

12 FAM 220 INVESTIGATIONS

*(TL:DS-94; 10-27-2003)
(Office of Origin: DS/DDB/DDP)*

12 FAM 221 SCOPE AND RESPONSIBILITY

(TL:DS-39; 08-15-1994)

The Bureau of Diplomatic Security (DS) provides a broad range of investigative services through its Office of Investigations and Counterintelligence (DS/DSS/ICI).

12 FAM 221.1 Types of Investigative Services

(TL:DS-39; 08-15-1994)

- a. The Bureau of Diplomatic Security and the Office of the Inspector General share responsibility in the investigation of passport and visa offences where Department of State employees are involved. The responsibilities of each in these investigations are outlined in joint operational guidelines.
- b. DS provides several categories of investigative services.

12 FAM 221.1-1 Security-Related Investigations

(TL:DS-39; 08-15-1994)

DS/DSS/ICI investigates all matters relating to personnel and operations security of the Department of State and the Foreign Service. These investigations range from routine background investigations of applicants to investigations of attempted penetration involving personnel or physical and technical facilities. Investigations include damage assessments of successful penetrations, unauthorized disclosure of classified information, and any matters reflecting adversely on the integrity or trustworthiness of Department personnel.

12 FAM 221.1-2 Investigations for Other Department Elements

(TL:DS-90; 06-24-2003)

DS/DSS/ICI provides investigative services for other offices of the Department such as the Bureau of Human Resources (HR), the Office of the Inspector General (OIG), the Bureau of Consular Affairs (CA), and ad hoc investigations abroad, as requested by a chief of mission.

12 FAM 221.1-3 Investigations for Other U.S. Government Departments and Agencies

(TL:DS-39; 08-15-1994)

DS/DSS/ICI may honor requests for investigative assistance abroad on behalf of other departments or agencies of the Federal Government pursuant to 22 U.S.C. 3904 (3). Criminal investigative assistance abroad must be coordinated through DS/CR/CIL.

12 FAM 221.1-4 Criminal Investigations Abroad

(TL:DS-39; 08-15-1994)

Outside the United States, DS conducts criminal investigations for the Department of illegal passport or visa issuance or use, other investigations as authorized by law, and authorized investigations requested by other U.S. law enforcement agencies, pursuant to 12 FAM, 22 U.S.C. 2709, 22 U.S.C. 3927, and 22 U.S.C. 4804.

12 FAM 221.2 Bureau of Diplomatic Security Support Agreements with Other Agencies

(TL:DS-39; 08-15-1994)

DS has a number of interagency agreements, memoranda of understanding, and exchanges of letters with the investigative, law enforcement, and security offices of other U.S. Government agencies. In some instances, DS may have more than one agreement with an agency depending on the subjects involved. These agreements establish the parameters of cooperation and jurisdiction between the two agencies in specified areas relating to security matters. The texts of current agreements are on file with the Division of Policy and Planning (DS/PPB/PPD).

12 FAM 221.3 INTERPOL Relationships

(TL:DS-39; 08-15-1994)

As part of its law enforcement duties, DS serves as the Department's representative to INTERPOL. INTERPOL is an important channel for liaison with foreign law enforcement organizations and provides DS a useful avenue for exchange of information and file checks on behalf of the Department.

12 FAM 221.4 DS Personnel Authorized to Conduct Investigations

(TL:DS-39; 08-15-1994)

- a. Special agents of the Department of State and the Foreign Service conduct investigations. DS/DSS/ICI authorizes special agents in the field offices and regional security officers (RSOs) abroad to open investigations and provides direction and guidance for the conduct of those investigations. In some investigations at posts, limited checks and inquiries may be made by post security officers upon the instructions and guidance of the responsible RSOs and/or DS/DSS/ICI.
- b. The DS Criminal Investigation Division (DS/ICI/CR) instructs and gives guidance to all special agents and RSOs for the conduct of investigations.
- c. In some investigations, RSOs may instruct post security officers within their geographic region of responsibility to conduct limited checks and inquiries on specific cases.

12 FAM 221.5 Authorities

(TL:DS-39; 08-15-1994)

- a. Authority for DS to provide investigative services is contained in a number of laws, Executive Orders, and regulations. General citations are given here; sections of 12 FAM 220 that follow elaborate on specific types of investigations.
- b. Criminal violations: The acts by a Department employee, which constitute any form of malfeasance, are usually also violations of Federal criminal statutes (U.S.C. Title 18). An example of an illegal act would be the receipt of a bribe in exchange for issuance of a visa. Such an act would constitute a violation of 18 U.S.C. 1546 and/or 201.
- c. Administrative violations: Most misfeasance and nonfeasance investigations involve violations of Department regulations or the failure to perform duties required by these regulations. The Foreign Affairs Manual (FAM) Volumes 7 and 9 contain the Department of State's visa, passport, and consular services policies for posts.

- d. Pursuant to the Statute of Limitations provision, 18 U.S.C. 3291, "the indictment must be found or the information is instituted within ten years after commission" for violations of 18 U.S.C. sections 1541 to 1544, regarding nationality, citizenship, and passport offenses.
- e. Notice of the Department's "Security Records" system was published in the Federal Register at 42 FR 49699 dated September 27, 1977, amended January 18, 1980 at 45 FR 3692. The Department's security records are designated State System-36.
- f. Specific authority for maintenance of the security records system is found in E.O. 10450 and E.O. 12356.
- g. The following authorities also apply to this subchapter:
 - (1) 22 U.S.C. 4804;
 - (2) 22 U.S.C. 2709;
 - (3) 18 U.S.C. 3238;
 - (4) 5 U.S.C. 303;
 - (5) E.O. No. 10450, April 27, 1953, sections 2, 5 (3), and 8 (a);
 - (6) 22 U.S.C. 3927; and
 - (7) The Privacy Act of 1974 (5 U.S.C. 552a).

12 FAM 221.6 Related Offenses

(TL:DS-39; 08-15-1994)

In the course of a criminal investigation concerning passport and visa issuance and use fraud, charges may arise from related offenses. The following list includes the most common related offenses:

- (1) False claim to U.S. citizenship (18 U.S.C. 911);
- (2) False statements generally (18 U.S.C. 1001);
- (3) Fraud and related activity in connection with identification documents (18 U.S.C. 1028);
- (4) Conspiracy to commit offenses or to defraud the United States (18 U.S.C. 371);

- (5) Accessory after the fact (18 U.S.C. 3);
- (6) Misprision of a felony (18 U.S.C. 4); and
- (7) Bribery of a public official (18 U.S.C. 201).

NOTE: DS does not have warrantless arrest authority for 18 U.S.C. 371; however, the U.S. attorney may add this to a complaint or a bill of indictment.

12 FAM 221.7 Investigative Method

12 FAM 221.7-1 Fairness, Objectivity, and Impartiality

(TL:DS-39; 08-15-1994)

- a. All investigations and interviews must be conducted in a fair, impartial, objective, and business-like manner to ensure fairness both to the individual being investigated and to the Department of State. Any investigator who knows of circumstances about a given case which might adversely affect his or her fairness, impartiality, or objectivity must make those circumstances known to the immediate supervisor before initiating the investigation.
- b. Investigators conducting personnel investigations shall not employ any techniques in violation of law, such as unauthorized intrusions on private property or other activities proscribed by law.
- c. Investigators shall not investigate persons or incidents without authority. Moreover, they shall be particularly careful not to investigate persons other than the subject of the inquiry, or to create the impression that they are doing so. Occasionally in background investigations, interest may legitimately focus on persons other than the main subject under investigation, but there must be direct and reasonable relevance of the other person's activity to the subject's general suitability, fitness, or loyalty. (See 12 FAM 232.)

12 FAM 221.7-2 Accuracy and Completeness

(TL:DS-39; 08-15-1994)

- a. Reports of investigation must be complete and accurate. Unsupported conclusions, conflicting statements, or unverified allegations must be investigated further and either corroborated or refuted whenever possible. Investigators must investigate any incomplete record of

criminal activity to obtain specific details and to determine final disposition of the matter.

- b. When information of a potentially disqualifying nature surfaces, an investigator must probe further to acquire sufficient details to permit a reasonable evaluation. Investigators may seek guidance from their immediate superiors when necessary in furtherance of a complete and objective investigation.
- c. To obtain maximum effectiveness, investigations must be well planned, carefully executed, and properly reported in a timely manner. Upon receipt of a request for a personnel investigation or collateral lead, the investigators shall:
 - (1) Study the basic material, including any special instructions;
 - (2) Identify the objectives of the investigation and essential issues involved; and
 - (3) Determine the facts required to resolve them.
- d. Investigators must abide by and follow any legal constraints relevant to an investigation. This includes any criminal or administrative due process safeguards with respect to either subjects or sources.

12 FAM 222 CRIMINAL INVESTIGATIONS DIVISION

12 FAM 222.1 Criminal Investigations Liaison Branch (DS/CR/CIL)

(TL:DS-39; 08-15-1994)

DS/CR/CIL conducts special criminal investigations at the request of:

- (1) The Inspector General of any Executive department having personnel at U.S. posts abroad or as requested by the Office of the Inspector General (OIG), Department of State;
- (2) Other Federal, State, and local law enforcement agencies which have primary investigative jurisdiction, but for which investigative activity is required outside the United States; and
- (3) A Federal agency or department having primary investigative

responsibility for other criminal violations (including waste, fraud, and mismanagement cases, which fall under OIG jurisdiction); and investigations requested by the Department of Justice.

12 FAM 222.2 Diplomatic Security (DS) and Inspector General (OIG) Relationship

(TL:DS-39; 08-15-1994)

- a. To ensure uniformity in assisting with the conduct of investigations sponsored by the Office of the Inspector General (OIG), all DS communications concerning such investigations must be routed through the chief of Criminal Investigations (DS/ICI/CR). DS personnel must be aware of this routing procedure and strictly adhere to its provisions.
- b. DS authority to investigate matters falling within the purview of the OIG is based on DS independent investigative authority and from the investigative authority of the Inspector General.
- c. DS special agents who receive information of interest to the OIG shall ascertain if the information has been or will be transmitted to the OIG via OIG channels. If the special agent determines that no notification to the OIG will be or has been made via normal channels, the agent will directly transmit this information to the chief, DS/ICI/CR, who will ensure it is forwarded to the OIG. Special agents should notify DS/ICI/CR by telegram, memorandum, or in emergency circumstances, by telephone, and follow up in writing.

12 FAM 222.3 Inquiry at Post Regarding Counterfeit Currency

(TL:DS-39; 08-15-1994)

- a. The RSO should conduct a preliminary inquiry to establish, at a minimum:
 - (1) Who initially reported the counterfeit;
 - (2) Under what circumstances (to include when and where) the counterfeit notes were discovered; and
 - (3) If possible, the identity of the person or institution initially attempting to pass the counterfeit notes.
- b. If appropriate, the RSO may conduct relevant interviews.

