigation or prosecution of the criminal activity. Victims with information about a cime of which they are not the victim will not be considered to possess information concerning qualifying criminal activities.

When the victim is under 16 years of age, incapacitated or incompetent, he or she is not required to personally possess information regarding the qualifying criminal activity. The parent, guardian, or "next friend" of the minor petitioner may provide that information. "Next friend" is a person who appears in a lawsuit to act for the benefit of an alien victim. The "next friend" is not a party to the legal proceeding and is not appointed as a guardian.

B. **Provide an explanation of the victim's helpfulness to the investigation or prosecution of the criminal activity.** A victim must provide evidence to USCIS that he or she (or, in the case of an alien child under the age of 16 or who is incapacitated or incompetent, the parent, guardian, or next friend of the alien) has been, is being, or is likely to be helpful to a certifying law enforcement official in the investigation or prosecution of the qualifying criminal activity.

Being "helpful" means assisting law enforcement authorities in the investigation or prosecution of the qualifying criminal activity of which he or she is a victim. Alien victims who, after initiating cooperation, refuse to provide continuing assistance when needed will not meet the helpfulness requirement. There is an ongoing responsibility on the part of the victim to be helpful, assuming there is an ongoing need for the victim's assistance.

You, the certifying official, will make the initial determination as to the helpfulness of the petitioner. USCIS will give a properly executed Supplement B, U Nonimmigrant Status Certification significant weight, but it will not be considered conclusory evidence that the victim has met the eligibility requirements. USCIS will look at the totality of the circumstances surrounding the alien's involvement with your agency and all other information known to USCIS in determining whether the alien meets the elements of eligibility.

Part 5 - Family members implicated in criminal activity.

List whether any of the victim's family members are believed to have been involved in the criminal activity of which he or she is a victim. An alien victim is prohibited from petitioning for derivative U nonimmigrant status on behalf of a qualifying family member who committed battery or extreme cruelty or trafficking against the alien victim which established his or her eligibility for U nonimmigrant status. Therefore, USCIS will not grant an immigration benefit to a qualifying family member who committed qualifying criminal activities in a family violence of trafficking context.

Part 6 - Certification.

Please read the certification block carefully. **NOTE:** If the victim unreasonably refuses to assist in the investigation or prosecution of the qualifying criminal activity of which he or she is a victim, even after this form is submitted to USCIS, you **must** notify USCIS by sending a written statement to: USCIS - Vermont Service Center, 75 Lower Welden Street, St. Albans, VT 05479-0001. Please include the victim's name, date of birth, and A-number (if available) on all correspondence.

OMB No. 1615-0104; Expires 08/31/2010

Department of Homeland Security
U.S. Citizenship and Immigration Services

I-918 Supplement B, U Nonimmigrant Status Certification

START HERE - Please type or print in black ink.

For USCIS Use Only.

Returned	Receipt
Date	
Date	
Resubmitted	
Date	
Date	
Reloc Sent	
Date	
Date	
Reloc Rec'd	
Date	
Date	

Remarks

Part 1. Victim information.

Family Name | Given Name | Middle Name

Other Names Used *(Include maiden name/nickname)*

Date of Birth *(mm/dd/yyyy)*

Gender ☐ Male ☐ Female

Part 2. Agency information.

Name of Certifying Agency

Name of Certifying Official | Title and Division/Office of Certifying Official

Name of Head of Certifying Agency

Agency Address - Street Number and Name | Suite #

City | State/Province | Zip/Postal Code

Daytime Phone # *(with area code and/or extension)* | Fax # *(with area code)*

Agency Type
☐ Federal ☐ State ☐ Local

Case Status
☐ On-going ☐ Completed ☐ Other _____

Certifying Agency Category
☐ Judge ☐ Law Enforcement ☐ Prosecutor ☐ Other _____

Case Number | FBI # or SID # *(if applicable)*

Part 3. Criminal acts.

1. The applicant is a victim of criminal activity involving or similar to violations of one of the following Federal, State or local criminal offenses. *(Check all that apply.)*

☐ Abduction	☐ Female Genital Mutilation	☐ Obstruction of Justice	☐ Slave Trade
☐ Abusive Sexual Contact	☐ Hostage	☐ Peonage	☐ Torture
☐ Blackmail	☐ Incest	☐ Perjury	☐ Trafficking
☐ Domestic Violence	☐ Involuntary Servitude	☐ Prostitution	☐ Unlawful Criminal Restraint
☐ Extortion	☐ Kidnapping	☐ Rape	☐ Witness Tampering
☐ False Imprisonment	☐ Manslaughter	☐ Sexual Assault	☐ Related Crime(s)
☐ Felonious Assault	☐ Murder	☐ Sexual Exploitation	☐ Other: *(If more space needed, attach seperate sheet of paper.)*
☐ Attempt to commit any of the named crimes	☐ Conspiracy to commit any of the named crimes	☐ Solicitation to commit any of the named crimes	

Form I-918 Supplement B (08/31/07)

Part 3. Criminal acts. *(Continued.)*

2. Provide the date(s) on which the criminal activity occurred.
   Date *(mm/dd/yyyy)* | Date *(mm/dd/yyyy)* | Date *(mm/dd/yyyy)* | Date *(mm/dd/yyyy)*

3. List the statutory citation(s) for the criminal activity being investigated or prosecuted, or that was investigated or prosecuted.

