ADS Chapter 566

Personnel Security Investigations and Clearances

Full Revision Date: 12/02/2011
Responsible Office: SEC/PS
File Name: 566_120211

Functional Series 500 - Management Services
ADS Chapter 566 - Personnel Security Investigations and Clearances
POC for ADS 566: Tara Debnam, tdebnam@usaid.gov

This chapter has been revised in its entirety.

Table of Contents

Functional Series 500 - Management Services
ADS Chapter 566 - Personnel Security Investigations and Clearances

566.1 OVERVIEW

Effective Date: 09/26/2011

This chapter covers personnel security background investigations conducted on direct-hire employees, United States Personal Service Contractors (USPSCs), institutional contractors, and other categories of personnel. The subsequent adjudication of these investigations form the basis for the issuance of a Federal Personal Identity Verification card (PIV card) or any other badge or building pass which provides unescorted access to USAID space and/or access to classified National Security information.

566.2 PRIMARY RESPONSIBILITIES

Effective Date: 09/26/2011

a. The **Office of Security (SEC)** is responsible for conducting personnel security investigations for employees to determine the security eligibility of USAID employees and personal services contractors (PSCs). SEC also conducts background investigations on institutional contractors working under unclassified contracts for the purposes of facility access as required under **Homeland Security Presidential Directive 12 (HSPD-12)**.

b. The **Director of Security (D/SEC)**

(1) Is the designated Senior Agency Official under **Executive Order (EO) 12968, Access to Classified Information**;

(2) Directs and administers the USAID personnel security program; and

(3) Chairs the USAID Security Clearance Review Panel (SCRP) or designates an alternate.

c. The **Deputy Director of Security (DD/SEC)** is the decision authority (or designates an alternate) for the reduction, denial, or revocation of an individual's eligibility for access to classified National Security information.

d. The **Chief of the Personnel Security Division (SEC/PS)**

(1) Issues assignment restriction recommendations for initial security clearances with the advice and counsel of the Chief, Counter-Terrorism Information Security Division (SEC/CTIS);

(2) Directs the administrative withdrawal (non-punitive) of an individual's personnel security clearance and any approved special access due to a prolonged absence from the Agency of a direct-hire or USPSC employee;

(3) Suspends security clearances and periodically reviews the status of conditional clearances and clearance suspensions; and

(4) Authorizes special investigations to resolve derogatory or potentially disqualifying information which may have a bearing on an individual's eligibility to retain their security clearance or facility access authorization or continued suitability or fitness for Government employment.

e. The **Executive Secretariat (ES)** is the approval authority for determining whether positions require the incumbent to have access to Sensitive Compartmented Information (SCI) and whether that access is retained with position transitions. When determined appropriate by ES, they will notify the Agency's hiring authority to permit the appropriate change of position sensitivity in the Agency's official manning document (**USAID Staffing Pattern**).

f. The **Federal Bureau of Investigation (FBI)** is responsible for conducting investigations for all persons nominated by the President for positions which are subject to Senate confirmation.

g. The **Assistant Inspector General for Management (AIG/M)** is responsible for making suitability determinations as outlined in **5 CFR 731.104** for Inspector General direct-hire employees and takes appropriate adverse actions against current federal employees as stipulated in **5 CFR 752.404,** including written continued employment determinations based on potentially disqualifying information furnished by SEC or any other federal law enforcement or investigation entity.

h. The **Deputy Assistant Administrator for Human Capital and Talent Management (DAA/HCTM)**

(1) Serves as an SCRP member (or designates an alternate);

(2) Implements assignment restrictions or recommendations;

(3) Works with Bureaus and Independent Office (B/IO) management to make position sensitivity and public trust designations for General Schedule (GS) and other positions within their organizations; and

(4) Ensures any and all changes to position designations are officially recognized and recorded in the USAID Staffing Pattern.

i. The **Chief of the Employee and Labor Relations Division (HCTM/ELR)**

(1) Reviews adverse information collected by SEC during the course of an initial or follow-up background investigation and makes suitability determinations for USAID direct-hire employees as outlined in **5 CFR**

731.203 and makes fitness for duty decisions for employees not in the competitive service as outlined in **Executive Order (EO) 10450, Security Requirements for Government Employment**.

(2) Takes appropriate adverse actions against current Federal employees as stipulated in **5 CFR 752.404/EO 10450,** including written continued employment determinations based on potentially disqualifying information furnished by SEC or any other federal law enforcement or investigation entity.

(3) Reviews adverse information collected by SEC during the course of an initial or follow-up background investigation and makes fitness for duty determinations for U.S. Personal Service or Institutional Contractors working on unclassified contracts as outlined in **Executive Order (EO) 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information** (using the same standards defined in **EO 10450**).

(4) Notifies the appointment authority when a USPSC or institutional contractor is found unsuitable or unfit for employment.

