ADS Chapter 569

Counterintelligence and Insider Threat Program

Partial Revision Date: 04/19/2013
Responsible Office: SEC/OD
File Name: 569_041913

Functional Series 500 - Management Services
Chapter 569 – Counterintelligence and Insider Threat Program
POC for ADS 569: Fitzgerald Bobo, (202) 712-1725, fbobo@usaid.gov

Table of Contents

Chapter 569 – Counterintelligence and Insider Threat Program

569.1 OVERVIEW

Effective Date: 12/02/2011

This ADS chapter establishes the mandatory policies and required procedures for the USAID Counterintelligence and Insider Threat Program. The primary focus of this ADS chapter is to ensure that USAID personnel understand and report potential threats from foreign intelligence and terrorism to USAID. Counterintelligence and Insider Threat awareness and education, policies and procedures are designed to ensure that USAID personnel recognize and report any of the following:

a. Attempted or actual espionage, subversion, sabotage, terrorism or extremist activities directed against USAID and its personnel, facilities, resources, and activities;

b. Indicators of potential terrorist associated insider threats;

c. Unauthorized intrusions into automated information systems;

d. Unauthorized disclosure of classified information; and

e. Indicators of other incidents that may indicate foreign intelligence or terrorism targeting USAID.

This ADS chapter applies to personnel working for USAID, to include: Direct Hire Foreign Service or General Schedule employees, Contractors, and Foreign Service Nationals (FSNs); hereinafter referred to as personnel.

USAID personnel must abide by the contents of this ADS chapter when assigned domestically and additionally **12 FAM 260, Counterintelligence** when assigned overseas, permanently or on temporary duty (TDY).

Individuals operating under a "classified contract" that are obligated to meet additional security requirements should abide by the policies and procedures outlined in their respective DD Form 254. The DD Form 254 is maintained by USAID's Office of Security (SEC) and Facility Security Officers.

569.2 PRIMARY RESPONSIBILITIES

Effective Date: 04/19/2013

a. The **USAID Director of Security (D/SEC)** is responsible for:

(1) Providing oversight of the USAID Counterintelligence (CI) and Insider Threat Program.

(2) Either internally or via agreement with external agencies, establishing the technical capability, subject to appropriate approvals, to monitor user activity on all classified networks in order to detect activity indicative of insider threat behavior.

(3) Coordinating division or higher-level approval of CI activities when required (e.g., forwarding information on matters that require a referral to the Federal Bureau of Investigations and coordination with USAID General Counsel).

(4) Developing policies and procedures for properly protecting, interpreting, storing, and limiting access to user activity monitoring methods and results to authorized personnel.

(5) Developing agreements, in coordination with the Insider Threat Program, GC, and Chief Information Security Officer (CISO), for USAID personnel with security clearances to sign and acknowledge that their activity on any agency classified or unclassified network, to include portable electronic devices, is subject to monitoring and could be used against them in a criminal, security, or administrative proceeding.

(6) Developing classified and unclassified network banners, in coordination with the Insider Threat Program, GC, and CISO, informing network users that their activity on the network is being monitored for lawful United States Government authorized purposes and can result in criminal or administrative actions against the users.

(7) Establishing reporting guidelines for Security, Information Assurance, Human Resources, and other relevant organizational components to refer relevant insider threat information directly to the Counterintelligence and Insider Threat Program.

(8) Establishing an insider threat centralized analysis, reporting and response capability.

(9) Referring issues to appropriate internal and external entities to determine disciplinary and criminal actions for personnel who fail to comply with the terms of this chapter.

(10) Ensuring professional development for USAID CI personnel.

(11) Establishing an Insider Threat Working Group with representation and support from offices within USAID to include: Security, General Counsel, Inspector General, Chief Information Office, Management Bureau, Human Resources, among other relevant organizational components, as necessary.

(12) Establishing guidelines and procedures for the retention of information necessary to complete assessments required by EO 13587.

b. The **Office of Security, Counterterrorism and Information Security Division, Counterintelligence Branch (SEC/CTIS/CI)** is responsible for:

(1) Managing and providing functional oversight of the USAID CI and Insider Threat program.

(2) Conducting CI and Insider Threat awareness training for USAID personnel.

(3) Conducting CI and Insider Threat activities as outlined in this ADS chapter.

(4) Evaluating information concerning a potential insider threat to determine in a timely manner, CI equity; and subsequently referring to appropriate offices, in accordance with reporting requirements of the ADS and related national-level policies, to determine if the information uncovered is sufficient to warrant:

- The initiation of a personnel security investigation based on suitability and fitness concerns;
- The initiation of an Inspector General investigation; and
- Response from Human Resources, Management, the Chief Information Office, General Counsel, or other offices concerning violations of ethics, privacy, among other incidents.

c. The **Office of Security, Personnel Security Division (SEC/PSD),** is responsible for referring to the Counterintelligence and Insider Threat Program, any information uncovered during the personnel security investigations and clearance review process that warrants a CI referral based on the adjudicative guidelines as well as any information reportable in accordance with section **569.3.3** of this chapter.

d. **USAID Office of Human Capital and Talent Management (HCTM)** is responsible for:

(1) Providing a list of proposed overseas assignees to SEC to allow for review of assignments to Critical Human Intelligence (HUMINT) threat posts and CI awareness training prior to departure.