- c. The RSO should report the results of interviews to the U.S. Secret Service (USSS) by memorandum or by telegram, if there are no attachments. The following information describing the counterfeit notes should be included:
- (1) Denomination;
 - (2) Type of note: For example, a Federal Reserve note which has a green seal and serial number; a U.S. note which has a red seal and serial number; or a silver certificate which has a blue seal and serial number;
 - (3) Series;
 - (4) Serial number;
 - (5) Check letter;
 - (6) Face plate number;
 - (7) Back plate number; and
 - (8) For Federal Reserve notes, the name of the issuing bank.
- d. In exigent circumstances, the RSO should address telegraphic traffic to the USSS for immediate action.
- e. The USSS must coordinate requests through DS/CR/CIL before posts perform additional investigative activities.
- f. The chief, DS/ICI/CR, or designee, will acknowledge receipt of the information and forward it to the appropriate authority.

12 FAM 222.4 CLASS Lookouts

(TL:DS-39; 08-15-1994)

Based on the results of investigative information provided by DS/CR/PF or DS/CR/VF, the Bureau of Consular Affairs (CA/PPT) will record and maintain the name of the violator of visa, passport, and other Federal laws in the Consular Lookout and Support System (CLASS).

12 FAM 223 PASSPORT FRAUD INVESTIGATIONS

12 FAM 223.1 Other Referrals of Passport Fraud Offenses

(TL:DS-39; 08-15-1994)

- a. The Passport Fraud Section (DS/CR/PF) investigates passport fraud cases and carries out related enforcement functions for the Department. DS/CR/PF is responsible for administrative case control and directs investigations of all passport fraud cases referred to it by the Bureau of Consular Affairs, Passport Agencies.
- b. Although most referrals of passport fraud offenses originate from the Bureau of Consular Affairs' Office of Passport Services Directorate (CA/PPT), information concerning a possible passport violation can come to the attention of DS/CR/PF from Department field offices; posts; other Federal, State, and local agencies; or private citizens. DS/CR/PF refers such leads on to CA/FPP together with a request for background information. Following a check of appropriate passport records, CA/FPP forwards all pertinent information, including the passport application, to DS/CR/PF for further investigation. Regardless of origin, an investigation is always conducted on behalf of the Bureau of Consular Affairs.

12 FAM 223.2 Responsibilities

(TL:DS-39; 08-15-1994)

For the purpose of conducting passport fraud investigations, special agents may:

- (1) Obtain and execute search and arrest warrants;
- (2) Make arrests without warrant for any offense concerning passport or visa issuance or use, if the special agent has reasonable grounds to believe that the person has committed or is committing such an offense;
- (3) Obtain and serve subpoenas and summonses issued under the authority of the United States; and
- (4) Carry firearms for the purpose of performing these duties authorized by this section if designated by the Secretary, and qualified, under regulations approved by the Attorney General for the use of firearms.

12 FAM 223.3 Liaison between Bureaus of

Diplomatic Security and Consular Affairs

12 FAM 223.3-1 General

(TL:DS-39; 08-15-1994)

- a. The Office of Fraud Prevention Programs in the Bureau of Consular Affairs (CA/FPP) is responsible for the implementation of the consular anti-fraud program, including deterrence of passport fraud.
- b. DS/CR/PF is responsible for the criminal investigation and enforcement functions relating to the passport fraud aspects of this program, as authorized by the Congress in 22 U.S.C. 2709. In furtherance of these efforts, DS/CR/PF consults, as appropriate, with the Office of the Deputy Assistant Secretary for Passport Services (CA/PPT) and with CA/FPP.
- c. CA/PPT is responsible for approving and coordinating needed passport services support for DS investigative and enforcement activities.
- d. The Office of Citizenship Appeals and Legal Assistance (CA/PPT/C) is responsible for authorizing Passport Services employees to testify at trials and to assist in preparing evidence.

12 FAM 223.3-2 Passport Fraud Responsibilities

(TL:DS-39; 08-15-1994)

- a. The Office of Fraud Prevention Programs (CA/FPP) is responsible for the implementation of the consular anti-fraud program, including detection, prosecution, and deterrence of passport fraud, which depends in large measure upon the active cooperation of the Bureau of Diplomatic Security (DS). CA/FPP will:
 - (1) Ensure that requests for investigative assistance are made in a timely manner, i.e., as soon as possible once the violation is established;
 - (2) Apprise DS/CR/PF of all pertinent information developed by fraud coordinators and consular officers prior to cases being referred for investigation, and furnish to DS/CR/PF copies of any additional information received by CA/FPP after a case has been referred;
 - (3) In necessary instances, provide DS/CR/PF with the original documentation associated with a request for an investigation;
 - (4) Advise DS/CR/PF if any other agency is inquiring about or is

- interested in a case referred to DS/CR/PF for investigation; and
- (5) Designate a single contact point in CA/FPP to serve as continuing liaison with DS/CR/PF in all passport fraud-related matters.
- b. In support of the basic CA/FPP responsibility for the detection and prosecution of passport fraud, the Bureau of Diplomatic Security (DS/CR/PF) will:
- (1) Investigate all cases of alleged passport fraud referred to it by CA/FPP, and coordinate with the Office of the Inspector General on cases of mutual interest;
 - (2) Notify CA/FPP early in the process of expanded investigations, i.e., any other investigation undertaken in pursuit of a referred case;
 - (3) Notify CA/FPP upon initiating an investigation in cases of alleged passport fraud detected and referred by other Federal, State, or local agencies or other sources;
 - (4) Pursue, in a timely manner, investigations for the purpose of determining applicant's bona fides or, if fraud was perpetrated, by one individual or affiliated individuals;
 - (5) Present, with the cooperation of CA/FPP, cases of substantial passport fraud, and/or related violations of other Federal statutes, to the Department of Justice (office of the U.S. attorney) for possible prosecution;
 - (6) Ensure that original documentation is handled in such a manner as to preserve its evidentiary value, and return such passport records, including all attachments, as expeditiously as possible to CA/FPP. The disclosure of information on passport records, or release of such records, must comply with the Privacy Act, Freedom of Information Act, and Department policy;
 - (7) Provide CA/FPP with copies of all related pending and closed reports of investigations and final orders pertaining to prosecutions; and
 - (8) Designate a single contact point in DS/CR/PF to serve as the continuing liaison with CA/FPP in all passport fraud-related matters.

12 FAM 223.4 Passport Fraud Branch Investigations

(TL:DS-39; 08-15-1994)

a. The Passport Fraud Branch (DS/CR/PF) investigates the following offenses:

(1) Issuance without Authority (18 U.S.C. 1541; see text in 12 FAH-4 H-111);

(2) False Statement in Application and Use of Passports (18 U.S.C. 1542; see text in 12 FAH-4 H-111);

(3) Forgery or False Use of Passports (18 U.S.C. 1543; see text in 12 FAH-4 H-111);

(4) Misuse of Passports (18 U.S.C. 1544; see text in 12 FAH-4 H-111);

(5) Safe Conduct Violation (18 U.S.C. 1545; see text in 12 FAH-4 H-111).

b. DS special agents and investigators should be aware of the following pertinent regulations and procedures which relate to the conduct of passport fraud investigations and to duties which agents may be assigned in this connection. The Office of Citizenship Appeals and Legal Assistance (CA/PPT/C) exercises the Secretary's authority to revoke or deny any U.S. passport.

(1) Passport U.S. Government Property (22 CFR 51.9; see text in 12 FAH-4 H-114);

(2) Surrender of Passport (22 CFR 51.76; see 12 FAM 223.5-3);

(3) Denial of Passports (Mandatory) (22 CFR 51.70(a); see text in 12 FAH-4 H-115);

(4) Denial of Passport (Permissive) (22 CFR 51.70(b); see text in 12 FAH-4 H-115);

(5) Revocation or Restriction of Passports (22 CFR 51.72).

12 FAM 223.5 Investigative Policy

12 FAM 223.5-1 DS/CR/PF Responsibility

(TL:DS-39; 08-15-1994)

DS/CR/PF is responsible for administrative case control, policy, and procedural guidance for those passport fraud cases referred to it for

investigation, including authorization for investigation, assignment of a case control number, and tasking the appropriate field office to conduct the investigation. DS/CR/PF also coordinates staff work and information on all cases; case agents must transmit all case information to DS/CR/PF on a timely basis to ensure optimum case processing.

12 FAM 223.5-2 Role of DS Field Offices

(TL:DS-90; 06-24-2003)

- a. Once DS/CR/PF opens a case, the DS field offices conduct the investigation. The field office special agent in charge assigns a "case agent" who has primary operational responsibility to interview sources, gather evidence, obtain and execute search warrants, obtain and execute arrest warrants, make warrantless arrests, and ensure that the investigation is conducted in accordance with Federal Rules of Criminal Procedures and DS Guidelines.
- b. Passport fraud is often related to other criminal activities. Therefore, it is essential for the case agent to coordinate with local offices of appropriate law enforcement agencies to exchange pertinent information such as: the Federal Bureau of Investigation (FBI), the U.S. Secret Service (USSS), the Immigration and Naturalization Service (INS), the Drug Enforcement Administration (DEA), Criminal Investigation Division, U.S. Army (CID), the Internal Revenue Service (IRS), the U.S. Customs Service, and the Bureau of Alcohol, Tobacco, and Firearms, as well as State and local law enforcement agencies.
- c. If a case agent determines that sufficient evidence exists for probable cause, the basis for the determination, together with the facts and circumstances relating to the case, must be discussed with the appropriate assistant U.S. attorney (AUSA). The AUSA may request additional investigation prior to accepting or declining prosecution of the case. Case agents facilitate such requests by coordinating with DS/CR/PF, as appropriate, and by conducting further investigations within their field office area. Case agents continue to work with the AUSA through the trial of the case in Federal court. If the AUSA declines a case, the agent must communicate the declination to DS/CR/PF as soon as possible.

12 FAM 223.5-3 Recovery of Passports

(TL:DS-39; 08-15-1994)

- a. 22 CFR 51.9 states that a passport shall at all times remain the property

of the United States and shall be returned to the U.S. Government upon demand.

- b. The Department's authorized representative (usually the case agent) is authorized to demand the surrender of a revoked passport. If the bearer refuses to do so, CA/PPT may invalidate the passport by notifying the bearer in writing of the invalidation (22 CFR 51.76).
- c. Only CA/PPT/C may revoke or deny U.S. passports in accordance with regulations, whether within the United States or abroad. However, a passport may be confiscated and retained pursuant to an arrest without formal notification of revocation.