(Note: The Agency Deputy Administrator will make the suitability determinations for Administratively Determined positions and Political Appointees.)

j. The **Designated Agency Ethics Official (DAEO)** is responsible for serving as a Security Clearance Review Panel (SCRP) member.

k. Assistant Administrators and Directors of Independent Offices (and designees) make the position sensitivity and public trust designations (in conjunction with the AMS Officers) for all General Schedule (GS) and Administratively Determined (AD) positions within their organization. Chiefs, Foreign Service Personnel and Civil Service Personnel Divisions are responsible for ensuring that subsequent changes to position designations are officially recognized and recorded in the **USAID Staffing Pattern**. They are also responsible for providing the Office of Security (SEC) with their Investigative Forecasts annually for budgetary and resource planning.

l. The Authorized Requestor is responsible for initiating all candidates into the Office of Personnel Management's (OPM's) on-line system, e-QIP (Electronic Questionnaire for Investigation Processing), for completion of the Standard Form (SF) 85, 85P, or 86 as well an initial quality review of the security package to ensure that all necessary forms have been completed, signed and dated prior to submission to SEC.

m. Supervisors, managers, and employees are responsible for reporting to SEC any behaviors, activities, or situations involving USAID employees, USPSC's and institutional contractors that may bear on the individual's eligibility to receive or retain a

security clearance. (See issues for consideration as outlined in the **Federal Adjudicative Guidelines for Determining Eligibility for Access to Classified Information**.) Security Reporting Requirements are covered by U.S. Department of State (DoS) Foreign Affairs Manual **12 FAM 270, Security Reporting Requirements**.

n. The **Security Clearance Review Panel (SCRP)** reviews derogatory information pertaining to Agency applicants and employees based on a due-process referral. The Panel either sustains or overrules the decisions to deny, reduce, or revoke an individual's eligibility for access to classified information.

o. The **Contracting Officer** is responsible for rescinding a contract offer when an individual is found unfit for employment.

p. **Bureaus and Independent Offices (B/IOs)** are responsible for designating the position sensitivity levels for their positions in conjunction with the Office of Human Capital and Talent Management.

566.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES

Effective Date: 09/26/2011

The Office of Security (SEC) conducts personnel security background investigations in accordance with the Director of National Intelligence (DNI), Director of Central Intelligence (DCI), and Office of Personnel Management (OPM). Personnel security background investigations and adjudications are primarily conducted using the standards issued under the following three EOs:

- **EO 13467** gives the Director of National Intelligence (DNI) as the new "Security Executive Agent" sole responsibility over security and public trust clearance processing and the Director of the Office of Personnel Management the responsibility to serve as the "Suitability Executive Agent".

- **EO 10450**, which provides for each agency to establish and maintain programs to ensure that the employment and retention of any civilian officer or employee is clearly consistent with the interests of the national security.

- **EO 12968, Access to Classified Information** which establishes a uniform federal personnel security program for employees who will be considered for initial or continued access to classified information.

The personnel security standards outlined in the **Intelligence Community Directive (ICD) 704** apply to positions designated as Special-Sensitive.

The scope of personnel security background investigations is based on the security clearance requirements, the public trust designation of the position, the National Security sensitivity level and the requirement for access to federal facilities and/or

information systems. No background investigation will be initiated until SEC receives all required security forms.

The OPM electronic security questionnaire (e-QIP) replaces the paper version of the Standard Form (SF), 85, 85P, and 86 for security clearances and facility access requests. These forms can be accessed by invitation only from an authorized requestor or SEC via the OPM secure portal.

USAID will not employ, or contract for personal services with, any individual until a favorable eligibility determination has been made by SEC. Unescorted access to USAID facilities will not be granted unless, at a minimum, a facility access investigation under **HSPD-12** has been conducted and favorably adjudicated. Additionally, a favorable adjudicative determination must be rendered prior to permitting a candidate unescorted access to all USAID office space, issuance of USAID credential(s), or permitting access to sensitive or classified information under the control of the Agency.

Security concerns should be reported to the USAID SEC as well as to the Regional Security Officer (RSO) for overseas posts **ADS 569.3.3**.

566.3.1 Suitability/Fitness Determinations

Effective Date: 09/26/2011

Suitability, when referring to direct-hire positions within the competitive service, is defined as determinations based on an individual's character or conduct that may have an impact on the integrity or efficiency of the service (**5 CFR 731**).

Suitability also applies to other direct-hire positions such as Foreign Service, Foreign Service Limited, Administratively Determined and part-time or intermittent interns or other direct hires which are held to the same standards as stipulated in **EO 10450**.

Fitness, when referring to an institutional contractor or USPSC, is fitness to perform work on behalf of the Government as a contractor employee (**EO 13467** and **EO 10450**).