4. Did the criminal activity occur in the United States, including Indian country and military installations, or the territories or possessions of the United States? ☐ Yes ☐ No

   a. Did the criminal activity violate a Federal extraterritorial jurisdiction statute? ☐ Yes ☐ No

   b. If "Yes," provide the statutory citation providing the authority for extraterritorial jurisdiction.

   c. Where did the criminal activity occur?

5. Briefly describe the criminal activity being investigated and/or prosecuted and the involvement of the individual named in Part 1. Attach copies of all relevant reports and findings.

6. Provide a description of any known or documented injury to the victim. Attach copies of all relevant reports and findings.

Part 4. Helpfulness of the victim.

The victim (or parent, guardian or next friend, if the victim is under the age of 16, incompetent or incapacitated.):

1. Possesses information concerning the criminal activity listed in **Part 3.** ☐ Yes ☐ No
2. Has been, is being or is likely to be helpful in the investigation and/or prosecution of the criminal activity detailed above. *(Attach an explanation briefly detailing the assistance the victim has provided.)* ☐ Yes ☐ No
3. Has not been requested to provide further assistance in the investigation and/or prosecution. *(Example: prosecution is barred by the statute of limitation.) (Attach an explanation.)* ☐ Yes ☐ No
4. Has unreasonably refused to provide assistance in a criminal investigation and/or prosecution of the crime detailed above. *(Attach an explanation.)* ☐ Yes ☐ No

Form I-918 Supplement B (08/31/07) Page 2

Part 4. Helpfulness of the victim. *(Continued.)*

5. Other, please specify.

Part 5. Family members implicated in criminal activity.

1. Are any of the victim's family members believed to have been involved in the criminal activity of which he or she is a victim? ☐ Yes ☐ No

2. If "Yes," list relative(s) and criminal involvement. *(Attach extra reports or extra sheet(s) of paper if necessary.)*

Full Name	Relationship	Involvement

Part 6. Certification.

I am the head of the agency listed in **Part 2** or I am the person in the agency who has been specifically designated by the head of the agency to issue U nonimmigrant status certification on behalf of the agency. Based upon investigation of the facts, I certify, under penalty of perjury, that the individual noted in **Part 1** is or has been a victim of one or more of the crimes listed in **Part 3**. I certify that the above information is true and correct to the best of my knowledge, and that I have made, and will make no promises regarding the above victim's ability to obtain a visa from the U.S. Citizenship and Immigration Services, based upon this certification. I further certify that if the victim unreasonably refuses to assist in the investigation or prosecution of the qualifying criminal activity of which he/she is a victim, I will notify USCIS.

Signature of Certifying Official Identified in Part 2. **Date** *(mm/dd/yyyy)*

Form I-918 Supplement B (08/31/07) Page 3

21.0 INFORMATION DISCLOSURE

21.1 GENERAL

Agents must maintain materials in investigative files with an understanding that documents may be subject to disclosure to subjects and witnesses in investigations, the public, and Congress. It is critical to place in INV files only information that is accurate, timely, and relevant to the matter under investigation.

21.2 LITIGATION-RELATED REQUESTS FOR TESTIMONY OR DOCUMENTS

An INV employee may be requested or subpoenaed to provide testimony or documents in a deposition, trial, or other similar proceeding, relative to information the employee may have acquired in the course of performing official duties or because of the employee's official capacity.

In accordance with regulations at 6 C.F.R. Part 5, Subpart C, INV employees may not provide testimony or produce documents in third party litigation unless specifically authorized to do so. An INV employee who receives any request to provide documents or recorded testimony will notify the managing SAC/ASAC who will forward the request to Counsel to the Inspector General for resolution. The SAC/ASAC will notify the DAIGI--Field Operations.

This does not apply to requests from Department of Justice attorneys representing the United States, its agencies, officers, or employees, or to Federal, state, local, or foreign prosecuting and law enforcement authorities in connection with criminal law enforcement investigations, prosecutions, or other proceedings.

21.3 REQUESTS FOR ACCESS TO INVESTIGATIVE RECORDS

The primary means for third parties to obtain access to INV files are via the Freedom of Information Act (FOIA), 5 U.S.C. § 552, and the Privacy Act (PA), 5 U.S.C. § 522a.

FOIA provides that any person has a right to obtain access to federal agency records unless they are protected from disclosure by exemption or law enforcement exclusion. The PA regulates the collection, maintenance, use and disclosure of personal information by federal agencies. Its purpose is to balance the government's need to maintain and share information about individuals with the rights of individuals against unwarranted invasions of their privacy. Counsel has primary responsibility for advising the OIG on records disclosure under FOIA and for responding to requests for information under FOIA and PA. All INV employees are responsible for ensuring that requests under these statutes for information in INV files are forwarded to Counsel to the Inspector General.