12 FAM 223.5-4 DS/CR/PF Notification

(TL:DS-39; 08-15-1994)

If a Federal arrest warrant is issued on the basis of a DS investigation, the agent must immediately report it to DS/CR/PF for further processing. DS/CR/PF will notify CA/PPT and the National Crime Information Center (NCIC), an entity administered by the Federal Bureau of Investigation.

12 FAM 224 VISA FRAUD

12 FAM 224.1 General

(TL:DS-39; 08-15-1994)

The Bureau of Diplomatic Security, Visa Fraud Section (DS/CR/VF), investigates visa fraud cases and carries out related enforcement functions for the Department of State. DS/CR/VF has primary responsibility for administrative and operational case control and investigation of all such cases referred to it by the Bureau of Consular Affairs, Office of Fraud Prevention Programs (CA/FPP), State and local agencies, other Federal agencies, and other sources.

12 FAM 224.2 Authority and Responsibilities

(TL:DS-39; 08-15-1994)

- a. DS/CR/VF provides investigative assistance in visa fraud-related cases in support of CA/FPP. Investigative and arrest authority relating to enforcement of visa fraud and consular issuance fraud are set forth in 22 U.S.C. 2709 (see also 18 U.S.C. 1546). Under regulations specifically

prescribed by the Secretary of State, special agents may conduct investigations concerning the issuance, production, or use of fraudulent visas. For the purpose of conducting such investigations, special agents may:

- (1) Obtain and execute search and arrest warrants;
 - (2) Make arrests without warrant for any offense concerning illegal passport or visa issuance or use if the special agent has reasonable grounds to believe that the person has committed or is committing such offense;
 - (3) Obtain and serve subpoenas and summonses issued under the authority of the United States; and
 - (4) Carry firearms for the purpose of performing these duties authorized by this section, if designated by the Secretary and qualified, under regulations approved by the Attorney General for the use of firearms.
- b. Statute of limitations: An indictment must be brought or an investigation must be instituted "within five years next after such offense shall have been committed." (18 U.S.C. 3282.)

12 FAM 224.3 Liaison between Bureaus of Diplomatic Security and Consular Affairs

(TL:DS-39; 08-15-1994)

- a. DS/CR/VF provides investigative assistance on visa fraud matters at the request of the Bureau of Consular Affairs Office of Fraud Prevention Programs (CA/FPP). Investigations are undertaken to determine the nature, scope, or validity of visa fraud allegations. Investigative and arrest authority relating to enforcement of visa fraud and consular malfeasance falls under provisions of 22 U.S.C. 2709.
- b. DS/CR/VF will transmit such information to CA/FPP with a request for background information as appropriate. Following a check of appropriate files, CA/FPP will forward all pertinent information to DS/CR/VF for investigation. DS/CR/VF also obtains information from visa records, maintained at posts abroad, collected through regional security officers.

12 FAM 224.4 Investigative Policy

(TL:DS-90; 06-24-2003)

- a. DS/CR/VF is responsible for administrative control of all visa fraud cases investigated by DS and provides policy and procedural guidance to agents assigned cases.
- b. Once DS/CR/VF opens a case, the DS special agent or RSO designated as case agent conducts the investigation. Special agents are authorized to interview sources, gather evidence, make arrests, issue warrants and serve as liaison with other agencies, as appropriate. A case agent will have primary operational responsibility to present evidence to the assistant U.S. attorney (AUSA) who will determine if sufficient evidence exists to warrant prosecution and to ensure that the investigation is conducted in accordance with applicable criminal law and procedure standards and DS guidelines. (See 12 FAM 224.5.)
- c. The U.S. Immigration and Naturalization Service (INS) has the primary responsibility for immigration fraud which occurs within the United States. However, DS may conduct its own investigation of the same factual situation either jointly with INS or independently. These investigations most frequently deal with the timely verification of the bona fides of sponsoring U.S.-based organizations, schools, businesses, persons, etc.
- d. At posts, consular officers are primarily concerned with the detection of fraud and the verification of the bona fides of a visa applicant's supporting documentation. If a consular officer develops information to indicate that significant visa fraud activities are being carried out within the host country, the consular officer may seek the assistance of the RSO to provide investigative support. This support could take many forms, including seeking the cooperation of local authorities to investigate and prosecute visa fraud suspects. (See 12 FAM 225.)
- e. Visa fraud is often related to other criminal activities. To obtain relevant information, investigative agents should coordinate with local offices of appropriate law enforcement agencies such as the Federal Bureau of Investigation (FBI), the Immigration and Naturalization Service (INS), the Drug Enforcement Administration (DEA), the U.S. Customs Service, as well as State and local police agencies.
- f. Once the case agent determines that sufficient evidence exists to warrant prosecution, the agent discusses the basis for the determination and the facts and circumstances of the case with the appropriate assistant U.S. attorney (AUSA). The U.S. attorney may request additional investigation by the case agent prior to accepting or declining prosecution of the case. Agents will respond to this request by conducting further investigation and will continue to work with the AUSA through the trial of the case in Federal court.

12 FAM 224.5 Policy Guidelines

(TL:DS-39; 08-15-1994)

- a. Regional security officers may respond to requests for investigative assistance received from their resident and constituent posts, and are to provide a summary of the case to the Chief, Criminal Investigations Division (DS/ICI/CR) as soon as possible.
- b. Domestic field offices may initiate visa fraud investigations only upon authorization from the Chief of DS/ICI/CR. Domestic field offices or CA/FPP will forward allegations of visa fraud to the Chief of DS/ICI/CR for action.

12 FAM 224.5-1 Liaison with Immigration and Naturalization Service (INS)

(TL:DS-39; 08-15-1994)

- a. Domestic field offices may coordinate with the local offices of INS when initiating a domestic case. Many cases will lend themselves to a joint investigative effort by DS and INS, particularly where large scale or unusual visa fraud is involved. Before initiating a joint effort, a DS agent must seek authorization from the Chief, DS/ICI/CR.
- b. Regional security officers tasked with the investigation of a visa fraud case at Foreign Service posts not having INS representatives must route all requests for INS checks, inquiries, and assistance through DS/ICI/CR. RSOs may directly request checks, inquiries, and assistance from the INS representative if one is located at post; however, RSOs should advise DS/ICI/CR of any such request.

12 FAM 225 CONSULAR ISSUANCE FRAUD INVESTIGATIONS

12 FAM 225.1 General

(TL:DS-39; 08-15-1994)

- a. Investigation of allegations of consular issuance fraud on the part of U.S. Department of State employees falls within the investigative purview of the Visa Fraud Branch (DS/CR/VF), in coordination with the Office of the Inspector General (OIG). (See 12 FAM 225.7.)

- b. Some activities, which fall within this area, are clearly violations of Federal law whereas others constitute violations of State Department administrative and procedural policy. (See 12 FAM 225.7.)
- c. Visa use fraud is fraud committed by non-employees and can include bribery or use of a falsely obtained visa.

12 FAM 225.2 Use of Issuance Fraud Investigations Assignment and Control

(TL:DS-39; 08-15-1994)

- a. DS/CR/VF has responsibility for initiating, directing, and closing all investigations of cases, which fall under the purview of 12 FAM 225. Special agents and RSOs should rely on guidance and direction from DS/CR/VF in the conduct of investigations.
- b. DS/CR/VF will assign RSOs a visa use or issuance fraud case using a DS channel telegram or a communication channel appropriate to the matter under investigation.

12 FAM 225.3 Investigation Tasking

(TL:DS-39; 08-15-1994)

- a. DS/CR/VF will authorize all visa use or issuance fraud investigative tasking for special agents and RSOs. Special agents or RSOs shall not request the services of other Department or DS offices to develop investigative leads. If a lead needs follow-up, send a request giving pertinent information to DS/CR/VF, which will assign action to the appropriate field offices or posts abroad.
- b. RSOs should not directly task other RSOs to investigate leads, except in those instances where expeditious handling is critical. In these cases, RSOs advise DS/CR/VF immediately of such taskings. If tasking is done by telegram, add DS/CR/VF as an "info" addressee.

12 FAM 225.4 Liaison with Foreign Law Enforcement Agencies

(TL:DS-39; 08-15-1994)

Special agents must be alert to the fact that certain cases may not only involve criminal or administrative issues, but may also have political

ramifications, which could affect U.S. foreign policy interests. Special agents conducting visa issuance investigations must obtain approval of DS/CR/VF prior to any exchange of information with any foreign law enforcement agency.

12 FAM 225.5 Controls and Administrative Guidance

12 FAM 225.5-1 "Need to Know" Policy

(TL:DS-39; 08-15-1994)

Because visa issuance fraud cases may involve allegations of criminal activity or other misconduct on the part of Department employees, make every effort to limit dissemination of the information. Limit knowledge of the initial allegations and subsequent investigative efforts to determine their validity only to individuals with a "need to know." This policy protects both the integrity of the investigation and the privacy of the employee concerned.

12 FAM 225.5-2 Release of Case Documents

(TL:DS-39; 08-15-1994)

DS/ICI/CR must specifically approve in writing the release of any documentation pertaining to a consular issuance fraud investigation except to DS special agents with a "need to know."

12 FAM 225.5-3 Report Allegations

(TL:DS-39; 08-15-1994)

- a. All DS offices must report every allegation of consular malfeasance directly to DS/CR/VF, which is responsible for notifying OIG and, when appropriate, CA/FPP.
- b. Report allegations of consular malfeasance by memorandum to DS/CR/VF or DS channel telegram. Send all memoranda via registered mail (pouch or domestic).

12 FAM 225.5-4 Foreign Passports Obtained for Evidentiary Purposes

(TL:DS-39; 08-15-1994)

Foreign passports are normally the property of the government which issued them, and they should not be confiscated at a preliminary stage of the investigation. However, if an individual agrees to surrender his or her passport, the agent must explain that the surrender of the passport is voluntary and that the passport can be returned to the bearer at any time. However, if identity on the foreign passport is fraudulent, it can be confiscated. In such instances, DS agents will treat the passport as evidence and immediately forward it to DS/CR/VF.

12 FAM 225.6 Prosecuting Visa Issuance Fraud Cases

(TL:DS-39; 08-15-1994)

- a. Requests for legal guidance from U.S. attorneys or local prosecutors regarding visa issuance fraud investigations must be approved in advance by DS/CR/VF. The majority of illegal and/or improper acts investigated by DS/CR/VF occur outside the United States and DS/CR/VF will determine which U.S. attorney's office will be contacted for legal guidance.

NOTE: Both informal and/or formal presentations to foreign prosecutors must have the approval of the appropriate chief of mission and the Chief, DS/ICI/CR before any approach is made.