(Note: Hereafter the term “suitability” will be used when referring to suitability for direct hires within the competitive service; the term “fitness” will be used when referring to fitness to perform work on behalf of the Government for contractor employees).

If a security investigation uncovers significant adverse information bearing on an individual's suitability/fitness, SEC will refer this information to HCTM/ELR. If the adverse information also bears on the individual’s continued eligibility for a security clearance or facility access authorization, SEC will hold in abeyance a clearance/access determination until a suitability/fitness decision is made.

HCTM/OIG/M (for IG employees) determines the employment suitability or, when appropriate, any adverse action (**5 CFR 752**) for direct-hire employees. HCTM is responsible for making the final fitness determination for the USPSC or institutional

contractor when appropriate (**EO 13467**). For Administratively Determined and Political Appointees, the Agency's Deputy Administrator will make the employment suitability determinations.

When determining suitability/fitness HCTM/ELR must:

- Review adverse information collected by SEC during the course of a background investigation;
- Notify the individual, in writing, if they are found unsuitable/unfit;

If no response/appeal is received from the individual within 30 days, provide SEC and the Authorized Requestor a final written determination as to whether the individual is suitable/fit for employment.

If it is determined that an individual is not suitable/fit for employment, the Authorized Requestor must submit to SEC a request to cancel the security investigation.

(Note: For USPSC's and institutional contractors that are found unfit, the authorized requestor will notify the contracting officer who will take appropriate action to rescind the offer.)

566.3.2 Personnel Security Background Investigations

Effective Date: 09/26/2011

Personnel Security Investigations are inquiries conducted by the Office of Security (SEC) designed to develop information pertaining to an individual for use in determining whether the employment, assignment to duties, or retention in employment of that individual is clearly consistent with the interests of National Security and USAID goals and objectives. These inquiries are designed to obtain verifiable information (whether positive or negative) about the subject of the investigation. This information will determine their

- Suitability/fitness for employment with the Agency;
- Eligibility for unescorted access to government facilities or information systems under **HSPD-12**;
- Eligibility for assignment to sensitive or critical duties; and
- Retention.

The goal of these investigative efforts is to ensure the individual's appointment is clearly consistent with the interests of National Security.

For prospective direct-hire employees, USPSC's and institutional contractors that do not already possess the level of security clearance or background investigation required for the position, a new security clearance and/or investigation must be requested from SEC.

HCTM, AMS Officers, EXOs or the authorized requestor (hereafter referred to as the "requestor") must initially submit to SEC via the SEC Investigations mailbox (**sclearances@usaid.gov**), the AID 6-1, the applicant's resume and the OF-306 form. (Note: For more information on USAID policies for transmitting and transporting Personally Identifiable Information (PII), see **ADS 508**).

SEC will process the request and verify that the clearance level requested is authorized and matches the position designation (for direct hires). If reciprocity can be applied, SEC will notify the requestor. If reciprocity cannot be applied, SEC will complete the required portions of the AID 6-1 and return to the requestor. Security clearances for institutional contractors are processed through the National Industrial Security Program (see **ADS 567**).

The applicant must complete and upload all security forms into e-QIP. Specific instructions on this process can be found on the Office of Security (SEC) Web site at: **http://inside.usaid.gov/SEC/dh-psc_clearances.html.**

SEC will return any security request that does not contain all of the required information and authorizations.

(1) For direct-hire employees the level of investigation and security clearance requested on the **Form AID 6-1, Request for Security Action** must be consistent with the level of public trust and national security sensitivity assigned to the position as reflected on the **USAID Staffing Pattern** or as designated under **566.3.2.2**, Position Sensitivity Designations. When a discrepancy exists between the AID 6-1 request and the position designation, the requestor must provide SEC with written clarification prior to the initiation of any investigation.

(2) For USPSC's or other employment categories the level of access must be consistent with the level of access defined in the statement of work in their contract or job description.

The forms and requirements for security clearance and facility access investigations can be found on the SEC Web site at: **http://inside.usaid.gov/SEC/dh-psc_clearances.html**.

SEC reserves the right to cancel any investigation if:

- The subject is unresponsive or unavailable for a security interview;

- SEC is unable to meet the Investigative Requirements as outlined in **EO 10450**, **EO 12968**, and **HSPD-12**;

- The investigation cannot reasonably be completed because the information needed to complete the investigation is not available or cannot be obtained using trusted sources; or

- Loss of Jurisdiction: the employee is no longer employed by USAID or the applicant is no longer being considered for employment with USAID.

SEC will notify the requestor upon cancellation in such cases.