INV employees should not release records to the public without first consulting with Counsel to the Inspector General.

21.4 COORDINATION WITH OFFICE OF ENTERPRISE ARCHITECTURE (OEA)

When FOIA or PA requests pertain to INV documents, Counsel to the Inspector General will request a records search through OEA. If records responsive to the request exist in INV, OEA will forward a complete copy of the records to Counsel to the Inspector General.

Where the request is for records maintained in an INV investigative file, OEA must confirm the status of the investigation with the investigating field office. It is also essential to inform Counsel whether the case is before the grand jury, at trial, and any other details relating to its open status. It is INV policy not to release any records in connection with an investigation that is open and ongoing.

21.5 LOCATING RECORDS RESPONSIVE TO THE REQUEST

OEA will make every effort to locate and retrieve all INV records responsive to a particular FOIA or PA request.

Should INV files contain records that originated with another agency, OEA will identify the records and the parent agency for Counsel to the Inspector General.

It is important that all information obtained pursuant to an express or implied grant of confidentiality be clearly identified to Counsel. (Chapter 11.9) Special care must be taken to avoid disclosing the identity of such persons to FOIA or PA requesters either directly, or by releasing information that could easily lead to identification.

It is important to identify any investigative techniques not generally known to the public, e.g., surveillance techniques employing specialized equipment that may be described or otherwise revealed in responsive records. Counsel will decide whether this type of information may be withheld under FOIA exemptions. However, before release of any such identified information, Counsel must consult with INV.

21.6 HANDLING SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION (PII)

Every INV employee is responsible for protecting information entrusted to us. An important part of this duty is to ensure that you properly use, protect, and dispose of sensitive PII.

PII is any information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor of the Department.

Some PII is public information that is not sensitive, such as the PII on a business card. Other PII is sensitive, such as a social security number or alien number, and requires stricter handling guidelines because of the increased risk to an individual if compromised.

Sensitive PII is personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone data elements. Examples of such PII include: social security numbers, driver's license numbers, or financial account numbers. Other data elements such as citizenship or immigration status; medical information; ethnic, religious, sexual orientation, or lifestyle information; and account passwords, in conjunction with the identity of an individual (directly or indirectly inferred), are also sensitive PII. In addition, the context of the PII may determine whether the PII is sensitive, such as a list of names of employees with poor performance ratings.

Sensitive PII requires stricter handling guidelines:

- Share sensitive PII with another DHS employee or contractor only if the recipient needs the information to perform official duties.
- Sensitive PII may be saved, stored, or hosted only on Government equipment.
- Do not take sensitive PII home or to any non-DHS approved worksite unless appropriately secured—sensitive PII in electronic form must be encrypted; paper records must be under the employee's control or in a locked container.
- When emailing sensitive PII outside a DHS system, send it as an encrypted attachment with the password provided separately. Within a DHS system, encryption is not required, although it is strongly recommended, especially when transmitting a large volume of sensitive PII.
- Do not mail or courier sensitive PII on CDs, DVDs, hard drives, USB drives, or other removable media unless the data is encrypted.

Additional information about protecting sensitive PII is available in the *Handbook for Safeguarding Sensitive Personally Identifiable Information*, at http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_spii_handbook.pdf.

21.7 REPORTING DATA COMPROMISES

INV employees must report to the OIG Helpdesk within one hour of confirming or suspecting a privacy incident. Reports should be sent electronically to OIGHelpdesk@dhs.gov and include "Privacy Incident" in the subject line. The incident should also be reported to the SAC/ASAC who will report to the managing DAIGI.

A reportable incident is any confirmed or suspected loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar situation involving access or potential access to sensitive PII in usable form, whether physical or electronic, by persons other than authorized users for other than authorized purposes.

Include in the report your name and contact information; the date and time of the incident; and a brief description of the circumstances including:

- Summary of the type of PII potentially at risk (do not include the specific PII, e.g., John Smith, 555-55-5555, etc., rather identify by type such as individual names, social security numbers, etc.);
- Number of individuals potentially affected and the number of records involved;
- Whether the disclosure was internal to DHS or external
- If external disclosure is involved, whether it was disclosed within the federal government or to others such as the public.

The report will be reviewed by a team of security, privacy, and legal subject matter experts to determine appropriate action, including mitigation and corrective action steps and any necessary notifications to individuals affected by the incident. A quick and effective response is critical to efforts to prevent or minimize any consequent harm from the privacy incident.

CHAPTER 21.0 - EXHIBITS

No Exhibits

22.0 OCCUPATIONAL HEALTH AND WELLNESS

22.1 General Policy

This chapter establishes policies and procedures concerning physical requirements and fitness for criminal investigators and supervisory criminal investigators within DHS OIG. The Office of Personnel Management (OPM) has established minimal medical requirements as a part of the qualification standards for criminal investigators. OPM has determined that the duties of these positions require moderate to arduous physical exertion involving walking and standing, use of firearms, and exposure to inclement weather. The OPM standards also address manual dexterity, vision, hearing, functioning limbs, and emotional and mental stability.