- b. Due to the international aspects and sensitivities of most visa fraud investigations, the DS/CR/VF case control officer will be the primary point of contact with the U.S. attorney's office and will serve as liaison between the Department of Justice and the DS special agents and RSOs abroad.

12 FAM 225.7 Referring Cases to OIG

(TL:DS-58; 08-11-1997)

RSOs must immediately report by DS/DSX channel message to DS/CR/VF all new cases of suspected consular visa issuance fraud that are brought to their attention. All tasking for RSOs must be coordinated with and channeled through DS/CR/VF. In some instances, the Office of the Inspector General (OIG) may have an interest in a consular malfeasance case. DS/CR/VF will notify the OIG, if appropriate, and will notify affected posts of OIG interest. OIG is not authorized to task RSOs directly for investigative assistance; however, RSOs must coordinate closely with OIG investigators visiting posts to conduct OIG investigations and should provide appropriate assistance if requested. RSOs must also coordinate very closely with OIG investigators in any case involving an FSN employee, since RSOs are

certifying officers for employment of FSN personnel. If tasked directly by a visiting OIG investigator, RSOs should immediately notify the administrative counselor/officer at post and DS/ICI/CR by DS channel message telegram.

12 FAM 226 PROTECTIVE INTELLIGENCE INVESTIGATIONS (DS/ICI/PII)

12 FAM 226.1 Responsibilities

(TL:DS-39; 08-15-1994)

- a. DS/ICI/PII is responsible for conducting protective intelligence investigations of terrorist and hostile activities to detect and deter acts of terrorism and to better protect diplomatic facilities and personnel.
- b. The following terrorist and/or hostile activities or attempted activities are of protective intelligence interest:
 - (1) Assassination;
 - (2) Assault;
 - (3) Bombing;
 - (4) Facility seizure;
 - (5) Hijacking;
 - (6) Kidnapping;
 - (7) Arson, in coordination with DS/ICI/CR;
 - (8) Threats (written, oral, telephonic, etc.);
 - (9) Hostile surveillance of U.S. Government facilities and personnel;
 - (10) Fraudulent use of visas and passports to facilitate travel by terrorists or others with a hostile intent against DS protectees, coordinated with DS/ICI/CR; and
 - (11) Miscellaneous activity (travel of terrorists, their modus operandi, other characteristics of foreign terrorist groups, requests for investigative assistance).

12 FAM 226.2 Policy and Programs

12 FAM 226.2-1 Investigations Involving Terrorist and Hostile Incidents and Activities

(TL:DS-72; 01-26-2001)

DS/ICI/PII plans, coordinates, controls, and conducts protective intelligence investigations involving terrorist incidents and hostile activities directed against U.S. diplomatic facilities and U.S. Government personnel and against other U.S. interests abroad and in the United States. Investigators conduct on-site investigations of terrorist incidents and/or provide appropriate guidance and supervision to field security personnel, domestically and abroad, involved in conducting or supporting protective intelligence investigations.

12 FAM 226.2-2 Protective Intelligence Investigations

(TL:DS-39; 08-15-1994)

- a. DS/ICI/PII monitors and interprets sensitive intelligence for the purpose of corroborating, developing, and expanding information regarding threats against diplomatic personnel and facilities in the United States and abroad to resolve threat information. DS/ICI/PII uses information derived from protective intelligence investigations to detect and deter terrorist and hostile acts against DS protectees and to enhance Department protective security procedures to prevent similar occurrences. These efforts are carried out by DS/ICI/PII agents and coordinated with DS/DSS/ITA.
- b. DS/ICI/PII conducts concentrated protective intelligence operations for special events or where a specific threat against a DS protectee exists. These operations include protective intelligence coordination and, where appropriate protective intelligence countersurveillance (PICS) for investigative purposes.
- c. DS/ICI/PII provides protective intelligence investigative support relating to the security of internationally protected persons assigned to or traveling in the United States. DS/ICI/PII has a DS special agent assigned to the FBI terrorism section who is responsible for coordination of FBI/DS investigative efforts regarding foreign officials in the Washington, D.C. area.

12 FAM 226.2-3 Task Force and Security Support Team

Participation

(TL:DS-39; 08-15-1994)

DS/ICI/PII participates as a member of Department and interagency task forces dealing with terrorist incidents and threats and coordinates with counterterrorist and law enforcement units from other agencies. Similarly, DS/ICI/PII provides investigative services in conjunction with the DS Mobile Security Division and security support teams, responding to terrorist or hostile incidents or high threat situations.

12 FAM 226.3 Rewards Program for Information on Terrorism

(TL:DS-90; 06-24-2003)

- a. Section 36 of the State Department Basic Authorities Act of 1956, as amended (22 U.S.C. 2708 et seq.), provides the authority for the Department of State to establish a rewards program for information on terrorism.
- b. The Bureau of Diplomatic Security (DS) administers this rewards program, and the Office of the Coordinator for Counterterrorism (S/CT) provides policy guidance, as needed, for the program.
- c. Within DS, DS/ICI/PII implements the program and is the Department point-of-contact for reward proposals and for information and actions concerning the program.

12 FAM 226.3-1 Authorities

(TL:DS-90; 06-24-2003)

- a. The Secretary of State may pay a reward of not more than \$5 million, except as set forth in 12 FAM 226.6-7 (a) and subject to available funding, to any individual who furnishes information leading to:
 - (1) The arrest or conviction, in any country, of any individual for the commission of an act of international terrorism; or
 - (2) The arrest or conviction, in any country, of any individual for conspiring or attempting to commit an act of international terrorism; or
 - (3) The arrest or conviction, in any country, of any individual for committing, primarily outside the territorial jurisdiction of the

United States, any narcotics-related offenses as more particularly described in 2 FAM 950; or

- (4) The arrest or conviction, in any country, of any individual aiding or abetting in the commission of an act described in subparagraph (1), (2) or (3); or
- (5) The prevention, frustration, or favorable resolution of an act described in subparagraph (1), (2) or (3), including by dismantling an organization in whole or in part; or
- (6) The identification or location of an individual who holds a key leadership position in a terrorist organization.

The act of international terrorism must be against a U.S. person or property.

- b. Section 103(a)(2)(B)(xi) of the Omnibus Diplomatic Security and Anti-terrorism Act of 1986 (22 U.S.C. 4802(a)(2)(B)(xi)) provides that security responsibilities of the Secretary of State shall include "Carrying out the rewards program for information concerning international terrorism authorized by Section 36(a) of the State Department Basic Authorities Act of 1956." By Delegation of Authority No. 214, Section 8, dated September 20, 1994, the Secretary of State delegated to the Assistant Secretary for Diplomatic Security the functions delegated to the Secretary of State by Section 103(a)(2) (22 U.S.C. 4802 (a)(2)) of the Omnibus Diplomatic Security and Anti-Terrorism Act of 1986, as amended.

12 FAM 226.3-2 The Interagency Rewards Committee on Terrorism Information

(TL:DS-90; 06-24-2003)

- a. An interagency committee, the Interagency Rewards Committee on Terrorism Information ("Terrorism Information Rewards Committee") has been established to address issues associated with this program and to consider proposals for rewards payments to potential recipients.
- b. The Terrorism Information Rewards Committee is chaired by the Director, Diplomatic Security Service (DS/DSS), or his or her designee, and is comprised of representatives from:
 - (1) The Office of Investigations and Counterintelligence, Protective Intelligence Division (DS/ICI/PII);
 - (2) The Bureau of Resource Management (RM);

- (3) The Office of the Coordinator for Counterterrorism (S/CT) (also represents the Interagency Working Group on Terrorism);
 - (4) The Office of the Legal Adviser (L);
 - (5) The Federal Bureau of Investigation (FBI);
 - (6) The Department of Justice, Criminal Division (DOJ);
 - (7) The Central Intelligence Agency (CIA);
 - (8) The National Security Council staff (NSC); and
 - (9) The Department of Treasury (DOT).
- c. As appropriate, representatives of other Department bureaus or other U.S. Government agencies may also confer with the Terrorism Information Rewards Committee, or be present as observers.
- d. Decisions of the committee shall generally be made by consensus, however, none of the agencies (other than the Department of State) participating in the committee meeting shall have the right to block a recommendation to pay a reward. Any disagreement with any aspect of a recommendation to pay a reward will be noted in the action memorandum to the Secretary in accordance with 12 FAM 226.6-6.

12 FAM 226.3-3 Protection of Informants

(TL:DS-90; 06-24-2003)

- a. If the Secretary determines that the identity of the recipient of a reward or of the members of the recipient's immediate family must be protected, the Secretary shall take such measures in connection with the payment of the reward as he or she considers necessary to effect such protection. Specific measures employed to protect the identity of a recipient or potential recipient (and immediate family members, as appropriate) beyond the security procedures generally applicable to the rewards program, as set forth in 12 FAM 226.5-4, will depend on the circumstances of each case, but include not identifying the reward recipient by name in the reports sent to Congress in accordance with 12 FAM 226.8. Generally, "immediate family members" will mean the same family members to which 8 U.S.C. 1101(a)(15)(S) applies.
- b. Informants and their immediate family may be eligible for participation in the Attorney General's Witness Security Program authorized under 18 U.S.C. 3521, et seq. DS/ICI/PII is the Department's point-of-contact for

this contingency. U.S. Government officials shall not make a promise or inducement of participation in this program without the express approval of the Department of Justice.

- c. Pursuant to 8 U.S.C. 1101(a)(15)(S), an informant may be eligible for a nonimmigrant visa, if, among other things, the Secretary of State and the Attorney General jointly determine that the informant possesses critical reliable information concerning a terrorist organization, enterprise, or operation; is willing to supply or has supplied such information to Federal law enforcement authorities or a Federal court; will be or has been placed in danger as a result of providing such information; and is eligible to receive a reward. The informant's immediate family may also be eligible for such visas.
- d. The post, working with the informant, should report to DS/ICI/PII what specific additional measures for protection of the identity of an informant are indicated and planned.

12 FAM 226.4 Rewards Program for Information on War Crimes

(TL:DS-90; 06-24-2003)

- a. Section 102 of Public Law 105-323, Section 1 of Public Law 106-277 and Section 36 of the State Department Basic Authorities Act of 1956, as amended (22 U.S.C. 2708 et seq.) provide the authority for the Department to establish a rewards program for information on persons indicted by the International Criminal Tribunal for the Former Yugoslavia (ICTY) or the International Criminal Tribunal for Rwanda (ICTR).
- b. In conjunction with the Office of War Crimes Issues (S/WCI), the Bureau of Diplomatic Security (DS) administers this rewards program and S/WCI and the appropriate regional bureau provide policy guidance, as needed, for the program.
- c. Within DS, DS/ICI/PII implements the program and is the Department's point-of-contact for reward proposals and for information and actions concerning the program.