566.3.2.1 Personnel Security Background Investigation Requirements or Other Employment Categories

Effective Date: 09/26/2011

SEC also conducts background investigations and adjudications for USPSC's, institutional contractors working on unclassified contracts, non-direct-hire positions for intermittent, temporary or seasonal employees, experts or consultants, or other persons employed by the Agency defined as "employees" for purposes of **EO 12968**. When no access to classified National Security information is required the individual must undergo at least a Facility Access investigation. This investigation is similar to a National Security type investigation but is adjudicated without the degree of importance considered necessary for determining eligibility for access to National Security information as described in **EO 12968**. A facility access investigation meets the investigative requirements for logical or facility access under **HSPD-12**.

No individual can be

1) Awarded a contract, or

2) Permitted to provide goods and/or services under a contract/agreement,

unless such an action/relationship is clearly consistent with the interests of National Security as determined by SEC. No individual will be employed by USAID, permitted access to classified information, allowed to work in USAID office facilities or allowed access to USAID information systems until

a. A personnel security or background investigation is completed at the level appropriate for the position (Note: Authorized requestors are permitted only to request the level of investigation consistent with the duties or access levels of the position);

b. It is determined that the individual's employment is clearly consistent with the interests of National Security and USAID goals and objectives; and

c. SEC issues a favorable adjudication or facility access eligibility determination.

SEC will not conduct a personnel security investigation for USPSC's and institutional contractors for the purpose of issuing a clearance eligibility determination, Facility Access Authorization or a building pass, unless the award contains the following:

(1) The requisite security-related clauses (**ADS 567, Classified Contracts and Contractor Personnel Security**); and

(2) A stipulation stating the contract is contingent on the award and retention of the required clearance and/or access authorization issued by SEC.

Note: See **ADS 567** for investigative policy and guidance concerning institutional contractors requiring security clearances. See **ADS 565, Physical Security Programs (Domestic)** for guidance on obtaining USAID badges and facility access policies for other Federal agency employees and individuals assigned to USAID.

566.3.2.2 Position Sensitivity Designations

Effective Date: 09/26/2011

Every direct-hire position must have a designation indicating the level of security clearance and/or facility access required to perform the duties of the position. (Note: For USPSCs, the level of security clearance required to perform under the contract is determined by the operating unit).

Positions requiring a security clearance are those requiring the incumbent to work with classified information or work in areas where classified information is created, generated, discussed, handled, processed, stored or disposed of. Consideration for the need to work with classified information must include the regularly assigned work area and other office space or organizations visited on a regular or TDY basis.

The National Security Sensitivity designation options are

- Non-Sensitive – no security clearance is required,
- Noncritical-Sensitive – a Secret security clearance is required,
- Critical-Sensitive – a Top Secret security clearance is required, and
- Special-Sensitive – a Top Secret security clearance with access to Sensitive Compartmented Information (SCI) is required.

Heads of USAID Bureaus/Independent Offices (B/IOs) and their designee, in conjunction with HCTM, are required to make position designations as they have direct

knowledge of what information the positions are required to access. The designation for all USAID/Washington positions can be viewed in the **USAID Staffing Pattern**. A need to change the designation must be coordinated through the Office of Human Capital and Talent Management, Civil Service Personnel (HCTM/CSP). All positions in the Staffing Pattern for overseas locations are Foreign Service and therefore are automatically designated Critical Sensitive at a minimum. Missions desiring to designate positions as "Special Sensitive" to allow for Sensitive Compartmented Information (SCI) access must coordinate the requirement with USAID/ES and HCTM/FS.

566.3.2.3 Public Trust Designations

Effective Date: 09/26/2011

All direct-hire positions require a public trust designation of Low, Moderate or High. Non-Sensitive public trust positions do not require or provide a security clearance; however, individuals applying for or encumbering Public Trust positions are subject to background investigations, periodic updates, special investigations, and other actions. (Note: At this time, public trust designations do not apply to USPSC's.)

The basis for determining the public trust level is found in **Public Trust Designations**. The public trust designation within each Bureau/Independent Office (B/IO) is recommended by the head of the organization to HCTM and can be viewed in the **USAID Staffing Pattern**.

566.3.2.4 Employee Update Investigation Requirements

Effective Date: 09/26/2011

The National Security Policies, found in **EO 12968**, mandate periodic reinvestigations of federal employees and contractors (including USPSCs). The interval between the initial investigation and subsequent update investigations is determined by the type of investigation and level of security clearance an employee holds.

SEC will periodically conduct an investigation to update every employee's security clearance/investigation, at intervals prescribed by applicable U.S. Government Standards. SEC will notify employees, in writing, of the requirement to undergo an update investigation and initiate them into e-QIP. Employees who fail to submit the required forms and releases to permit the conduct of their update investigation may have their security clearance and access to USAID facilities and information systems suspended. In these instances, SEC will notify the employee's supervisor and the appropriate appointment authority of the employee's failure to comply and consequence.