5 CFR Part 339 authorizes agencies to establish physical requirements for specific positions if the requirements are essential for successful job performance. OPM has determined the positions of criminal investigator and supervisory criminal investigator to be primary or rigorous positions requiring incumbents to be physically vigorous. DHS OIG is responsible for ensuring that criminal investigators are physically qualified for these positions. Therefore, before appointment, each applicant selected for a GS-1811 position with DHS OIG must undergo a physical examination.

The mandatory physical examination is a medical/physical evaluation performed by Federal Occupational Health (FOH), a division of the Department of Health and Human Services. The results of the examination and the reports from the laboratory tests are reviewed by a Medical Review Officer (MRO) employed by FOH. The MRO prepares a written statement based on the medical findings, which addresses the applicant's ability to meet the medical and physical requirements for the position sought.

22.2 Physical Requirements and Medical Standards

The DHS OIG has adopted the physical requirements and medical standards that were developed for criminal investigators based on the recommendations of the former President's Council on Integrity and Efficiency *(Exhibit 22-1)*. The council recommended the establishment of mandatory physical requirements and medical standards for applicants and incumbents in the criminal investigator job series for the Offices of Inspector General throughout the Federal government.

The physical requirements should be considered during the review of the medical history and physical examination. They are not intended to be all encompassing nor are they meant to establish absolute requirements for criminal investigators. Rather, they are provided to aid the examining physician and DHS OIG management officials in determining what medical problems may hinder the ability of criminal investigators to satisfactorily perform the actual work without causing undue risk to themselves or others. They are also provided to ensure consistency in the

application of these standards for applicants for employment as well as for current employees considered for assignment to criminal investigator positions.

22.3 Pre-Employment Physical Examinations

The DHS OIG requires that all criminal investigator applicants meet specific physical requirements and medical standards prior to being hired. All applicants for the position of criminal investigator (Special Agent) positions are made aware of the conditions of employment in the vacancy announcement.

All applicants selected for appointment will be required to undergo a pre-employment medical examination by an Agency-designated physician to determine if they are physically and mentally qualified to perform the full range of duties of the position, unless the selectee is already employed as a GS-1811 and has passed a medical examination administered by a Federal agency within the previous 12 months. In this case, the selectee may submit documentation of the examination to the MRO as proof of medical fitness for duty in lieu of a pre-employment medical examination. In addition, applicants must be informed that, if hired, they will be subject to periodic medical examinations for the purposes of assessing their fitness to retain the position.

DHS OIG will withdraw its conditional offer of employment from any selectee who refuses to submit to the required examination. DHS OIG personnel involved in the candidate interview process should make certain that these requirements are discussed with all candidates at the time of initial interview.

Tentative selectees will be required to submit to urinalysis to screen for illegal drug use prior to appointment unless currently a DHS OIG employee occupying a position already subject to random drug testing. Appointment to the position is contingent upon a negative test result. After appointment, the employee will be included in the agency's random drug testing program.

22.4 Scheduling Pre-Employment Physicals

The Human Resources Division (HRD) in the OIG's Office of Management schedules the applicant for a pre-employment physical after the Office of Investigations makes a tentative selection. FOH will send the results of the completed examination and any recommendations from the MRO to HRD.

22.5 Review by Medical Officer

The MRO will review the results of the physical examination. Based on the review, the MRO will make a recommendation and will submit a written memorandum to HRD containing the results of the review and the recommendation of the MRO as to the applicant's medical fitness for duty as a criminal investigator. HRD will transmit the results and any recommendations to the applicant and the results of the examination and MRO review to the selecting official.

22.6 Employability Determination

Employment related decisions involving health status are fundamentally management, not medical, decisions. Medical information may be relevant, indeed dominant, in the outcome, but OIG management has both the obligation to consider issues which are not strictly medical (e.g., reasonable accommodation or undue hardship on agency operations) and the authority to hold medical information to a standard of relevance and veracity. Accordingly, the medical examination cannot determine an individual's ability to perform the essential duties of a criminal investigator. This responsibility rests solely with the OIG selecting official or his/her designee. (Medical consultant services will be obtained if necessary.)

A. OIG must obtain OPM approval of any agency decision to medically disqualify a certified preference eligible candidate.

B. If the applicant/employee requests the opportunity to submit supplementary medical documentation from his/her personal physician, such documentation must be reviewed and considered by the deciding OIG official. Supplementary physical examinations from a personal physician will be paid for by the applicant/employee.

C. OIG deciding officials must comply with applicable OPM guidelines for specific medical conditions.

22.7 Reconsideration

Should an applicant/employee be found to have a significant impairment that precludes him/her from selection or retention as a criminal investigator (and the impairment is correctable), he/she will be given the opportunity to take corrective action. If the individual can present medical documentation within 90 days that the impairment has been corrected, the individual will then be eligible for reconsideration. The DHS OIG reserves the right to have such individuals re-examined by an agency-designated physician. If, based on an immediate need to fill a vacancy, the Assistant Inspector General for Investigations (AIGI) determines that the position may not be held vacant for this additional 90 days, the individual may be given priority consideration for the next vacancy after presenting evidence that the impairment has been corrected.