12 FAM 226.4-1 Authorities

(TL:DS-90; 06-24-2003)

- a. The Secretary of State may pay a reward to any individual who furnishes information leading to:

- (1) The arrest or conviction in any country; or
 - (2) The transfer to, or conviction by, the ICTY or the ICTR of any individual who is the subject of an indictment confirmed by a judge of such Tribunal for serious violations of international humanitarian law as defined under the statute of such Tribunal. The statute of the ICTY means the Annex to the Report of the Secretary General of the United Nations pursuant to paragraph 2 of Security Council Resolution 827 (1993), and the statute of the ICTR means the statute contained in the annex to Security Council Resolution 955 (1994).
- b. Rewards under this section shall be subject to any requirements or limitations that apply to rewards under Section 36 of the State Department Basic Authorities Act of 1956, as amended (22 U.S.C. 2708 et seq.), with respect to the ineligibility of government employees for rewards (12 FAM 226.5-1), maximum reward amount (12 FAM 226.6-7(a)), and procedures for the approval and certification of rewards for payment (12 FAM 226.6-7).

12 FAM 226.4-2 The Interagency Rewards Committee on War Crimes Information

(TL:DS-90; 06-24-2003)

- a. An interagency committee, the Interagency Rewards Committee on Violations of Humanitarian Law in the Former Yugoslavia and in Rwanda ("War Crimes Information Rewards Committee"), has been established to address issues associated with this program and to consider proposals for rewards payments to potential recipients.
- b. The War Crimes Information Rewards Committee is chaired either by the Director, Diplomatic Security Service (DS/DSS) or by the Ambassador-at-Large for War Crimes (S/WCI), or his or her designee, and is comprised of representatives from:
 - (1) The Bureau of Diplomatic Security (DS);
 - (2) The Bureau of Resource Management (RM);
 - (3) The appropriate regional bureau (EUR or AF);
 - (4) The Office of War Crimes Issues (S/WCI);
 - (5) The Office of the Legal Adviser (L);

- (6) If, as determined in consultation with the Department of Justice, Criminal Division, the proposed reward concerns a matter over which there is Federal criminal jurisdiction, the Department of Justice, Criminal Division (DOJ);
 - (7) The Central Intelligence Agency (CIA);
 - (8) The Department of Defense (DOD); and
 - (9) The National Security Council staff (NSC).
- c. As appropriate, representatives of other Department bureaus or other U.S. Government agencies may also confer with the War Crimes Information Rewards Committee or be present as observers.
- d. Decisions of the committee shall generally be made by consensus, however, none of the agencies (other than the Department of State) participating in the committee meeting shall have the right to block a recommendation to pay a reward. Any disagreement with any aspect of a recommendation to pay a reward will be noted in the action memorandum to the Secretary in accordance with 12 FAM 226.6-6.

12 FAM 226.5 Rewards Programs Guidelines

12 FAM 226.5-1 Ineligibility of Government Officers or Employees

(TL:DS-90; 06-24-2003)

An officer or employee of any entity of Federal, State, or local government or of a foreign government who, while in the performance of his or her official duties, furnishes information as described in 12 FAM 226.3-1 (a) or 12 FAM 226.4-1 (a) shall not be eligible for a reward under the rewards programs. Such an officer or employee may, however, in the case of 12 FAM 226.3-1 (a), be eligible for participation in the Witness Security Program.

12 FAM 226.5-2 Coordination with Relevant Host-Government Authorities

(TL:DS-72; 01-26-2001)

The rewards programs shall be carried out in such a manner as to supplement and complement the bona fide security and law enforcement efforts of relevant host-government authorities who bear the primary

responsibility in these areas. To this end, all stages of the rewards process (see 12 FAM 226.6) will be closely coordinated whenever appropriate with responsible host-government authorities. Such coordination will be accomplished primarily between the regional security officer (RSO) and local security and law-enforcement authorities.

12 FAM 226.5-3 Responsibilities

(TL:DS-90; 06-24-2003)

- a. At post, the RSO is primarily responsible for the rewards programs at each post within that officer's jurisdiction. Such responsibility includes implementation of each of the stages of the rewards process as set forth in 12 FAM 226.6, including coordination, at each stage where appropriate, with host-government authorities. In carrying out these responsibilities, the RSO shall remain subject to the overall direction and supervision of the deputy chief of mission (DCM) and principal officer(s) concerned and shall coordinate with other officers at post, as appropriate.
- b. Within the Department, all proposals to pay a reward under these programs, whatever their source, will be coordinated by DS, and in the case of war crimes, with S/WCI. In carrying out this responsibility, DS shall consult with the members of the Terrorism Information Rewards Committee or the War Crimes Information Rewards Committee, as appropriate. Consultation may take the form of meetings of the relevant rewards committee or circulation of written proposals to committee members.

12 FAM 226.5-4 Security Procedures

(TL:DS-72; 01-26-2001)

- a. All telegraphic communications relating to the implementation of these programs must be transmitted in appropriate channels with classification level and distribution controls sufficient to ensure the security of these operations and persons involved. Such communications include:
 - (1) Proposals that rewards be paid;
 - (2) Reports of information received in response to a reward offer;
 - (3) Measures taken in response to information received;
 - (4) Contacts with host-government authorities;
 - (5) Instructions from the Department to posts; and

- (6) Other relevant information.
- b. Names of informants and information that may lead to their identification must be transmitted through the ROGER Channel.
- c. All other documents relating to implementation (such as internal memoranda) are to be given a similar level of protection. In particular, information relating to identities of informants and times, places, and circumstances of contacts with U.S. officials must be handled in accordance with appropriate operational security procedures.

12 FAM 226.5-5 Accounting for Funds

(TL:DS-90; 06-24-2003)

Fiscal responsibility and accountability for funds appropriated for use in carrying out the rewards programs will reside with the Department of State, Bureau of Resource Management (RM). RM will also be responsible for instituting appropriate financial controls, including such controls as may be necessary to maintain the confidentiality of payments within the framework of internal control and audit requirements.

12 FAM 226.6 Rewards Process

12 FAM 226.6-1 Offers to Pay Rewards

(TL:DS-90; 06-24-2003)

- a. The Department, posts, or other agencies may propose that a reward be offered for information on either terrorism or war crimes in accordance with these regulations and authorities set forth in 12 FAM 226.3-1 and 12 FAM 226.4-1.
- b. Such proposals may include that a reward be offered jointly with a foreign government.
- c. A generic reward offer for information relating to all potential targets may also be proposed.
- d. Any reward proposals must be cleared by DS, L, and RM, and, as appropriate, EUR (war crimes information with respect to ICTY), AF (war crimes information with respect to ICTR), S/WCI (war crimes information), S/CT (terrorism information), and the Department of Justice. Relevant posts shall also be consulted regarding proposed reward offers and may be directed to consult with respective host governments

or the ICTY or the ICTR, as appropriate.

- e. When a reward offer is cleared as set forth in 12 FAM 226.6-1(d), it may then be publicized in accordance with 12 FAM 226.6-2.

12 FAM 226.6-2 Publicizing Rewards Offers

(TL:DS-90; 06-24-2003)

- a. Reward programs or reward offers may be publicized through media campaigns to include the use of posters developed by the Department. These campaigns may also be posted on the rewards programs' web site on the Internet: <http://www.rewardsforjustice.net>.
- b. Both Department and post-initiated media announcements of reward offers should include:
 - (1) A brief opening paragraph setting forth the relevant facts (e.g., the terrorist incident or the indictment);
 - (2) A statement announcing the basic elements of the program including:
 - (a) The amount up to which the U.S. Government is authorized to pay (currently, up to \$5 million, subject to the Secretary's authority in 12 FAM 226.6-7 (a)); and
 - (b) The means by which potential informants may contact the Department; and
 - (3) A statement indicating that all responses will be kept confidential.
- c. Supplemental reward offers (see 12 FAM 226.6-7 (d)) may also be publicized.
- d. In no case may a Department or other agency official agree to pay a reward under this program without express approval from the Department through DS/ICI/PII in accordance with 12 FAM 226.6.
- e. All reward program announcements and other media campaigns shall be cleared by DS, L, and RM, and, as appropriate, EUR (war crimes information with respect to ICTY), AF (war crimes information with respect to ICTR), S/WCI (war crimes information), S/CT (terrorism information), and the Department of Justice. Relevant posts shall also be consulted regarding proposed announcements and may be directed to consult with respective host governments or the ICTY or ICTR, as appropriate.

12 FAM 226.6-3 Actions upon Receiving Information at Post in Response to Reward Offers

(TL:DS-90; 06-24-2003)

- a. The chief of mission of the post shall designate one officer, normally the responsible RSO, to collect all information received in response to a reward offer. Any other officer or employee of the post receiving such information shall immediately convey it to the officer designated, subject only to considerations of protection of intelligence sources and methods or the proprietary nature of the information.
- b. The designated officer will report to the DCM and be responsible for initially evaluating the credibility and relevance of the information.
- c. The officer must also ensure that the information is properly coordinated at the post and promptly transmitted to the Department through appropriate secure channels. Post will consult with the Department and, if deemed appropriate, transmit this information to other posts that may have an interest, and, if appropriate, to host-country and/or ICTY or ICTR authorities. If the information concerns a terrorist incident, the officer must also ensure that the information is promptly reported to a representative of the Federal Bureau of Investigation.
- d. The Department will usually issue instructions on specific measures to take in response, such as follow-up questioning of an informant or further contacts with host-country authorities. If, however, information received at post is of sufficient credibility and urgency to warrant responsive action in the absence of instructions from the Department, the responsible officer(s) at post should take the necessary steps and inform the Department immediately.
- e. These programs do not supersede existing walk-in policies. All information should be coordinated with appropriate embassy officers.

12 FAM 226.6-4 Proposals to Pay Rewards

(TL:DS-90; 06-24-2003)

- a. Proposals that a reward be paid under either of these rewards programs may originate at post, at the Department, or at other agencies. If a proposal originates at post, the designated officer will coordinate it, and the chief of mission or DCM in the country involved shall approve it before post forwards it to the Department for consideration. Included with any such proposal must be specific details concerning the factors set forth in 12 FAM 226.6-5. In no case may a post agree to pay a reward under

these rewards programs without express approval from the Department through DS/ICI/PII in accordance with 12 FAM 226.6.