566.3.3 Security Clearance(s)

Effective Date: 09/26/2011

The Office of Security (SEC), Personnel Security Division, manages the personnel security clearance program. SEC reviews and analyzes investigations of employment

candidates, employees and others seeking access to USAID to ensure that granting an individual access to classified information is clearly consistent with the interests of national security.

566.3.3.1 Clearance Requirements

Effective Date: 09/26/2011

a. A Top Secret security clearance is required for all officers and employees who are:

- Appointed by the President with the advice and consent of the Senate;
- Appointed to a position to which the basic rate of pay is fixed according to Executive Levels I – V under **5 USC Chapter 53, Subchapter 2**;
- In a position for which the basic rate of pay is equal to or greater than Level V of the Executive Schedule;
- In the Foreign Service (FS);
- General Schedule (GS) employees working in positions designated Critical-Sensitive or Special-Sensitive; or
- USPSC's requiring access to National Security information classified at the Top Secret level. (Note: This requirement must be specified in the contract and justified by the duties of the position.)

b. A Secret security clearance, or appropriate level of investigation based on the public trust and national security sensitivity, is required for all General Schedule (GS) employees working in positions designated as Noncritical-Sensitive and USPSCs requiring access to National Security information classified at the Secret level;

c. Individuals in positions designated as Non-Sensitive will not be issued a security clearance; however, they will be subject to an appropriate level investigation for their determined position and granted facility access, as deemed appropriate by the Office of Security;

d. Domestic, non-U.S. citizens, such as legal aliens and/or green card holders, will be subject to the appropriate level of investigation as well. (Note: If an individual is unable to provide the required and/or a sufficient amount of verifying information needed to conduct the appropriate level of investigation, access will be denied and the investigation cancelled);

e. Individuals requiring Federal credentials or access to Government facilities or information systems, pursuant to **HSPD-12**, must have, at a minimum, been

subject to a requisite investigation prior to the issuance of this Federal Government identification card (commonly referred to as PIV or personal identity verification card). This investigation must be consistent with the investigative requirements outlined in **HSPD-12.**

When the adjudicative determination of an investigation is favorable, SEC notifies the authorized requestor of the determination by issuing an **AID Form 500-3, Security Investigation and Clearance Record**.

566.3.3.2 Investigation Requirements
Effective Date: 09/26/2011

SEC will not conduct investigations on:

- Individuals no longer employed by USAID;
- Persons employed by another government Agency/Detailees/Participating Agency Service Agreement and Resource Support Service Agreement (PASA/RSSA) employees;
- Individuals that have an open personnel security investigation by another Agency or Department;
- Non-U.S. citizen PSCs or detailees;
    - Non-U.S. citizens employed overseas (FSNs, TCNs, EFMs) as these investigations are conducted by the RSO at post
- USAID Fellows which fall under a classified institutional contract; and
- Any male born after December 31, 1959 that is not registered with the Selective Service (unless they have documentation of a legal exemption).

566.3.3.3 USPSC Clearance Requirements and Position Designations
Effective Date: 09/26/2011

The office/post issuing the USPSC contract must determine the access requirement (Top Secret, Secret, Confidential, or Facility Access [formerly Employment Authorization]) necessary for the successful performance of the contract. When a USPSC requires a Top Secret clearance, the authorized requestor (or designee) must submit the locally coordinated (Mission Director or designee, Contracting Officer (CO), and Regional Security Officer (RSO) endorsement [if overseas]; AA if located in Washington) written justification to SEC and ensure the contract statement of work is consistent with the clearance/access requested, along with the **AID Form 6-1** and a complete security packet (if required). The written justification must include the specific types of information/facilities the USPSC requires access to in order to perform work

under the terms and conditions of the contract. (Note: SEC will not initiate investigative actions on requests for Top Secret clearances for USPSCs without the required written justification).

In addition to the above, Agency contracting authorities must ensure that all USPSC contracts contain the appropriate security language, identifying the level of security clearance and/or facility access authorization the contractor must possess in order to perform under the contract. An individual contractor's inability to obtain the requisite clearance/access will be considered appropriate grounds for the Agency to terminate the contractual relationship with the USPSC.

566.3.3.4 Temporary Clearance/Facility Access

Effective Date: 09/26/2011

Once a request for security action is reviewed, SEC will make an initial eligibility determination as to whether issuance of a Temporary clearance or Facility Access is appropriate. SEC will provide an **AID Form 500-3** or cable attesting to the award of the Temporary clearance or Facility Access authorization.

SEC will notify the authorized requestor in writing if the Temporary clearance or Facility Access authorization is denied or withdrawn due to a subsequent determination of ineligibility. If derogatory information is developed SEC may, at any time, withdraw a temporary clearance. When a temporary clearance or temporary facility access is withdrawn, action must be taken by the appointment authority (or their designee) immediately to remove the person from the work place and terminate logical and physical access.