22.8 Waiver of Medical Standards/Physical Requirements

All requests for waivers of criminal investigator medical standards and/or physical requirements will be forwarded for decision to the AIGI. The AIGI may call upon medical consultant services if deemed necessary.

A. Failure to meet the established medical standards or physical requirements means that the individual is not qualified for the position unless there is sufficient evidence that he/she can perform the duties of the position safely and efficiently despite a condition that would normally be disqualifying. The DHS OIG must waive any physical requirement for a person who is able to demonstrate the capacity to perform

safely and efficiently. Factors that will be considered in deciding whether or not to waive a standard or requirement for OIG employment/retention include:

- health and safety considerations;
- recent satisfactory performance in the same or similar positions;
- successful performance of other life activities with similar physical and environmental demands;
- successful performance of a real or simulated work sample; and
- a determination that the condition may be reasonably accommodated (without undue hardship on the agency) to permit effective performance.

B. The decision as to whether or not an applicant/employee can perform safely and efficiently rests with the AIGI, in consultation with the Assistant Inspector General for Management and Counsel to the Inspector General.

C. A history of a medical condition may be considered disqualifying only if the condition itself is normally disqualifying, a recurrence cannot medically be ruled out, and the duties of the position are such that a recurrence would pose a reasonable probability of substantial harm.

For example, while an early history of epilepsy, by itself, would not ordinarily be disqualifying for any position, a particular history of epilepsy, depending upon the specific nature of the condition, may be disqualifying. Each case must be decided on its own merits. Generally speaking, as long as the candidate is presently able to do the job, he/she is qualified unless the possibility that the condition might recur would present a substantial health and safety risk.

22.9 Reasonable Accommodation

In accordance with the Rehabilitation Act of 1973, as amended, and the Americans with Disabilities Act, as amended, the DHS OIG will make reasonable accommodation to the known physical or mental limitations of qualified disabled applicants/employees if the accommodation will permit the disabled applicant/employee to perform the essential functions of the position in question without endangering the health and safety of the individual or others, unless the accommodation would impose an undue hardship on the OIG.

Individuals seeking such accommodation must, as determined by the OIG, submit to the medical examination required by the OIG and/or produce medical documentation to support the request.

22.10 Cost of Examination and Testing

Costs of the medical examination, including specified tests and reasonable travel expenses (for employees), will be paid by DHS OIG. Additional tests, corrective action, follow-up treatment, and/or additional medical examination recommended by the examining physician to determine the applicant's ability to meet the standards will be the responsibility of the individual applicant/employee.

22.11 Frequency of Medical Examinations

Unless waived, all new criminal investigators will undergo a medical examination before entering on duty. Periodic medical examinations will be administered at least every 36 months thereafter, until the criminal investigator's 45th birth date. All criminal investigators over the age of 45 will undergo a periodic medical examination at least every 24 months. All criminal investigators will be subject to a medical examination whenever there is a question about the employee's continued ability to meet the physical or medical requirements of the position. In certain situations, the Office of Investigations may order a psychiatric examination (including a psychological assessment). For example, the Office of Investigations may order a psychiatric examination if a current general medical examination indicates no physical explanation for behavior or actions that may affect the safe and efficient performance of the agent's duties.

22.12 Records

When the physical examination process has been completed, HRD will establish an employee medical folder for each applicant/employee. All medical documentation will be maintained in the employee medical folder. This folder is maintained separately from the Official Personnel Folder, and the information is covered under the provisions of the Privacy Act. This folder will be physically located in a secured area of HRD or secured electronically.

Access to the information contained in this folder will be available only to the applicant, employee, the representative of the employee (whom the employee has designated in writing), servicing personnel specialist(s), medical consultants, and OIG management officials who are involved in making employment/retention determinations.

The medical folder will be maintained for the length of the individual's employment with DHS OIG. If an employee transfers to another Federal agency, the employee medical folder will be transferred to the gaining agency. When the employee leaves Federal service, the medical folder will be retired to the Federal Records Center.

22.13 Mandatory Periodic Physical Examinations

DHS OIG agents will take mandatory periodic physical examinations to determine fitness for duty. The frequency of these examinations will be based solely on age and date of last physical. See section 22.11 for the schedule.

Employees who refuse to submit to required periodic examinations will be subject to reassignment or appropriate disciplinary action.

22.14 Scheduling of Periodic Physical Examinations

At the beginning of each fiscal year, HRD will provide the AIGI with a list of all personnel required to complete a physical examination during the year. PHYSICALS CANNOT BE SCHEDULED WITHOUT THE CONCURRENCE FROM HRD. The Office of Investigations will designate one staff person in Headquarters and in each field office to contact FOH to schedule the examinations as required. Every effort will be made for an examination to be conducted at a facility convenient to either an agent's work or home location. Examinations should be conducted by the end of the agent's birth month, except that no examination should be scheduled during the fourth quarter of any fiscal year. Employees whose birthdays are in July, August, or September should be scheduled either the quarter immediately preceding or immediately following their birthdays.