- b. If a proposal originates within the Department, the relevant rewards committee will normally seek the views of the relevant post(s) before recommending the payment of a reward.
- c. Posts proposing recipients should advise the relevant rewards committee through DS/ICI/PII of any host-country sensitivities bearing upon the decision-making process. For example, host-country legal restrictions as may apply to payment, or promise of payment, to witnesses for their testimony must be considered in making recommendations, as well as the effect that payment of a reward would have on law enforcement efforts of host-country authorities.
- d. Posts should also advise whether in the case of rewards for terrorism information, any specific measures for protection of the identity of the proposed recipient are deemed necessary (see 12 FAM 226.3-3 and 12 FAM 226.5-4).
- e. A post may suggest a reward amount to the Department as part of its proposal in light of the considerations listed in 12 FAM 226.6-5.

12 FAM 226.6-5 Reviewing Rewards Proposals

(TL:DS-90; 06-24-2003)

- a. Section 102(e) of Public Law 105-323, as amended, directs the Secretary of State to ensure that priority is given for payments of rewards to individuals described in Section 36 of the State Department Basic Authorities Act, as amended (22 U.S.C. 2708) (i.e., individuals providing information in connection with terrorism or narcotics) and that funds paid for rewards for war crimes information are paid only after any and all due and payable demands are met under Section 36 of that Act.
- b. The relevant rewards committee will review proposals to pay rewards to informants in light of this section 12 FAM 226.6-5.
- c. In cases covered by Section 36(b)(1), (2) or (4) of the State Department Basic Authorities Act of 1956, as amended (22 U.S.C. 2708(b)(1), (2) or (4)), concerning information leading to the arrest or conviction for commission of, or for attempt or conspiracy to commit, or for aiding or abetting an act of international terrorism, the decision to pay a reward and the amount thereof depend on various considerations, including in particular the following:

- (1) The seriousness of the injury or potential injury to U.S. persons or property, and the degree to which the terrorist act was targeted against U.S. persons or property;
 - (2) The number and degree of seriousness of the act(s);
 - (3) The likelihood that the information provided has materially aided in bringing the perpetrators to justice;
 - (4) The value of the information with respect to the arrest and/or prosecution of the individual(s) responsible for the act of international terrorism;
 - (5) The degree of participation in the terrorist act of the individual(s) arrested and/or prosecuted (for example, whether the individual was an accessory, passive participant, active participant, leader, or mastermind);
 - (6) The degree of risk faced by the potential reward recipient and his or her family in providing the information;
 - (7) The degree to which the arrest or conviction will seriously impede the functions of a terrorist organization;
 - (8) The degree to which the individual(s) voluntarily cooperated with authorities; and
 - (9) The attitude of relevant government authorities toward a reward payment.
- d. In cases covered by Section 36(b)(5) or (6) of the State Department Basic Authorities Act of 1956, as amended (22 U.S.C. 2708(b)(5) or (6)), concerning information leading to (i) the prevention or frustration of an act of international terrorism, (ii) the favorable resolution of an act of international terrorism, (iii) the dismantling of a terrorist organization in whole or significant part, or (iv) the identification or location of an individual who holds a key leadership position in a terrorist organization, the decision to pay a reward and the amount thereof will depend on various considerations, including in particular the following:
- (1) The credibility and specificity of available information indicating, as applicable, (i) that there is a threat of such an act, (ii) the on-going activities of the terrorist organization or threat, or (iii) the identification or location of the individual who holds a key leadership position in a terrorist organization;
 - (2) The seriousness of the danger to U.S. persons or property indicated

by the available information;

- (3) The likelihood that, and the degree to which, the information provided has materially aided in successfully, as applicable, (i) avoiding or countering the threat, (ii) favorably resolving an act of international terrorism or an ongoing international terrorist activity (e.g., a hostage-taking or an aircraft hijacking), (iii) dismantling a terrorist organization in whole or in part, or (iv) identifying or locating the key individual;
 - (4) The degree of risk faced by the potential reward recipient and his or her family in providing the information;
 - (5) The degree to which the recipient voluntarily cooperated with authorities; and
 - (6) The attitude of relevant government authorities toward a reward payment.
- e. In cases covered by Section 102 of Public Law 105-323, as amended, concerning information leading to the arrest or conviction, in any country, or the transfer to, or conviction by, the ICTY or the ICTR, of any individual who is the subject of an indictment confirmed by a judge of such tribunal for serious violations of international humanitarian law, as defined under the statute of such tribunal, the decision to pay a reward, and the amount thereof, will depend on various considerations, including in particular the following:
- (1) The number and degree of seriousness of the violations of international humanitarian law;
 - (2) The likelihood that the information provided has materially aided in bringing the indictee to justice;
 - (3) The value of the information with respect to the arrest and/or prosecution of the indictee;
 - (4) The degree of participation in the violation of international humanitarian law of the indictee (for example, whether the individual was an accessory, passive participant, active participant, leader, or mastermind);
 - (5) The degree of risk faced by the potential reward recipient and his or her family in providing the information;
 - (6) The degree to which the recipient voluntarily cooperated with authorities; and

- (7) The attitude of relevant government authorities toward a reward payment.
- f. Whether or not a reward is paid in any given case, and the amount of the reward, are matters wholly within the discretion of the Secretary of State, with the concurrence of the Attorney General if it is a matter over which there is Federal criminal jurisdiction.
- g. If a proposal to pay a reward is denied by a rewards committee, the Secretary of State or the Attorney General, DS/ICI/PII will advise the originating post, if any, of the decision by telegram, specifying the basis for denial.

12 FAM 226.6-6 Action Memorandum

(TL:DS-90; 06-24-2003)

If the relevant rewards committee decides to recommend a reward payment, the chairman of the rewards committee will send an action memorandum forward from DS, through the Under Secretary for Management, to the Secretary (for rewards of \$100,000 or more), or to the Under Secretary for Management with the concurrence of the Under Secretary of State for Political Affairs (for rewards of less than \$100,000), recommending that a reward be certified for payment. The action memo shall include:

- (1) A summary of the indictment/incident;
- (2) An analysis of the proposal in light of the considerations set forth in this section;
- (3) For cases involving international terrorism covered by Section 36(b)(1), (2), (4) or (5) of the State Department Basic Authorities Act of 1956, as amended (22 U.S.C. 2708(b)(1), (2), (4) or (5)), an analysis and a recommendation that the Secretary determine whether there is "act of international terrorism" as defined in Section 36(j)(1) of the State Department Basic Authorities Act of 1956, as amended (22 U.S.C. 2708(j)(1));
- (4) Other considerations that would affect the amount of the reward and/or the method of payment;
- (5) A recommendation as to the amount of the reward;
- (6) A recommendation as to any necessary measures to protect the identity of the recipient and/or members of the recipient's immediate family;

- (7) As appropriate, the dissenting opinion(s) of any rewards committee representatives involved in the decision to recommend payment of a reward; and
- (8) If the matter is one over which there is Federal criminal jurisdiction, a proposed letter seeking the concurrence of the Attorney General. See also 12 FAM 226.6-7 (c).

12 FAM 226.6-7 Reward Payment

(TL:DS-90; 06-24-2003)

- a. Generally, rewards may not exceed \$5 million U.S. dollars. If the Secretary of State determines personally, however, that the offer of payment of an award of a larger amount is necessary to combat terrorism or defend the nation against terrorist acts, he or she may authorize an award for a larger amount.
- b. Section 36(e)(2) of the State Department Basic Authorities Act of 1956, as amended (22 U.S.C. 2708(e)(2)), requires that the Secretary of State personally approve rewards of \$100,000 or more. By Delegation of Authority No. 180 dated August 8, 1989, the Secretary of State has delegated to the Under Secretary of State for Management the functions vested in the Secretary by Section 36 of the State Department Basic Authorities Act of 1956, as amended, with respect to the payment of rewards of less than \$100,000, subject to the concurrence of the Under Secretary of State for Political Affairs as to each proposed payment. Pursuant to Section 36(e)(3) of the Act, the Secretary of State must approve and certify for payment any reward granted under this authority. Pursuant to Delegation of Authority No. 180, the Under Secretary of State for Management, subject to the concurrence of the Under Secretary of State for Political Affairs as to each payment, may approve and certify for payment rewards of less than \$100,000.
- c. The Secretary shall determine the amount of the reward paid in his or her sole discretion. He or she shall generally seek the views of the other agencies, and in particular, the agency or bureau proposing the reward, when making his or her determination.
- d. Provided the Secretary or the Under Secretary for Management has decided that a reward shall be paid, and has received the concurrence of the Attorney General if it is a matter over which there is Federal criminal jurisdiction, DS/ICI/PII will notify post and arrangements will be made to pay the reward.
- e. Supplemental rewards may also be paid as follows:

- (1) In connection with the Rewards Program for Information on Terrorism, the Department has entered into arrangements with two non-U.S. Government entities, the Air Transport Association of America (ATA) and the Airline Pilots Association (ALPA), pursuant to which ATA and ALPA may supplement certain rewards the Department makes to individuals under the Rewards Program for Information on Terrorism. In general, ATA may make such supplemental rewards in connection with acts of international terrorism directed against U.S. air carriers that are members of ATA. ALPA may make such supplemental rewards in connection with acts of international terrorism directed against a U.S. air carrier's passengers, crewmembers, or aircraft whose flight deck members are represented by the ALPA.
- (2) With the approval of the Under Secretary for Management and with clearances from S/CT, S/WCI, L and other relevant bureaus, the Department may enter into arrangements with other non-U.S. Government entities to supplement the rewards the Department makes to individuals under the Rewards Program for Information on Terrorism or the Rewards Program for Information on War Crimes.

12 FAM 226.8 Reporting Requirements

12 FAM 226.8-1 Reports on the Payment of Rewards

(TL:DS-90; 06-24-2003)

Pursuant to Section 36(g)(1) of the State Department Basic Authorities Act of 1956, as amended (22 U.S.C. 2708(g)(1)), within 30 days after payment of any reward, the Secretary shall submit a report to the House Committee on International Relations and the Senate Committee on Foreign Relations with respect to that reward. DS/ICI/PII will prepare the report, which may be submitted in classified form if necessary, and which shall:

- (1) Specify the amount of the reward paid;
- (2) Identify to whom the reward was paid (when necessary to protect the recipient, an identification number may be used instead of a name);
- (3) State the acts with respect to which the reward was paid; and
- (4) Discuss the significance of the information for which the reward was paid in dealing with the respective acts.

12 FAM 226.8-2 Annual Reports

(TL:DS-90; 06-24-2003)

Pursuant to Section 36(g)(2) of the State Department Basic Authorities Act of 1956, as amended (22 U.S.C. 2708(g)(2)), not later than 60 days after the end of each fiscal year, the Secretary shall submit a report to the House Committee on International Relations and the Senate Committee on Foreign Relations with respect to the operation of the rewards programs. The report shall provide information on the total amounts expended during the fiscal year ending in that year to carry out the rewards programs, including amounts expended to publicize the availability of rewards.