(2) Ensuring assignment restrictions in accordance with **ADS 566, U.S. Direct-Hire and PASA/RSSA Personnel Security Program**.

e. USAID Insider Threat Program and Working Group Members are responsible for:

(1) Facilitating timely, and, if possible, electronic access to the information necessary to identify, analyze, and resolve insider threat matters involving their respective offices.

(2) Protecting the information, documents, files and materials provided by USAID Bureaus, Offices, and Missions in accordance with current and applicable federal laws, rules, regulations, and policy.

(3) Completing training in accordance with the White House Memorandum, "Early Detection of Espionage and Other Intelligence Activities through Identification and Referral of Anomalies," of August 23, 1996.

f. USAID personnel are responsible for:

(1) Reporting to the Counterintelligence and Insider Threat Program, all contacts, activities, indicators, or behaviors, as outlined in this ADS chapter and supporting issuances, that they observe or gain knowledge of which could adversely impact the responsible sharing and safeguarding of classified and sensitive but unclassified (SBU) information.

(2) Contacting the USAID Counterintelligence branch and following procedures in accordance with this ADS chapter for reporting CI and Insider Threat-related incidents. The CI Branch can be reached by phone at (202) 712-0990 or via unclassified email to **counterintelligence@usaid.gov**. For CLASSIFIED reporting, the USAID CI Branch can be reached via ClassNet email to **USAIDcounterintelligence@state.sgov.gov**.

(3) Abiding by the contents of this ADS chapter when assigned domestically and additionally **12 FAM 260** when assigned overseas, permanently or on temporary duty (TDY).

569.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES

569.3.1 Counterintelligence Activities

Effective Date: 04/19/2013

Counterintelligence activities include but are not limited to the following:

a. Conducting CI inquiries to establish the basis for CI investigations.

b. Maintaining a robust briefing and debriefing program.

c. Recommending changes to existing and proposed CI policy.

d. Analyzing and assessing threats posed by terrorists and foreign intelligence entities and advising the organization on potential threats.

e. Briefing the D/SEC on significant CI activities pursuant to this ADS chapter.

f. Conducting multi-disciplinary CI threat assessments of overseas USAID Missions.

g. Managing an insider threat program in coordination with other USAID offices and other agencies as appropriate.

h. Providing CI support to USAID personnel security investigations.

i. Providing CI support to USAID assignment reviews.

j. Developing and maintaining a foreign visit program to support visits to USAID/Washington by representatives of a foreign nation.

k. Coordinating polygraph and credibility assessments for USAID.

l. Conducting and/or coordinating CI inquiries and investigations with the Department of State's (DoS) Bureau for Diplomatic Security (DS) and members of the intelligence community, as appropriate.

m. In coordination with other agencies, administering the CI program overseas for USAID personnel.

n. Providing CI support to incidents involving CI in cyberspace.

o. Providing CI threat data in support of USAID Operations Security (OPSEC) Program.

p. Conducting liaison with intelligence community members, Federal partners, and local law enforcement entities.

q. Managing a prioritized CI Outreach Program to promulgate policy and conduct CI assessments in overseas Missions.

r. Conducting assignment reviews of USAID personnel proposed for permanent assignment to Critical HUMINT threat posts in accordance with 12 FAM 263.3, Post Procedures.

569.3.2 Counterintelligence and Insider Threat Awareness Training
Effective Date: 12/02/2011

In addition to the overseas threat, USAID faces the insider threat. The insider threat is exemplified by an individual or group within the Agency or related organization who attempts to compromise the mission through espionage, acts of terrorism, support to terrorist organizations or unauthorized release or disclosure of classified or Sensitive But Unclassified (SBU) information. The potential of the insider threat to cause serious damage to the mission of USAID underscores the necessity for a focused and effective CI program.

USAID personnel must receive initial, annual, and periodic training on the threats posed by the following:

a. Foreign intelligence services,

b. Terrorism,

c. Insider threats,

d. Unauthorized disclosures,

e. Computer intruders, and

f. Individual reporting responsibilities.

When assigned overseas, USAID personnel should receive training from the Regional Security Officer (RSO) or Post Security Officer (PSO). (See **12 FAM 450, Security Support Agreements** and **12 FAM 564, Briefings**).

Certain USAID personnel may be especially vulnerable to exploitation by foreign intelligence services or terrorists. Foreign intelligence services have traditionally targeted and continue to target personnel with access to sensitive compartmented information (SCI) and special access program (SAP) information.