22.15 Reporting the Results of Periodic Physical Examinations

The FOH examining physician will forward the results of the physical examination to the MRO. After reviewing the results, the MRO will forward the results of the examination to HRD who will file the report in the employee's medical folder. Any recommendations from the MRO for additional testing or follow-up or results finding the agent unfit for duty as a GS-1811 will be brought to the attention of the employee and the AIGI.

Chapter 22.0 - EXHIBITS

Exhibit 22-1, Physical Requirements for DHS OIG Criminal Investigators

I. BACKGROUND

Any physical condition that would hinder an individual's full, efficient, and safe performance of his/her duties as a criminal investigator or failure to meet any of the required physical qualifications will usually be considered disqualifying for employment. Exception is made when convincing evidence is presented that the individual can perform the essential functions of the job efficiently and without hazard to himself/herself or others.

II. SCOPE

These physical requirements apply to all DHS OIG positions classified in the GS-1811 criminal investigator series. Therefore, any employee who occupies such a position may be periodically subject to a physical examination, by a licensed physician, to determine the individual's ability to perform the duties of the position.

III. PHYSICAL REQUIREMENTS

A. The duties of the OIG criminal investigator position require moderate to arduous physical exertion involving walking and standing, use of firearms, and exposure to inclement weather. The work requires physical strength and stamina. Individuals must be able to conduct long period s of surveillance, pursue and restrain suspects, and carry equipment utilized in investigative efforts. The environment involves work indoors and outdoors in a variety of potentially dangerous and stressful situations, as well as exposure to physical attack, including the use of lethal weapons. Applicants/employees must be in good health, physically fit, and possess the following general attributes in order that they may satisfactorily perform the duties of the position of criminal investigator:

- full range of motion of limbs and trunk;
- arms, hands, legs, and feet sufficiently intact and functioning;
- average manual dexterity and hand-eye coordination;
- average strength for age and build;
- acceptable eyesight and hearing;
- normal vocal abilities; and
- emotional and mental stability.

B. The applicant/employee must have no physical impairments that inhibit performance of required practical exercises and tasks while in mandatory training programs either at the Federal Law Enforcement Training Center (FLETC) and/or other training facilities approved by the DHS OIG. Specific information regarding FLETC practical exercise performance requirements for the 8-week basic Criminal

Investigator Training Program can be found at http://www.fletc.gov/student-information/student-information-bulletin/glynco/training-program-information.

IV. MEDICAL STANDARDS

Any disease, condition, or impairment not specifically listed in these medical standards which interferes with the safe, efficient, and expected performance of the duties and responsibilities of a criminal investigator may also constitute grounds for medical disqualification.

A. Eyesight

The occupational significance of this area concerns the ability to see and be free of visual problems. Any condition that may interfere with visual acuity or put the eye at risk may render an individual unable to meet the functional requirements for the position of criminal investigator. The individual must possess the following:

Near Vision corrected or uncorrected must be sufficient to read Jaeger Type 1 to 4 at 13 to 16 inches. Normal depth perception and peripheral vision are required.

Normal contrast sensitivity is required to rule out problems with night vision.

Far Vision uncorrected no worse than 20/200 (Snellen) in each eye, with correction to 20/20 in one eye and at least 20/40 in the other eye.

Color Vision sufficient to distinguish basic colors—red, green, and yellow.

The following are examples of impairments that may affect the individual's ability to perform required criminal investigator functions:

Current Cataracts
Glaucoma
Proliferative Retinopathy
Retinal Detachment
Refractive Keratoplasty

B. Ears and Hearing

The occupational significance of this area concerns the ability to hear and to maintain body equilibrium on standard test vestibular function. The ability to hear the conversational voice and whispered speech with or without the use of a hearing aid is required. Ability to hear is acceptable if the individual meets the standard by audiometer test with or without a hearing aid, where there is auditory discrimination at 35 decibels at 1000, 2000, and 3000 Hz level in each ear.

The applicant/employee must be retested after a noise-free period of at least 15 hours before he/she can be disqualified for hearing loss.

C. Nose, Mouth, and Throat

The occupational significance of this area is that distinct speech, odor detection, and free breathing are required. The presence of any serious acute or chronic disease or condition affecting the respiratory system and/or functional abnormality of the ears, nose, mouth, or throat which interferes with the applicant's ability to perform required criminal investigator functions are to be considered, such as any abnormality that would prevent the normal use of personal protective equipment.