12 FAM 227 PERSONNEL INVESTIGATIONS

12 FAM 227.1 Scope

(TL:DS-94; 10-27-2003)

- a. All U.S. Government positions are designated in terms of their national security sensitivity to assure appropriate screening under E.O. 10450 (see 12 FAM 230). A full field background investigation is required for sensitive positions. Sensitive positions are those in which an individual, either deliberately or through negligence, could adversely affect the security interests of the United States. Because of the potential risk to national security it is essential that sensitive positions be filled only by persons of demonstrated loyalty and trustworthiness. Absence of disqualifying information about an individual is insufficient to make a positive determination about a person's eligibility for a sensitive position; enough positive information must be known about the individual to lead a reasonable person to conclude that the individual under investigation can be trusted with responsibility for matters of more than routine consequence to the nation, and the individual will maintain that trust in the face of unusual pressures or hazards. The purpose of the background investigation is to acquire the information necessary and relevant for such a determination.
- b. The main objective of a personnel security investigation is to establish the individual's general character, integrity, and trustworthiness, as demonstrated by past conduct and acceptance of responsibility. This will permit an assessment of the probability that the individual will perform his or her duties faithfully and responsibly, and will hold in confidence, even under adverse circumstances, matters of official business which require discretion.

12 FAM 227.2 Authority

(TL:DS-94; 10-27-2003)

- a. The Secretary has delegated authority to the Bureau of Diplomatic Security to conduct employment related investigations based on the following executive orders and laws:
 - (1) *Public* Law 99-399, August 27, 1986 (codified at 22 U.S.C. 4804 (3)(D));
 - (2) Executive Order (E.O.) 10450 dated April 27, 1953, specifically section 3(b);
 - (3) E.O. 12356 dated April 2, 1982, National Security Information;
 - (4) E.O. 10865 dated February 20, 1960, Safeguarding Classified Information within Industry;
 - (5) The Foreign Service Act of 1980 as amended.
- b. Public Law 89-554 (5 U.S.C. 7531-7533), enacted September 6, 1966, gives to the heads of major U.S. Government agencies, including the Secretary of State, the power to summarily suspend and remove any employee of the agency when deemed necessary "in the interests of national security." 5 U.S.C. 7531-7533 codified the Department's basic authorizing legislation for its personnel security program.

12 FAM 227.3 Responsibilities

(TL:DS-94; 10-27-2003)

The Personnel Security/Suitability Division of the Bureau of Diplomatic Security (DS/ICI/PSS) directs the conduct of personnel security investigations of employees, applicants, contractors and others seeking access to Department of State information and/or facilities. It also assists in conducting or directing the conduct of such civilian investigations abroad for other federal agencies.

12 FAM 227.3-1 Other Agency Requests for Personnel Investigations

(TL:DS-94; 10-27-2003)

The Personnel Security/Suitability Division (DS/ICI/PSS) is the central authorizing office for requests by other agencies for personnel investigations

requiring field inquiries, employment verification and source interviews by regional security officers (RSOs). DS/ICI/PSS does not usually consider routine requests for record checks, e.g., police, embassy, credit, telephone subscriber information, etc., as constituting a personnel investigation (see 12 FAM 231.4). By mutual agreement, requests from other federal law enforcement agencies for record checks on employees of USIA and AID may be made directly to RSOs.

12 FAM 227.3-2 Investigations for Local Guard Programs

(TL:DS-94; 10-27-2003)

As a matter of policy, RSOs are responsible for conducting background checks of prospective guard personnel. In some cases, the RSO has tasked commercial contractors to conduct portions of the investigation. The RSO must in all cases be satisfied with the effectiveness of the contractor investigation. RSOs themselves must complete local police checks and must review files of appropriate agencies at post. The RSO must keep the results of these investigations for subsequent inspection by DS supervisory personnel.

12 FAM 227.3-3 DS Personnel Authorized to Conduct Personnel Investigations

(TL:DS-94; 10-27-2003)

DS special agents and contract special investigators may conduct investigations domestically. Regional security officers (RSOs) may conduct investigations abroad. Post security officers, with the instruction and guidance of regional security officers, may also conduct limited checks and inquiries in some applicant-type investigations.

12 FAM 227.4 Security Records

(TL:DS-94; 10-27-2003)

- a. DS/ICI/PSS manages and maintains the records program for the Bureau of Diplomatic Security (DS) and certifies security clearances of Department employees. DS/ICI/PSS also facilitates the review and release of Reports of Investigation (ROIs) to authorized representatives of other U.S. Government agencies in accordance with the provisions of the Privacy Act of 1974 (5 U.S.C. 552a).
- b. DS/ICI/PSS maintains security records on the following categories of individuals:

- (1) Employees and former employees of the Department;
 - (2) Applicants for Department employment who have been or are presently being investigated;
 - (3) Contractors working for the Department;
 - (4) Recipients of cultural grants;
 - (5) Individuals requiring access to the official Department of State premises who have undergone or are undergoing security clearance;
 - (6) Individuals involved in matters of passport and visa fraud;
 - (7) Individuals involved in matters of unauthorized access to classified information;
 - (8) Alien prospective spouses of U.S. citizen personnel of the Department of State;
 - (9) Individuals whose activities have a potential bearing on the security of Department or Foreign Service operations; and
 - (10) Persons relevant to providing protective services for the Secretary of State, visiting foreign dignitaries, and heads of state, and to protecting the Department's official premises.
- c. DS/ICI/PSS also retains information copies of investigations of individuals conducted abroad at the request of federal agencies and documents and reports furnished to the Department by other agencies concerning individuals whose activities the other agencies believe may have a bearing on U.S. foreign policy interests.
- d. Security files contain various types of investigatory material relating to the individuals and categories described above including:
- (1) Applications for employment; *Form* SF-171, Personal Qualifications Statement;
 - (2) *Form* SF-86, Security Investigations Data for Sensitive Positions;
 - (3) *Form* DS-1894, Reports of Investigation;
 - (4) Protective intelligence reports;
 - (5) Fingerprints;

- (6) Photographs; and
- (7) Internal memoranda.

12 FAM 227.4-1 Dissemination of Security Files

(TL:DS-94; 10-27-2003)

- a. DS/ICI/PSS ensures that the security files are only disseminated in accordance with proper procedures. The office keeps records of all requests for information, release forms, and Reports of Investigation generated in the course of DS personnel and other investigations and clearances.
- b. DS/ICI/PSS also certifies, for the Department, the status and level of employee security clearances in response to requests from other U.S. Government agencies and offices.
- c. These U.S. Government agencies may access DS security files for the following reasons:
 - (1) To make a determination of general suitability for employment or retention in employment;
 - (2) To grant a contract or issue a license, grant or security clearance;
 - (3) Pursuant to statutory intelligence responsibilities or other lawful purposes; and
 - (4) Pursuant to oversight review authority with regard to an agency's investigative responsibilities.
- d. Routine users from other U.S. Government agencies permitted access to DS security files are limited to seeing the:
 - (1) Personal Qualifications Statements (*Form* SF-171);
 - (2) Security Investigation Data for Sensitive Positions (*Form* SF-86); and
 - (3) Reports of Investigations (*Form* DS-1894).

12 FAM 227.4-2 Retention of Security Files

(TL:DS-94; 10-27-2003)

DS security records are retired or destroyed in accordance with the

published schedules of the Department (see 5 FAM Chapter 400, *Records Management*).

12 FAM 228 SPECIAL INVESTIGATIONS BRANCH

12 FAM 228.1 Scope and Authority

(TL:DS-94; 10-27-2003)

- a. The Bureau of Diplomatic Security, Special Investigations Branch (DS/CAS/SI), has the primary responsibility for administrative and operational case control of nonroutine investigations which go beyond the mandate of other DS investigative offices. It is specifically charged with conducting and/or coordinating the following:
 - (1) Special personnel security investigations such as employee misconduct and security clearance suitability;
 - (2) Unauthorized disclosure and compromise of classified and/or sensitive security information; and
 - (3) Special criminal investigations.
- b. DS/CAS/SI investigates complaints, allegations, information, and unusual incidents involving Department of State employees and all U.S. Government personnel under the authority of a chief of mission. Unusual incidents are those which go beyond routine security program concerns. In general, DS/CAS/SI investigates matters which:
 - (1) Could adversely affect an individual's security clearance and access to classified information, including special clearance, or which could affect the propriety of the individual's continued access;
 - (2) Could affect a DS decision or recommendation concerning physical, procedural, or personnel security;
 - (3) Are necessary to assess the possibility or extent of compromise of sensitive information which could damage the national security, to the extent that the Department or its missions control the information concerned and are responsible for it; and
 - (4) Must be reported pursuant to law, executive order, or regulation.
- c. Some incidents or allegations fall within the primary investigative

jurisdiction of other offices of the Department or U.S. Government agencies. However, if the matter also relates to a DS security responsibility, DS/CAS/SI will open an SI file under the appropriate case category for coordination purposes and any eventual DS action.

12 FAM 228.1-1 Post Investigations

(TL:DS-94; 10-27-2003)

The chief of mission or principal officer is responsible for efficient mission management which includes the security program. DS will inform the chief of mission of any DS/CAS/SI investigation of personnel to be initiated at post or of any matter related to the security of post operations. DS will provide necessary guidance and instructions to RSOs or DS special agents for the conduct of such investigations. As necessary, RSOs will keep the chief of mission or other key post officials informed of progress and should also consult DS Washington or request assistance as appropriate. Report immediately any modification of instructions to DS/CAS/SI.

12 FAM 228.1-2 Responsibilities to Other Agencies

(TL:DS-94; 10-27-2003)

When a matter reasonably appears to fall within the investigative jurisdiction of another agency, DS officers shall cooperate and assist that agency in carrying out its responsibilities to the extent possible. Many situations will require a careful review by DS/CAS/SI of all circumstances to ensure a balancing of the concerns of affected agencies. Prior to initiating an investigation, RSOs should alert and provide preliminary details of such cases to DS/CAS/SI for guidance. DS/CAS/SI will brief the other agency and provide the RSO with guidance on how to proceed.

12 FAM 228.2 Procedures

(TL:DS-94; 10-27-2003)

- a. DS/CAS/SI controls and supervises all special investigations. Accordingly, all matters relating to a special investigation which develop in the field must be transmitted to SI on a timely basis to enable that office to fulfill its case control responsibilities.
- b. The authority for officially opening a special investigation lies solely with DS/CAS/SI. Cases not originating from SI are not considered formally "opened" until DS/CAS/SI receives appropriate written notification and assigns a case control number.