569.3.2.1 Conduct of Counterintelligence and Insider Threat Awareness Training
Effective Date: 12/02/2011

a. SEC provides CI-awareness training at the unclassified level to ensure it reaches the widest possible audience. SEC may provide classified training to USAID personnel who possess appropriate security clearances and need-to-know accesses.

b. SEC conducts counterintelligence and insider threat training on an annual basis, as well as initially, for new personnel assigned to USAID. SEC provides refresher training to personnel as needed.

c. SEC ensures that briefing materials reflect recent and relevant examples of national security crimes (e.g., espionage and terrorism) and are tailored to both the audience and geographic area.

d. SEC presenters use a variety of awareness and educational media to develop a strong and professional presentation.

e. SEC presenters may prepare training for large audiences, small groups or individuals.

Methods:

a. **Live training by CI Agent**. Live training, wherein the CI agent is the presenter, is the preferred means of delivering CI awareness training. This offers several advantages. First, the trainer can tailor their presentation to audience needs. Second, the trainer can respond to unique situations and answer specific questions. Third, personnel can report threat-related incidents to a live agent. Fourth, the audience becomes familiar with the responsible party.

b. **Live training by approved personnel**. In certain circumstances, SEC/CTIS may designate personnel from other offices to conduct CI awareness training in order to satisfy requirements. The designated briefer and training materials must be approved by SEC/CTIS prior to conducting the training. For example, in overseas areas where USAID missions are not collocated with a US Embassy, it is possible that USAID personnel may not be briefed by the RSO or PSO regarding CI. Also, in overseas areas where there are few USAID personnel, it might not be feasible to deploy a CI agent to brief a small number of personnel. In these scenarios, approving an alternate USAID direct-hire employee to conduct the CI training in accordance with the standards outlined in this ADS chapter would be ideal.

c. **Alternative training**. When live training is not possible, CI agents may coordinate with appropriate offices to develop alternative scenarios to conduct CI awareness training and meet the requirements of this ADS chapter. Alternative training may include the use of video equipment or other electronic media, such as computer-based and web-based training.

SEC/CTIS/CI will provide CI briefings to personnel which, at a minimum, include the following discussion points:

Content of Counterintelligence and Insider Threat Awareness Training provided by SEC

- The fact that foreign adversaries consider USAID personnel to be both lucrative sources of information and attractive targets of terrorism.
- The methods and techniques used by foreign adversaries to place personnel under obligation or evoke willingness to collect information on USAID activities, personnel, and facilities, and actual situations which highlight these methods.
- The methods used by terrorists to target USAID personnel and the vulnerabilities that terrorists exploit to harm USAID.
- The means by which an "insider threat" may exploit knowledge of the organization's plans and intentions to provide operational information to the enemy, and the means which an insider may employ to target USAID personnel.
- The types of situations and indicators of both espionage and terrorism that should be reported.
- That failure to report CI incidents specified in this ADS chapter is a violation of policy and may result in disciplinary or adverse administrative action.
- The damage that espionage and the terrorist insider have caused to U.S. national security, employing recent examples as evidence.
- The intelligence threat posed by friendly foreign countries.
- The tactics and techniques used by official foreign visitors to obtain unauthorized access and/or information from USAID installations.
- The need to be cautious while accessing online social networking sites (chat rooms, blogs, and online dating sites) and the ways in which foreign intelligence services have exploited these sites to assess USAID personnel for potential future recruitment or to acquire classified or SBU information.
- Cautions against posting blogs with information about an individual's official duties, plans and intentions or any other information that may be exploited by a foreign intelligence service or terrorist organization.
- Unsolicited correspondence and how it is used by foreign intelligence and terrorist organizations.
- How to respond to and report CI and insider threat-related incidents.

569.3.3 Reporting Requirements

Effective Date: 12/02/2011

It is USAID policy that: USAID personnel must report any contact information or circumstances that could pose a threat to the security of U.S. personnel, USAID or other U.S. resources, and classified national security information (hereafter referred to as "classified information") or SBU information under **E.O. 13526, Classified National Security Information** to an appropriate authority.

Personnel who fail to comply with the USAID security policies and procedures will be subject to administrative and/or disciplinary action. (See **ADS 485, Foreign Service Discipline** and **ADS 487, Disciplinary and Adverse Actions Based on Misconduct**)

USAID personnel must cooperate with and assist CI agents in the conduct of their official duties. Personnel must refrain from discussing the details of a reported incident to anyone unless authorized by the CI agent or their representative.

569.3.3.1 Reportable CI and Insider Threat-related Incidents

Effective Date: 12/02/2011

USAID personnel must report the following:

a. Attempts by anyone, regardless of nationality, to obtain or acquire unauthorized access to classified or unclassified information concerning USAID, in the form of facilities, activities, personnel, technology or material through any of the following methods: questioning, elicitation, trickery, bribery, threats, coercion, blackmail, photography, observation, collection of documents or material, correspondence (including electronic correspondence) or automated systems intrusions.

b. Contact with an individual, regardless of nationality, under circumstances that suggest USAID personnel may be the target of attempted recruitment by a foreign intelligence service or terrorist organization.

c. Any USAID personnel who are engaging in or have engaged in actual or attempted acts of treason, spying or espionage.

d. Any USAID personnel who are in contact with persons known or suspected to be members of or associated with a foreign intelligence service or services, security or terrorist organizations.

e. Any USAID personnel who have contact with anyone possessing information about the following: planned, attempted, suspected or actual terrorism, espionage, sabotage, subversion or other intelligence activities directed against USAID or the United States.

f. Any USAID personnel who are providing financial or other material support to terrorist organizations or to someone suspected of being a terrorist.

g. Any USAID personnel who are associated with or have connections to known or suspected terrorists.

h. Any USAID personnel who are in contact with any official or citizen of a foreign country when the foreign official or citizen:

(1) Exhibits excessive knowledge of or undue interest in USAID

personnel or their duties beyond the normal scope of friendly conversation.