D. Peripheral Vascular System

The occupational significance of this area concerns the efficiency of the vascular system for maintaining adequate blood flow. Any condition that may interfere with the peripheral vascular system's normal functioning could render the individual unable to meet the functional requirements for the position of criminal investigator. The following are examples of impairments that may affect the individual's ability to perform required duties:

Chronic Venous Insufficiency
Peripheral Vascular Disease
Thrombophlebitis

E. Heart and Cardiovascular System

The occupational significance of this area concerns the ability of the heart to provide the functional work capacity to meet the oxygen demands of physical work tasks. Any condition that would interfere with heart function could render an individual unable to meet the functional requirements for the position of criminal investigator. The following are examples of impairments that may affect the individual's ability to perform required duties:

Angina
Cardiomyopathy
Congestive Heart Failure
Coronary Artery Disease
Electrocardiogram Abnormalities (associated with disease; including arrhythmia incompatible with functional work capacity)
Hypertension (with repeated readings which exceed 150 systolic and 90 diastolic without medication)
Organic Heart Disease
Mild Controlled Hypertension (less than 140 over 90 with limited medication may be acceptable)

Pacemakers, prosthetic valves, or implanted cardiac defibrillators

F. Chest and Respiratory System

The occupational significance of this area concerns lung function, breathing capacity, and freedom from airway obstruction. This is a key area for job performance in terms of the respiration needed to perform physical tasks and to be free to move about in various environments. Any condition that may significantly interfere with breathing capacity could render the individual unable to meet the functional requirements for the position of criminal investigator. The following are examples of impairments that may affect the individual's ability to perform required duties:

Asthma (associated with reduced pulmonary function)
Chronic Bronchitis (associated with decreased pulmonary function)
Chronic Obstructive Pulmonary Disease
Bronchiectasis
Pneumonectomy
Pneumothorax
Pulmonary Tuberculosis (active or with significant lung destruction)
Reduced Pulmonary Function (if forced expiratory volume at one second is less than 65 percent of vital capacity)

G. Abdomen and Gastrointestinal System

The occupational significance of this area concerns a variety of gastrointestinal disorders that can affect performance of job tasks by imposing severe individual discomfort. Any functional disorders rendering the applicant incapable of sustained attention to work tasks, e.g., chronic diarrhea and discomfort secondary to such disorders, could render an individual unable to meet the functional requirements for the position of criminal investigator. The following are examples of impairments that may affect the individual's ability to perform duties:

Active Hepatitis
Active Peptic Ulcer Disease (not adequately controlled on medication)
Cirrhosis of the Liver
Chronic Inflammatory Bowel Disease
Gastrointestinal Bleeding
Femoral Hernia (not surgically repaired)
Inguinal Hernia (not surgically repaired)

H. Genitourinary and Reproductive System

The occupational significance of this area concerns renal failure and genitourinary dysfunction. Any condition affecting the genitourinary tract rendering an individual

unable to meet the functional requirements for the position of criminal investigator should be considered.

Pregnancy will not disqualify the individual for the position. However, some training and law enforcement assignments will be deferred until the end of the pregnancy.

The following are examples of impairments that may affect the individual's ability to perform required duties:

Acute and Chronic Nephritis
Nephrosis
Obstructive Uropathy
Polycystic Kidney Disease
Pyelonephritis
Recurrent Urinary Calculi
Renal Failure
Symptomatic Prostatic Hypertrophy
Severe Dysmenorrhea or Symptomatic Endometriosis

I. Endocrine and Metabolic Systems

The occupational significance of this area concerns any abnormality of the endocrine system that may affect job performance. Any excess or deficiency in hormonal production can produce metabolic disturbances affecting weight, stress adaptation, energy production, and a variety of symptoms such as elevated blood pressure, weakness, fatigue, and collapse. Any such disturbance of maintenance of body functions may affect ability to meet the functional requirements for the position of criminal investigator. The following are examples of impairments that may affect the individual's ability to perform required duties:

Adrenal Dysfunction
Thyroid Disease (not controlled and stable)
Pituitary Dysfunction
Symptomatic Hypoglycemia
Diabetes Mellitus*

* A diabetic condition is not usually disqualifying if there have been no significant complications (e.g., cardiovascular, visual, renal, neurological, alteration of consciousness) and the condition is controlled by diet and/or exercise, or oral medication, **or if the condition is insulin requiring, there has been no evidence of severe hypoglycemic insulin reactions (e.g., alteration of consciousness) during the past year.**

J. Musculoskeletal System

The occupational significance of this area concerns the mobility, stability, flexibility, and strength to perform physical job tasks efficiently with minimum risk of injury. Disorders affecting the musculoskeletal system are acceptable if the individual meets the basic movement, strength, flexibility, and coordinated balance criteria in the functional requirements for the position of criminal investigator. The following are examples of impairments that may affect the individual's ability to perform required duties:

Disease or Deformity of:
Bones or Joints;
Intervertebral Disks; and
Muscles and Tendons
Previous Injury (impairing performance)
Cervical Spine or Lumbosacral Fusion (affecting performance)
Herniated Disk
Loss in Motor Ability from Tendon or Nerve Injury
Major Extremity Amputation
Digit Loss (incompatible with function)

K. Hematopoietic and Lymphatic Systems

The occupational significance of this area concerns chronic disorders that may affect overall health in a disabling manner. Any disorder in this area can lead to reduced capability to perform intense physical exertion, or place the applicant at undue risk and affect the applicant's ability to meet the functional requirements for the position of criminal investigator. The following are examples of impairments that may affect the individual's ability to perform required duties:

Leukemia
Severe Anemia
Thrombocytopenia or Clotting Disorders

L. Nervous System

The occupational significance of this area concerns the functioning of the central and peripheral nervous system. The applicant should have normal sensation of hot and cold in the hands and feet; normal sense of touch in the hands and feet; and normal reflexes and balance. Dysfunction in this area can increase the probability of accidents and/or potential inability to perform a variety of physical tasks, as exemplified in the functional requirements for the position of criminal investigator. The following are examples of impairments that may affect the individual's ability to perform required duties:

Epilepsy (not controlled)
Multiple Sclerosis
Cerebrovascular Disease (including aneurysms and vascular malfunctions)
Other Disease or Disorder of the Nervous System (producing loss of strength, coordination, or other dysfunction impairing full performance, including sequelae of previous injury, infection, or other disease)

M. Malignant Diseases

The occupational significance of the disease must be related to the individual's ability to adequately function and to perform the physical work tasks as exemplified in the requirements for the position of criminal investigator.

N. Psychiatric Conditions

The occupational significance of this area is concerned with the presence of serious mental disease, which can adversely affect critical judgment and perceptive patterns necessary for safe performance of required law enforcement tasks, as exemplified in the functional requirements and environmental factors for the position of criminal investigator.

O. Medication Standard

All medications will be evaluated to ensure that safe and efficient job performance will not be adversely affected by their use. All medications will be reviewed considering the following factors:

Medication type and dosage requirements;
Potential drug side effects and adverse reactions;
Potential drug-drug, drug-environmental, and drug-food interactions;
Drug toxicity;
Medical complications associated with long term use; and
History of patient compliance.

Medications such as narcotics, sedative hypnotics, barbiturates, amphetamines, or any other drug with the potential for addiction, that is taken for extended periods of time (usually beyond 10 days) or is prescribed for a persistent or recurring underlying condition would generally be considered disqualifying.

V. ORIENTATION FOR EXAMINING PHYSICIAN

A proper examination of applicants/employees requires the physician to relate the physical examination and medical history to the demands of the job, as exemplified in the functional requirements for the position of criminal investigator. Accordingly, the examining physician should be provided with the following:

- Physical Requirements for Criminal Investigators (this Exhibit)
- Medical Standards (this Exhibit)
- Position Description for Criminal Investigator
- FLETC Training Requirements for Criminal Investigators (http://www.fletc.gov/student-information/student-information-bulletin/glynco/training-program-information).

It is important that the examining physician be aware that the position of criminal investigator requires the individual to be physically fit in order to perform required law enforcement tasks, which may include surveillance, searches, arrests, physical tactics, and the use of firearms.

The criminal investigator must possess the ability to analyze records, documents, and other evidence related to suspected criminal activity. Proper vision is required in order to conduct searches and review physical evidence. A reasonable degree of physical strength is also required in order to carry or move bulk materials and/or boxes of records that are made available through searches.

To perform surveillance, a criminal investigator must stand for long periods of time and/or be mobile at a moment's notice. Inability to remain stationary for long periods of time, as a result of chronic diarrhea or urinary frequency, could also interfere with the performance of this activity. Sensory deficits also may render the individual unable to perform surveillance.

Physical confrontation may occur when search warrants are being served or arrests are being made by a criminal investigator. The inability to carry out these tasks, due to loss of a limb or weakness secondary to local or systemic disease, could place the individual or co-workers at risk.

Judgments must be made concerning an applicant's previous history of mental illness or its symptoms since the carrying of firearms implies that reasonable judgment and mental stability must be present. Adequate visual acuity and motor coordination are also required for the proper use of firearms and for the training activities related to the position of criminal investigator.

It may be found that an individual has two or more medical conditions where each one in and of itself is not sufficiently disabling to disqualify the person for employment. However, the combination of medical or physical conditions may collectively hinder the individual's functional capacity to perform activities relating to law enforcement functions. This could place the individual at personal risk to himself/herself or others. If so, the examining physician should so indicate in his/her medical findings.

VI. EXAMINING PHYSICIAN'S CONCLUSIONS

After the examining physician has completed the physical examination and has reviewed all of the laboratory results, the results of the medical examination should be reported by the examining physician on the OIG approved medical examination form (Optional Form 178, SF-88, or revisions thereto).

His/her findings should be recorded on the approved medical examination form using one of the following statements:

A. No Significant Findings – All medical requirements for the position of criminal investigator have been satisfied.

B. Significant Medical Findings – The medical findings are noted and it is the opinion of the examining physician that the individual cannot perform the essential functional requirements efficiently and without hazard to himself/herself or others.

C. Additional Testing Requirements – Final assessment cannot be made until specific tests are conducted or repeated.

The tests recommended are:
_____
_____.

VII. REPORTS ON MEDICAL FINDINGS

All completed medical reports on examinations, along with all laboratory results, should be sealed in an envelope and forwarded to Department of Homeland Security, Office of the Inspector General, Human Resources Division, Mail Stop 2600, 245 Murray Drive, SW, Building 410, Washington, DC 20528.