- c. Special agents, PSOs, or RSOs receiving information and/or allegations which may merit "Special Investigations" status must submit the information to DS/CAS/SI for preliminary assessment, research, and guidance before initiating any substantive investigation. However, field personnel may conduct limited investigative activities:
 - (1) If they believe that additional information is needed for DS/CAS/SI to make a decision to open a case; and
 - (2) If security concerns require immediate action.
- d. From time to time there may be situations where insufficient information exists to formally open an SI case. In such situations, DS/CAS/SI may authorize a preliminary inquiry to determine whether or not additional investigation is warranted. Whether or not a formal case is opened will depend on the results of the preliminary inquiry.
- e. Only DS/CAS/SI can officially close a case. The DS/CAS/SI case control agent will review the completed Report of Investigation (ROI) and determine whether further investigative action is needed. The DS/CAS/SI Branch Chief must approve formal closing of an investigation. DS/CAS/SI will then so inform the concerned chief of mission or Department official.

12 FAM 228.3 Policies for Special Personnel Security Investigations

12 FAM 228.3-1 Security Implications of Misconduct

(TL:DS-94; 10-27-2003)

- a. Employee misconduct is the concern of DS/CAS/SI, particularly if an employee occupies a sensitive position or has access to classified information. Other Department offices may be involved or have an interest in certain categories of employee misconduct; for example, alcohol and drug abuse, while primarily medical concerns also pose potential security problems. 3 FAM provides for appropriate coordination between M/MED and DS on such cases in order to take any necessary security precautions.
- b. Other problems or forms of personal misconduct, such as fiscal irregularities, normally handled in other channels including the Office of the Inspector General, may also require some security review. Security officers who become aware of such problems should coordinate with the appropriate post or Department supervisors and report to DS/CAS/SI any information regarding a genuine security concern.

12 FAM 228.3-2 Suicide, Mysterious Death, or Disappearance

(TL:DS-94; 10-27-2003)

Any suicide, attempted suicide, unexplained or mysterious death, or disappearance of an employee occupying a sensitive position may have adverse security ramifications. Domestically, executive directors should report mysterious deaths or disappearances to DS/CAS/SI. Abroad, RSOs or PSOs must report such incidents to DS/CAS/SI by immediate telegram and initiate a preliminary investigation. The preliminary investigation should:

- (1) Determine the facts of the case;
- (2) Ascertain if any past, present, or future security concerns are affected; and
- (3) Prepare a damage assessment for any possible loss or compromise of classified information.

12 FAM 228.3-3 Marine Security Guards

(TL:DS-94; 10-27-2003)

- a. Marine security guards are under the operational supervision of the chief of mission at each post where they are assigned. The chief of mission exercises this responsibility through the regional security officer (RSO). The Marine Corps retains the sole responsibility for the conduct and discipline of all Marines assigned for duty with the Department of State (DOS). Pursuant to the Manual for Courts-Martial 1984, the Manual of the Judge Advocate General, and other military directives, the commanding officer, Marine security guard battalion, is responsible for the administration of military justice within the battalion. A Marine commander's inquiry/investigation must comply with due process and other procedural requirements of the Uniform Code of Military Justice.
- b. Criminal and counterintelligence investigations of Department of the Navy (DON) personnel who are currently serving with the DOS will normally be conducted by special agents of the Naval Investigative Service (NIS). If requested by the DOS, such investigations may be conducted jointly with representatives of that Service. NIS involvement should be initiated by the MSG battalion commander. The authority of NIS special agents and detachment commanders conducting preliminary inquiries and investigations is limited to MSG or DON personnel. Interviews will not be conducted with Foreign Service national (FSN) or other mission personnel without the express concurrence of the RSO.

- c. Inform the RSO of all incidents of misconduct, criminal acts, personnel problems, or other matters that might effect the security of post operations.

12 FAM 228.3-4 Personnel of Other Agencies

(TL:DS-94; 10-27-2003)

RSOs and PSOs will report potential security problems related to misconduct by personnel of other U.S. Government agencies at Foreign Service posts to the chief of mission and to DS/CAS/SI; DS will coordinate at the headquarters level with the concerned agency to determine the scope of any necessary investigative coverage.

12 FAM 228.3-5 Misconduct by Employee Family Members

(TL:DS-94; 10-27-2003)

RSOs and PSOs must report all serious allegations or complaints of misconduct, which have an effect on the post, made against family members of U.S. citizen employees to the chief of mission or principal officer. If the complaint is security-related, also notify DS/ICI/CAS. DS/CAS/SI will not initiate any special investigation except by specific direction of the chief of mission or principal officer.

12 FAM 228.3-6 Alien Employees, Contractors, and Contractor's Employees

(TL:DS-94; 10-27-2003)

- a. RSOs and PSOs should make an initial determination of the potential severity and effect on post operations of any complaints or allegations made against Foreign Service national employees (FSNs), contractors or persons employed by a contractor, and coordinate results with the chief of mission or principal officer and the Chief, Division of Counterintelligence and Special Investigations (DS/ICI/CAS), as appropriate. Either official may authorize the RSO to conduct an official investigation. Damaging information developed in an investigation may constitute a basis for appropriate administrative action, including withdrawal of the employee's certification for continued employment. Investigators must take care during the investigation to ensure that the legal rights of the FSNs, contractors, and contractor's employees are protected both under U.S. and host-government laws.
- b. RSOs and PSOs report and investigate complaints or allegations against

FSNs, contractors, or contractor's employees employed at U.S. missions abroad by other agencies in the same manner as investigations of Department FSNs. In addition to the chief of mission and the Chief of DS/ICI/CAS, they must inform the appropriate senior official of the employing agency at post, or at the agency's headquarters, if there is no representative at post, of the initiation and progress of any such investigation.

12 FAM 228.3-7 Employee Conduct Investigations

(TL:DS-94; 10-27-2003)

- a. DS/CAS/SI conducts inquiries into allegations of unlawful, aberrant, notorious, or infamous conduct involving Department employees. (See 3 FAM.)
- b. Within the context of the Department's responsibility for the conduct of foreign affairs, an employee's personal traits or practices, including sexual practices (whether heterosexual or homosexual), may be relevant to evaluating stability, character, discretion, and susceptibility to undue influence or duress.
- c. If DS receives substantive allegations that an employee is involved in sexual conduct of an illegal or exploitable nature, DS/CAS/SI will make necessary inquiries (normally directly of the employee) to determine if he or she could be subject to undue influence or duress through exploitable personal conduct. If there is nothing unlawful, aberrant, notorious or infamous about the sexual conduct, the DS inquiry will be limited to determining whether the employee's sexual orientation and/or conduct may make the individual susceptible to blackmail or coercion. If the conduct is substantiated, DS/CAS/SI refers the case to DS/ICI/PSS for appropriate review and action. (See 12 FAM 232.3.)

12 FAM 228.4 Information Security Investigations Policy

12 FAM 228.4-1 DS/IST/APB Referral of Serious Compromises of Classified Information to DS/CAS/SI

(TL:DS-94; 10-27-2003)

Normally, all security violations are administratively processed by the DS Office of Information Security Technology's Information Security Programs (DS/CIS/IST); however, the DS Special Investigations Branch (DS/CAS/SI)

investigates serious breaches of classified information handling procedures. DS/CAS/SI works closely with DS/CIS/IST on these cases.

12 FAM 228.4-2 Loss, Unauthorized Disclosure, or Serious Compromise of Classified Information

(TL:DS-94; 10-27-2003)

- a. In each instance of loss, unauthorized disclosure, or compromise of classified or administratively controlled documents and information, it is the responsibility of DS to:
 - (1) Investigate the loss;
 - (2) Assess or coordinate the assessment of the resultant damages;
 - (3) Identify the contributing or responsible persons and procedures;
 - (4) Take or recommend remedial actions;
 - (5) Make a detailed formal report of the investigation.

12 FAM 228.4-3 Objectives

(TL:DS-94; 10-27-2003)

The objectives of security actions following a loss and possible compromise of classified information are twofold:

- (1) To determine the harm to the national security caused by the loss or compromise of the classified documents or information by means of a formal investigative procedure called a damage assessment investigation; and
- (2) To prevent further loss or compromise under similar conditions by providing remedial safeguards.

12 FAM 228.4-4 Unauthorized Disclosure of Sensitive Information

(TL:DS-94; 10-27-2003)

- a. Each agency is responsible for safeguarding its classified information. An unauthorized disclosure or "leak" is the compromise of classified or administratively controlled information by unauthorized disclosure to another person. DS/CAS/SI is the DS office responsible for the conduct

of unauthorized disclosure investigations. Regardless of where the incident occurred, notify DS/CAS/SI of compromise of classified information as soon as possible so an investigation can be initiated, if warranted. If a "media leak" or other unauthorized disclosure is made of classified information, the originating agency conducts an initial investigation to determine if any other agency was on distribution for or had access to the information. Should the initial inquiry disclose that another agency had access to the information, the originating agency will request that the receiving agency conduct an appropriate investigation.

- b. Unauthorized disclosure of national security information may be a violation of federal criminal statutes and violators may be subject to prosecution by the U.S. Department of Justice. Investigations of unauthorized disclosures of nonnational security material will be conducted according to administrative guidelines. Violators are subject to administrative sanctions, up to and including separation from the federal service. (See 12 FAM 230.)

12 FAM 228.5 Physical Security Investigations Policies

12 FAM 228.5-1 Scope

(TL:DS-94; 10-27-2003)

- a. DS has investigative responsibility for any threat or actual incident involving the physical security of classified material, official premises, or U.S. Government property for which DS personnel provide direct protection or security advisory services both domestically and abroad. This includes the unauthorized entry into official premises by force or stealth, tampering with safe storage equipment or diplomatic pouches, arson, bombing, sabotage or similar incidents.
- b. If another agency or Department office has a primary or superior investigative mandate concerning a particular matter, DS personnel will cooperate fully upon request. In such cases, DS will require copies of pertinent investigative reports or summaries, to determine whether any corrective procedures are required.
- c. When no superior authority exists or when such authority is unable to carry out its investigative responsibilities due to time or personnel considerations, DS personnel will initiate the necessary preliminary inquiries. Special agents or RSOs assigned to investigate the matter will notify DS headquarters and receive guidance from DS/CAS/SI or other appropriate DS offices.

12 FAM 228.5-2 Objectives

(TL:DS-94; 10-27-2003)

The objectives of any investigation of a physical security incident or threat may include the following:

- (1) Determine the cause or source of the problem;
- (2) Determine the identity of any culpable individual(s);
- (3) Recover any U.S. Government property involved;
- (4) Identify any classified information exposed to possible compromise;
- (5) Facilitate any necessary damage assessment; and
- (6) Provide a proper basis for any necessary corrective or disciplinary action.

12 FAM 229 UNASSIGNED