566.3.3.5 Reciprocity

Effective Date: 09/26/2011

Reciprocity is defined as the recognition and acceptance of security clearance background investigations and determinations completed by an authorized investigative or adjudicative agency of the Federal Government without further investigation or adjudication.

(See **Public Law (Pub. L) 108-458, The Intelligence Reform and Terrorism Prevention Act of 2004**, **EO 13381, Strengthening Processes Relating to Determining Eligibility for Access to Classified National Security Information**, and **EO 13488, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigation Individuals in Positions of Public Trust**).

When an **AID Form 6-1** is received, SEC will verify whether the applicant has a current and valid clearance/investigation that can be verified and/or reciprocated and notify the authorized requestor of this determination. When appropriate, SEC may request additional information.

Due to the different degrees of position sensitivity levels and public trust designations within Government, not all clearances and investigations can be reciprocated for all levels. If the clearance and/or investigation are unable to be verified or reciprocated, SEC will advise the authorized requestor that an appropriate investigation (new or updated) will be required prior to finalizing the hiring/contracting action.

566.3.3.6 Sensitive Compartmented Information (SCI) Access

Effective Date: 09/26/2011

Only employees in positions designated as Special Sensitive, or otherwise designated as requiring Sensitive Compartmented Information (SCI) access, will be processed for SCI access. (Note: Mission and Deputy Mission Directors serving in critical or high threat areas may be processed for SCI access upon assignment approval).

Requests for SCI access are processed by SEC in cooperation with the Executive Secretary (ES). All requests must be submitted by the employee's AMS Officer using the Request for SCI access, **AID Form 6-106**. The SCI request should be submitted to SEC via the SCI mailbox (**SEC-SCIRequests@usaid.gov**).

SCI requests must be approved through the respective Bureau Assistant Administrator or Independent Office Director. SCI requests will not be accepted if the request form is not completed in its entirety.

Employees may not initiate a request for SCI access when:

(1) They are in need of a periodic reinvestigation (PR), meaning their last investigation (SSBI or SSBI-PR) was completed more than five years ago.

(2) They hold a conditional clearance; although they may resubmit the request once the conditional clearance has been lifted (**566.3.5.1**).

(3) They do not hold a Top Secret clearance.

SEC will process the request and initiate any necessary investigative and/or adjudicative actions and coordinate with the designated sponsoring agency for a final eligibility determination.

An employee approved for SCI access will not be permitted access to SCI until he/she has completed a formal indoctrination briefing for this access and has completed the required Non-disclosure Agreement. SEC will provide the SCI indoctrination briefing for Agency employees assigned to USAID domestic facilities. SEC will coordinate with the servicing RSO at post if the employee is located overseas to ensure this mandatory indoctrination is received and the non-disclosure agreement is signed.

Agency employees granted access to SCI to support specific assignments/details must notify ES and SEC in writing once the assignment/posting identified in the initial request

for SCI has been terminated. ES will make a written determination to either continue or terminate the SCI access based on the employee's current or proposed assignment(s).

566.3.4 Reporting Requirements to SEC

566.3.4.1 Change in Employee Position
Effective Date: 09/26/2011

Appointment authorities must notify SEC prior to a change in the assignment or position of an employee. If the new assignment or position requires the employee possess a higher level security clearance or access managers must not provide access to that information until the requisite security clearance is issued.

When an employee's position is changed and requires a higher (or lower) level of security clearance, the authorized requestor must forward an **AID Form 6-1** to SEC indicating that a change in the employee's security clearance (upgrade or downgrade) is necessary and include any additional documents required to initiate this change.

566.3.4.2 Employee Reporting Requirements
Effective Date: 09/26/2011

Standards of conduct are set by **EO 12968** on Access to Classified Information. Employees who occupy positions of trust and handle sensitive information must report changes or incidents that may impact their clearance eligibility. Failure to comply with the standards may cause an employee's eligibility for security clearance or occupancy of a sensitive position to be reviewed and possibly revoked.

The **Federal Adjudicative Guidelines** are a valuable tool in determining if a life event or situation might result in a need to report. Self-reporting emphasizes personal integrity and is preferable to the incident or change being discovered and reported by others.

Examples of incidents and life events where reporting is required include:

- Change in Personal Status (marital, cohabitation, change in name) (**566.3.4.3**);
- Financial Problems (filing for bankruptcy, garnishment of wages, liens, evictions, inability to meet financial obligations);
- Arrests (any arrest regardless of whether charges were filed);
- Psychological/Mental Health Counseling;
    - There is no need to report if:
        - Counseling was not court ordered;

- Counseling was strictly marital, family of grief counseling (not related to violence by employee);
- Counseling was related to adjustments from service in a military combat environment;

- Counseling in and of itself is not a reason to revoke or deny eligibility for access to classified information or to a sensitive position, suitability or fitness to obtain or retain Federal employment, fitness to obtain or retain contract employment, or eligibility for physical or logistical access to federally controlled facilities or information systems;

- Substance Abuse Counseling;

- Violations, unauthorized or unlawful use involving Information Technology Systems; and

- Any behaviors, activities, or situations involving USAID employees, USPSC's and institutional contractors that may bear on the individual's eligibility to receive or retain a security clearance.