(2) Attempts to obtain classified or SBU information.

(3) Attempts to place USAID personnel under obligation through special treatment, favors, gifts, money or other means.

(4) Attempts to establish business relationships that are outside the scope of normal official duties.

i. Incidents in which USAID personnel or their family members traveling to or through foreign countries are contacted by persons who represent a foreign law enforcement, security or intelligence organization and

(1) Are questioned about their duties.

(2) Are requested to provide classified or unclassified information.

(3) Are threatened, coerced or pressured in any way to cooperate with the foreign official.

(4) Are offered assistance in gaining access to people or locations not routinely afforded Americans.

j. Known or suspected unauthorized disclosure of classified information to those not authorized to have knowledge of it, including leaks to the media.

k. Any USAID personnel who remove classified information from the workplace without authority or who possess or store classified information in unauthorized locations.

l. Attempts to encourage USAID personnel to violate laws or disobey lawful orders or regulations for the purpose of disrupting governmental activities (subversion).

m. Any USAID personnel participating in activities advocating or teaching the overthrow of the U.S. Government by force or violence, or seeking to alter the form of Government by unconstitutional means (sedition).

n. Known or suspected intrusions by a foreign entity into classified or unclassified information systems.

o. Incidents in which authorized users of Government information systems attempt to gain unauthorized access or attempt to circumvent security procedures or elevate their access privileges without approval.

p. Transmission of classified or SBU information using unauthorized communications or computer systems.

q. Anomalous or uncharacteristic behavior, unusual activities or other situations that have the potential to discredit USAID, individuals associated with USAID or USAID operations. Disreputable behavior may affect the employee's eligibility to receive or maintain a security clearance (See **ADS 566**).

569.3.3.2 Behavioral Threat Indicators

Effective Date: 12/02/2011

In an effort to raise awareness and vigilance, USAID personnel are encouraged to report, in accordance with the instructions in section 569.3.2.2, information regarding USAID personnel who exhibit any of the behaviors that may be associated with potential espionage or terrorist threats and those associated with extremist activity that may pose a threat to USAID or the U.S., as described in the following. A single indicator by itself does not necessarily mean that a person is involved in activities that threaten USAID or the U.S. However, reporting the behavior to the counterintelligence office will allow CI agents to appropriately assess the threat potential or if appropriate, refer the incident to another agency.

Indicators of Espionage	
Behaviors	**Indicators**
Foreign influence or connections	• Frequent or regular contact with foreign persons from countries which represent an intelligence or terrorist threat to the U.S. • Unauthorized visits to a foreign embassy, consulate, trade or press office, either in the U.S. or overseas. • Unreported contact with foreign government officials outside the scope of official duties. • Business connections, property ownership or financial interests internal to a foreign country. • Sending large amounts of money to persons or financial institutions in foreign countries. • Receiving financial assistance from a foreign government, person or organization.

Disregard for security practices	• Discussing classified information in unauthorized locations. • Improperly removing security classification markings from documents and computer media. • Bringing unauthorized cameras, recording or transmission devices, laptops, modems, electronic storage media, cell phones, or software into restricted areas where classified data is stored, discussed or processed. • Repeated involvement in security violations. • Removing, downloading or printing classified data from government computer systems without prior approval. • Requesting witness signatures on classified document destruction forms when the witness did not actually observe the destruction.
Unusual work behavior	• Attempts to expand access to classified information by repeatedly volunteering for assignments or duties beyond the normal scope of responsibilities. • Attempts to obtain information for which the person has no authorized access or need to know. • Using copy, facsimile machines, document scanners or other automated or digital equipment to reproduce or transmit classified material which appears to exceed job requirements. • Repeatedly performing non required work outside of normal duty hours, especially if unaccompanied. • “Homesteading” (requesting duty extensions in one assignment or location), when the assignment offers significant access to classified information. • Manipulating, exploiting or hacking government computer systems or local networks to gain unauthorized access.
Financial matters	• Unexplained or undue affluence without a logical income source. • Free spending or lavish display of wealth which appears beyond normal income. • A bad financial situation that suddenly reverses, opening several bank accounts containing substantial sums of money, or the repayment of large debts or loans. • Sudden purchases of high value or luxury items where no logical income source exists. • Attempts to explain wealth as an inheritance, gambling luck or a successful business venture, without facts supporting the explanation.
Foreign travel	• Frequent or unexplained trips of short duration to foreign countries. • Travel that appears unusual or inconsistent with a person’s interests or financial means.
Undue interest	• Persistent questioning about the duties of coworkers and their access to classified information, technology or information systems. • An attempt to befriend or recruit someone for the purpose of obtaining classified or unclassified information.

Soliciting others	• Offers of extra income from an outside venture to those with sensitive jobs or access. • Attempts to entice coworkers into criminal situations which could lead to blackmail or extortion. • Requests to obtain classified information to which the requestor is not authorized access.

Indicators of potential terrorist-associated insider threats

• Advocating support for terrorist organizations or objectives.
• Expressing hatred of American society, culture, government or principles of the U.S. Constitution.
• Advocating the use of unlawful violence or force to achieve goals that are political, religious or ideological.
• Sending large amounts of money to persons or financial institutions in foreign countries.
• Expressing a duty to engage in violence against the U.S. in support of a terrorist cause.
• Purchasing bomb-making materials or obtaining information about the construction and use of explosive devices or statements about acquiring materials to make a bomb.
• Expressing support for persons or organizations that promote or threaten the unlawful use of force or violence.
• Advocating loyalty to a foreign interest over loyalty to the U.S.
• Financial contribution to a foreign charity or other foreign cause linked to support to a terrorist organization.
• Evidence of terrorist training or attendance at terrorist training facilities.
• Repeated viewing of Internet Web sites, without official sanction, that promote or support terrorist themes.
• Posting comments or exchanging information, without official sanction, at Internet chat rooms, message boards or blogs that promote the use of force directed against the U.S.
• Joking or bragging about working for a foreign intelligence service or associating with terrorist activities.

569.3.3.3 Reporting Procedures

Effective Date: 12/02/2011

a. Individual Response

Personnel who know about a CI or insider threat-related reportable incident or are involved in a CI or insider threat-reportable situation, should do the following:

(1) Remain calm.

(2) If the incident involves a possible approach by foreign intelligence, remain noncommittal, neither refusing nor agreeing to cooperate.

(3) Do not, under any circumstances, conduct your own investigation or attempt to follow the other persons involved.

(4) Make note of the date, time, and place of the incident. Report the following information to the supporting CI office, if known or observed:

a. The physical description or identity of the person.
b. The license plate numbers and description of any vehicles involved.
c. Names of any witnesses or others who know about it.
d. Details of the incident.

(5) Limit knowledge of a CI-related incident to persons who have an absolute need to know.

b. Reporting CI and Insider Threat Incidents

(1) USAID personnel assigned domestically must report CI and insider threat-related incidents specified in section 569.3.2.1 to the Office of Security/Counterintelligence Branch within 24 hours after learning of the incident. The CI Branch can be reached by phone at (202) 712-0990 or via unclassified email to **counterintelligence@usaid.gov**. For CLASSIFIED reporting, the USAID CI Branch can be reached via ClassNet email to **USAIDcounterintelligence@state.sgov.gov**.

(2) When in an overseas environment, personnel must report CI-related incidents to the RSO in accordance with **12 FAM 262, Security Awareness and Contact Reporting** and **12 FAM 550, Security Incident Program**.

(3) USAID personnel are encouraged to read and report the behavioral indicators outlined in the additional help document to the Office of Security/Counterintelligence Branch as soon as possible after becoming aware of the information.

(4) If a CI agent is not available or a report cannot be made directly to the CI branch, contact the security office, explaining that you need to report a CI incident. Security will refer reports as securely and expeditiously as possible, but in all cases within 24 hours of being informed of the incident, to the CI branch, or

(5) If another person seeking to report a CI matter contacts you, assist the person in contacting the CI branch or a CI agent. Do not attempt to gather and report the information yourself. The CI agent requires direct access to the person who has firsthand knowledge of the incident. Do not share knowledge of the CI incident with unauthorized third parties.

c. Fabricated Reporting

Personnel who report threat-related incidents, behavioral indicators or CI and insider

threat matters that are intentionally false or fabricated may be subject to disciplinary or administrative action.

d. Obstruction of Reporting

USAID personnel and/or supervisors must not obstruct or impede any USAID employee from reporting a CI or insider threat-related incident, behavioral indicator or other CI matter.