(Note: The list is not all inclusive but is developed from the **Federal Adjudicative Guidelines**.)

All reporting information and inquiries (from inside the network only) should be sent to the SEC Reporting Mailbox (**SECReporting@usaid.gov**) and will be reviewed by SEC. All information reported via this mechanism must remain unclassified.

Information reported related to foreign travel, foreign contacts, and loss or compromise of information should be directed to SEC/CTIS. (Note: See **ADS 569.3.3, Counterintelligence Program-Reporting Requirements**, for more information on reporting foreign travel and foreign contacts; see **ADS 568.3.5, National Security Information Program** for additional information on reporting loss or compromise of information or security incidents).

566.3.4.3 Use of Information Technology Systems

Effective Date: 09/26/2011

The Chief Information Officer (CIO) must report all policy infractions and violations involving information technology systems (**ADS 545**) to the Office of Security, Chief of the Personnel Security Division. This information is considered when determining an employee's continued access to classified information as defined in the **Federal Adjudicative Guidelines**, Guideline M, Use of Information Technology Systems.

Once an initial, favorable adjudication for a security clearance has been made, as long as the employee is assigned to a sensitive position or has access to classified

information, the employee falls under the Continuous Evaluation Program (CEP). This ensures the employee maintains high standards of conduct and that questionable conduct or activities are promptly reported for adjudicative assessment.

All unclassified reporting information should be sent to the SEC Reporting Mailbox (**SECReporting@usaid.gov**) from inside the network. For classified reporting, please contact SEC to obtain the appropriate point of contact and reporting procedure.

566.3.4.4 Marriage or Cohabitation with Non-U.S. Citizens

Effective Date: 09/26/2011

A cohabitant is a person with whom you share bonds of affection, obligation or other commitment as opposed to a person with whom you live with for reasons of convenience (e.g. a roommate).

The decision to cohabitate with or marry a foreign national may have consequences for the employee's future assignments, eligibility for access to classified information, and even continued employment (if the spouse or cohabitant works for a foreign government or an instrumentality of a foreign government).

Intent to cohabitate with or marry a U.S. citizen who is also a citizen of a foreign nation (a dual citizen) will be processed under the same provisions.

All direct-hire employees and USPSCs encumbering sensitive positions who intend to marry or cohabitate with non-U.S. citizens must comply with the requirements of **12 FAM 275, Reporting Cohabitation with and/or Intent to Marry a Foreign National** and **3 FAM 4191, Employees Marrying Foreign Nationals**.

USAID employees (serving both domestically and abroad) must notify their supervisor in writing at least 90 days prior to the expected date of marriage and/or co-habitation to a foreign national. Once informed, the supervisor will notify HCTM to proceed with required actions and security checks as outlined in **12 FAM 275** and **3 FAM 4191**.

Failure of an employee to provide the required notification/approval of cohabitation with or marriage to a foreign national will result in the initiation of an appropriate investigation and/or immediate suspension (which may result in revocation) of the employee's security clearance.

566.3.4.5 Dual Citizenship

Effective Date: 09/26/2011

Dual citizenship is the simultaneous possession of two citizenships. Dual citizenship results from the fact that there is no uniform rule of international law relating to the acquisition of nationality. When processing requests for applicants who are dual citizens SEC will consider whether granting a security clearance is in the best interest of National Security.

SEC is required to consider dual citizenship during the conduct of all personnel security investigations and when making security clearance determinations in accordance with the **Federal Adjudicative Guidelines**.

566.3.5 Personnel Security Clearance Access Restriction
Effective Date: 09/26/2011

a. Undue Vulnerability

(1) Circumstances may be present or develop creating the potential for undue vulnerability of an employee as it concerns National Security interests. Examples of these circumstances include, but are not limited to, having non-US citizen relatives, planned or actual marriage or cohabitation with a non-U.S. citizen, membership in foreign business associations, etc.

(2) Prior to initiating revocation or denial of a security clearance, alternatives will be sought to reduce or eliminate the source of the vulnerability. These alternatives may involve placing a restriction on the individual's access to National Security Information and/or restrictions placed on current and/or future assignments. If SEC determines that vulnerability exists, the employee must be excluded from the assignment or situation creating the vulnerability to retain their personnel security clearance.

566.3.5.1 Conditional Clearances
Effective Date: 09/26/2011

Conditional clearances are considered on a case by case basis. When a conditional clearance is awarded, employees are required to comply with conditions set forth by the Office of Security (SEC). Failure to respond, comply with, or provide documentation required to support and maintain the conditional clearance may result in suspension or revocation of the security clearance.