569.3.4 Foreign Travel

Effective Date: 12/02/2011

The following requirements apply regardless of the threat level of the post where the USAID personnel are stationed or the threat level at the employee's departure location. Post threat levels are listed in the Security Environment Threat List (SETL) which is a classified document published by DoS on a semi-annual basis that defines the CI program requirements at post. The SETL is available on the classified network via links on the State Department's Web site and is also maintained by SEC. If personnel do not have access to the classified network, personnel must consult with SEC to determine threat-level listed in the SETL.

a. In accordance with 12 FAM 264, USAID personnel stationed overseas must notify the RSO or PSO of personal travel to countries with a critical human intelligence (HUMINT) threat post and certain countries with which the US does not have diplomatic relations, which are both listed in the SETL. Personnel should report foreign travel and schedule a defensive CI briefing at least two weeks before starting personal travel. Personnel must provide a notification of personal travel using the Foreign Travel Reporting Form or **12 FAM 264, Exhibit 264.2**. The RSO, PSO, or SEC will retain this information as part of the permanent record.

b. USAID personnel assigned domestically, especially those possessing a security clearance, are encouraged to contact SEC at least two weeks in advance of intended duty related or personal travel, to determine threat-level based on the SETL. Personnel may email their itinerary to the SEC/CTIS/CI group inbox at **counterintelligence@usaid.gov**. For CLASSIFIED reporting, the USAID CI Branch can be reached via ClassNet email to **USAIDcounterintelligence@state.sgov.gov**. SEC will review the itinerary against the SETL to determine if the travel is to a country with a critical HUMINT threat rating. SEC will notify the employee of any additional requirements necessary to complete prior to departure or upon return from travel. Additional requirements include a defensive CI briefing from SEC prior to travel to ensure compliance with country clearance requirements and travelers must also participate in a debriefing upon their return. SEC will only notify the traveler if additional requirements are necessary. SEC review of itineraries is not a step in the

approval process of personal travel and should not be considered agency approval or denial to travel.

c. The RSO, PSO or SEC, through DS, should provide pertinent information from the travel notification to U.S. embassies in the countries listed on the itinerary at least two weeks before the traveler's intended departure. SEC should coordinate with RSOs and PSOs for copies of their communications.

d. Travelers must immediately contact the nearest U.S. Consul, Attaché, RSO or duty officer if they are detained or subjected to significant harassments or provocation while traveling. Upon return to post of residence or USAID/W, the traveler must report any unusual incidents, including those of potential security concerns, to SEC, the RSO or PSO, as appropriate.

e. Personnel that have access to Sensitive Compartmented Information (SCI) have a special security obligation and are required to give advanced notification to SEC/CTIS, of their plans to travel overseas. Prior to such travel, personnel with SCI clearances must receive a defensive security briefing from SEC/CTIS. These special restrictions apply while individuals actively hold SCI clearances and for one year after their access to SCI has been terminated (See **Director of Central Intelligence Directive (DCID) 1/19**, **DCID 1/20** and **Intelligence Community Directive (ICD) 704**).

f. Spouses and adult dependents of personnel are encouraged to advise the RSO, PSO or SEC, as appropriate of their personal travel and to receive any available defensive security briefings, especially those at post of residence.

569.3.5 Foreign Contact

Effective Date: 12/02/2011

The President has directed via **Security Awareness and Reporting of Foreign Contacts, Presidential Decision Directive PDD/NSC-12, 05 August 1993**, that each department or agency of the U.S. Government must establish procedures, in consultation with the Department of Justice, requiring its employees to report all contacts with individuals of any nationality, either within or outside the scope of the employee's official activities, whenever

(1) An individual or group seeks illegal or unauthorized access to classified or otherwise sensitive information, or

(2) The employee is concerned that they may be the target of actual or attempted exploitation by a foreign entity.

In addition to the aforementioned topics, USAID personnel must report:

(1) Unofficial contact with a national from a country with Critical HUMINT Threat posts listed on the SETL if the employee and/or critical threat foreign national suggest, agree to, or actually have a second meeting after an initial encounter.

(2) Contact and/or association with a person or organization who the employee knows or suspects advocates the unlawful overthrow of the U.S. Government.

(3) Contact and/or association with a person who the employee knows or suspects is a member or supporter of foreign terrorist organizations.

(4) Unofficial contact with a person who the employee knows or suspects is a member of a foreign intelligence agency, regardless of nationality.

All USAID personnel assigned domestically or overseas, either permanently or on TDY, must immediately report any contacts with individuals of any nationality that occur under the circumstances referenced in this ADS chapter and **12 FAM 262.1** to SEC, RSO or PSO. USAID personnel must submit the report within one business day after the contact occurs. If you are assigned domestically and are unable to report within this time or if you are unsure about the need to report, you must notify SEC as soon as possible. If the RSO or PSO is unavailable, you must notify the Administrative Officer or the Deputy Chief of Mission.

All USAID personnel must provide the contact report to SEC. If you are a Government employee and possess access to the USAID intranet, then you should use the online reporting link on the USAID intranet portal to report foreign contacts **http://inside.usaid.gov/SEC/reportable_contact.html**.

If assigned overseas, USAID personnel must also outline the information regarding contact reports in the format described in **12 FAM 262**.

Reporting contacts under this CI program is not accomplished by, nor does it constitute the reporting required by **ADS 566** and **12 FAM 275, Reporting Cohabitation with and/or Intent to Marry a Foreign National**. Personnel must notify SEC (domestically) and RSOs or PSOs (overseas) of impending cohabitation or marriage to a non-U.S. citizen regardless of nationality. Notification of intent to marry a non U.S. citizen must be provided to SEC at least 90 days prior to actual marriage.

USAID supervisors, rating officers, and other USAID personnel with firsthand knowledge of security concerns involving a USAID employee must bring the concerns to the attention of SEC (domestically) or the RSO or PSO (overseas).

569.3.6 Briefing/Debriefing
Effective Date: 12/02/2011

a. As necessary, SEC will provide CI briefings to USAID personnel prior to departure for overseas assignments, overseas personal travel, and any travel to areas listed as Critical HUMINT Threat countries.

b. All personnel completing a tour of duty must receive a special in-depth CI debriefing conducted by SEC or, in the case of direct transfers, by the RSO or PSO of the gaining post. All PSC personnel must receive a special CI debriefing by either SEC or RSO. All TDY personnel must receive a special CI debriefing by SEC upon completion of the TDY or, in the case of TDY from one post to another, by the RSO or PSO of the post of residence. The RSO at the post of departure should notify DS/ICI and the RSO at a gaining post of USAID employee transfers so that debriefings can be scheduled. RSOs should forward copies of all special debriefings of USAID personnel to SEC.

c. For personnel assigned overseas, in the event that SEC is unable to travel to perform the briefing/debriefing in a timely manner, the RSO or PSO is responsible for conducting briefing/debriefing and awareness in accordance with **12 FAM 260**. The RSO or PSO should conduct a routine departure security debriefing for all USAID personnel completing a tour of duty at a post abroad prior to the employee's departure from post.

569.3.7 Special Access Programs
Effective Date: 12/02/2011

All USAID personnel that possess special access clearances must abide by any additional requirements as outlined in the Director of Central Intelligence Directives (See **DCID 1/19**, **DCID 1/20**, and **ICD 704**).

569.3.8 Polygraph Examinations
Effective Date: 12/02/2011

In some instances, USAID personnel may require a polygraph examination for certain voluntary assignments or voluntary details to other agencies. All polygraph examinations of USAID personnel will be consistent with guidance of the executive branch under the U.S. Constitution and laws of the United States, including those contained in Title 5, of the United States Code, the Foreign Service Act of 1980 (**22 U.S.C. 3901**), enabling legislation of the foreign affairs agencies, implementing Executive Orders, regulations, and directives, and the Employee Polygraph Protection Act (**29 U.S.C. 2001** et seq.).

a. USAID personnel must agree to submit to a polygraph for those sensitive positions in other U.S. agencies which require a polygraph examination. The polygraph in these instances is required to assist in determining the

employee's eligibility for initial or continued voluntary duty in those agencies.

b. SEC is the designated point of contact for polygraph examinations. SEC will coordinate with counterpart agencies to obtain polygraph examination services for USAID and to manage polygraph results.

569.4 MANDATORY REFERENCES

569.4.1 External Mandatory References

Effective Date: 04/19/2013

a. 12 FAM 260, Counterintelligence

b. 12 FAM 262, Security Awareness and Contact Reporting

c. 12 FAM 263.3-2, Critical Human Intelligence Threat Posts

d. 12 FAM 270, Security Reporting Requirements

e. 12 FAM 450, Security Support Agreements

f. 12 FAM 540, Sensitive But Unclassified Information (SBU)

g. 12 FAM 550, Security Incident Program

h. 12 FAM 564, Briefings

i. DCID 1/19, Security Policy for Sensitive Compartmented Information and Security Policy Manual, of March 1, 1995

j. DCID 1/20, "Security Policy Concerning Travel and Assignment of Personnel with Access to Sensitive Compartmented Information (SCI)," of December 29, 1991

k. EO 10450, "Security Requirements for Government Employment," of April 27, 1953

l. EO 12333, "United States Intelligence Activities," of December 4, 1981 (Amended)

m. EO 13526, "Classified National Security Information," of December 29, 2009

n. EO 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," of October 7, 2011

o. ICD 704, Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information, 01 October 2008

p. PDD/NSC-12, "Security Awareness and Reporting of Foreign Contacts," of August 5, 1993

q. Section 811 of the Intelligence Authorization Act for FY 1995

r. White House Memorandum, "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs," of November 21, 2012

569.4.2 Internal Mandatory References
Effective Date: 12/02/2011

a. ADS 566, US Direct-Hire and PASA/RSSA Personnel Security Program

b. ADS 567, Classified Contracts, Grants, Cooperative Agreements, and PSC/Recipient Personnel Security

c. ADS 568, National Security Information Program

569.5 ADDITIONAL HELP
Effective Date: 12/02/2011

There are no additional help documents for this chapter.

569.6 DEFINITIONS
Effective Date: 12/02/2011

The terms and definitions listed below have been included in the ADS Glossary. See the **ADS Glossary** for all the ADS terms and definitions.

access
The ability and opportunity to obtain knowledge of classified information. An individual is considered to have access by being in a place where national security information is kept, processed, handled, or discussed, if the security control measures that are in force do not prevent that person from gaining knowledge of such information. (**Chapters** 562, 566, 567, 568, **569**)

classified award
Contracts, grants, or cooperative agreements with positions requiring access to classified information and/or designated Restricted Space. These procedures are applicable to licensees, grantees, and certificate holders to the extent legally and practically possible within the constraints of applicable law and the Code of Federal

Regulations. (**Chapters 562**, **567**, **569**)

classified national security information (classified information)
Information that has been determined pursuant to **E.O. 12958** or any predecessor order to require protection against unauthorized disclosure and is marked (Confidential, Secret, or Top Secret) to indicate its classified status when in documentary form. It is also referred to as classified information.

(a) Confidential: Information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

(b) Secret: Information of which the unauthorized disclosure could reasonably be expected to cause serious damage to the national security.

(c) Top Secret: Information of which the unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security. (**Chapters 545**, **552**, **562**, **566**, **567**, **569**)

counterintelligence
Information gathered and activities conducted to detect, deter, or defend against espionage and other intelligence activities conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities. (**Chapter 569**)

counterintelligence analysis
The conversion of processed information into intelligence through the integration, evaluation, analysis, and interpretation of all source data and the preparation of intelligence products in support of known or anticipated user requirements. (**Chapter 569**)

counterintelligence awareness and education
Training is designed to ensure that USAID personnel recognize and report incidents and indicators of attempted or actual espionage, subversion, sabotage, terrorism or extremist activities directed against USAID and its personnel, facilities, resources, and activities; indicators of potential terrorist associated insider threats; illegal diversion of technology; unauthorized intrusions into automated information systems; unauthorized disclosure of classified information; and indicators of other incidents that may indicate foreign intelligence or terrorism targeting of USAID. (**Chapter 569**)

counterintelligence inquiries and investigations
An official, systematic, detailed examination or inquiry to uncover facts to determine the truth of a matter regarding a person or other entity who is or may have engaged in espionage; to detect and identify foreign intelligence collection against USAID; to detect and identify other threats to national security; to determine the plans and intentions of a terrorist group or other foreign adversary which presents a threat to lives, property, or

security of USAID; to determine the extent and scope of damage to national security; and to identify systemic vulnerabilities. (**Chapter 569**)

counterintelligence threat assessment
Examining the capabilities, intentions, and activities, past and present, of Foreign Intelligence Services and terrorist organizations as well as the security environment within which friendly forces operate to determine the level of threat. (**Chapter 569**)

Critical Human Intelligence (HUMINT) Threat post
A posting in a region or country where CI and/or HUMINT threat-levels are listed as high. (**Chapter 569**)

espionage
The act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense foreign policy with an intent or reason to believe that the information may be used to the injury of the United States or to the advantage of any foreign nation. The offense of espionage applies in time of war or peace. (**Chapters 562**, **569**)

insider threat
A person, known or suspected, who uses their authorized access to USAID facilities, systems, equipment, information or infrastructure to damage, disrupt operations, commit espionage on behalf of a foreign intelligence entity or support terrorist organizations. (**Chapter 569**)

liaison
That contact or intercommunication maintained between related offices and other agencies to ensure mutual understanding and unity of purpose and action. (**Chapter 569**)

need to know
A determination made by a possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to, knowledge, or possession of the classified information in order to perform official duties. The determination is not made solely by virtue of an individual's office, position, or security clearance level. (**Chapters 562**, **566**, **567**, **568**, **569**)

personnel
Personnel working for USAID, to include: Direct Hire Foreign Service or General Schedule employees, Personal Services Contractors (PSCs), and Foreign Service Nationals (FSNs). (**Chapter 569**)

sabotage
An act or acts with the intent to injure, interfere with, or obstruct the national defense or foreign policy of a country by willfully injuring, destroying, or attempting to destroy national defense or war material, premises, or utilities, to include human or natural

resources. (**Chapters 562**, **569**)

Security Environment Threat List (SETL)
A classified document published by DOS on a semi-annual basis that defines the threat levels at each post and defines the CI program requirements at post. (**Chapter 569**)

sensitive compartmented information (SCI)
All information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentalization have been or will be formally established. (**Chapter 569**)

subversion
An act or acts inciting USAID personnel to violate laws, disobey regulations, or disrupt official activities with the willful intent to interfere with, or impair the loyalty, morale, or discipline of USAID's personnel or mission. (**Chapter 569**)

terrorism
The unlawful use or threatened use of force or violence against individuals or property to coerce or intimidate governments or societies, often to achieve political, religious, or ideological objectives. (**Chapters 562**, **563**, 569)

threat level
Department of State (DOS) has developed six threat categories for use in defining the nature of threats at overseas posts: 1) Transnational Terrorism; 2) Indigenous Terrorism; 3) Political Violence; 4)Human Intelligence; 5) Technical; and 6) Crime. Within these four categories there are four threat levels indicating the frequency of threats directed against the U.S. official community:1) Critical; 2) High; 3) Medium; and 4) Low. Determinations of threat levels for each category at each post are based on the DOS Security Environment Threat List (SETL), issued semi-annually by DS/DSS/ITA. (**Chapters 562**, **563**, 569)

569_021522