566.3.5.2 Clearance Withdrawals for Non-Duty Status
Effective Date: 09/26/2011

When an employee encumbering a sensitive position is placed in a non-duty status or is absent from the Agency for a period exceeding 30 calendar days (excluding approved sick, annual or home leave), the appointment authority, must

1) Notify SEC, in writing, of the reason for the absence/non-duty status and the expected date of return to duty status; and

2) Notify SEC, in writing, at least 30 days prior to the planned return of the employee and the reason for the employee's extended absence (if it was not know in advance).

SEC may administratively withdraw the clearance until the subject returns to duty. If SEC determines that the non-duty status action and/or extended absence from the Agency calls into question the employee's continued security clearance eligibility, SEC will conduct an investigation when the employee returns and re-adjudicate the employee's security clearance eligibility. In the event SEC is unable to reach a determination that the re-instatement is in the interest of National Security, the employee will be afforded due-process as described in sub-paragraph **566.3.5.3 (b)**. This policy also extends to the following:

- Agency employees who fail a directed drug test after participating in the Agency's Drug Free Workplace Program, and

- Those employees that are participating in a voluntary or directed drug or alcohol treatment program.

SEC will notify the appointment authority when a decision is reached to re-instate an administratively withdrawn clearance by issuing a revised **AID Form 500-3**.

566.3.5.3 Personnel Security Clearance Access Suspension, Denial, Reduction, and Revocation

Effective Date: 09/26/2011

a. Suspension

The Chief, SEC/PS will suspend security clearances when there are grounds to question a person's continued eligibility for access to classified information.

When an individual's access to classified information is suspended, SEC will notify the following as appropriate:

- The appointment authority;

- The head of the office of assignment;

- The Chief Information Officer (logical access);

- The Chief of the International Security Programs or the EXO if overseas, (physical access); and

- The individual in writing of the suspension and the reasons for the action.

The Chief, SEC/PS will review cases in which the suspension has exceeded 90 days and decide whether action can be taken to bring the case to closure. Subsequent reviews will be triggered after each additional 90-day period of unresolved suspension.

b. Due Process

An adverse security clearance action involves the denial, reduction, or revocation of a security clearance. Whenever an adverse security clearance action is initiated, the individual subject to the action must be afforded due process. (Note: Due process will also be afforded to employees and USPSC's whose clearances were administratively withdrawn and re-instatement is not recommended).

SEC/PS must advise the individual, in writing, of the proposed action. SEC/PS must provide the individual with an explanation concerning the basis for taking the action, containing as much detail as possible. This detailed explanation must include the following:

- Copies of all relevant documents,
- Records, and
- Reports upon which the conclusion to initiate the action is based.

Some materials may not be releasable under the constraints of the **Privacy Act** or the **Freedom of Information Act** (See **5 USC 552a** and **5 USC 552**).

The individual will be advised of the right to be represented by counsel or other representative at his or her own expense. The individual will be advised of the opportunity to reply in writing and/or in person within 30 days to a designated SEC official. If the individual meets with the Chief, SEC/PS in person, a written summary or recording of the appearance will be made part of the individual's security file.

If the conclusion reached by the Chief, SEC/PS is changed as a result of the written or personal presentation, the eligibility determination will be appropriately modified and written notification will be sent to the individual.

If the conclusion reached by the Chief, SEC/PS to recommend, deny or revoke a security clearance is unchanged by the argument and/or additional information presented by the individual during the due-process proceedings or upon expiration of the 30-day time period, a recommendation for the action (denial, reduction, or revocation) along with the investigative file will be forwarded to the Deputy Director of the Office of Security (DD/SEC) to render a decision.

(1) If the DD/SEC disagrees with the conclusion of the Chief, SEC/PS, the access eligibility determination will be appropriately modified and written notification will be sent to the individual.

(2) If the DD/SEC agrees with the conclusion, the Deputy Director must notify the individual in writing of the decision. The DD will send a letter to the individual

- Advising the individual of the decision to deny, reduce, or revoke access eligibility;

- Advising the individual of the right to appeal the decision to the USAID Security Clearance Review Panel (SCRP) within 30 days and to send the request for an appeal, in writing, to the DD/SEC;

- Advising the individual that the decision of the SCRP is final unless the SCRP decides to refer the case to the Administrator for a decision; and

- Advising that the decision of the SCRP will be provided in writing.

(3) If the individual appeals the decision, the Security Clearance Review Panel must convene

- The DD/SEC forwards the complete investigative file to the Director of Security (D/SEC), who is the Chair of the SCRP.

- The D/SEC notifies the Deputy Assistant Administrator for Human Capital and Talent Management (DAA/HCTM) and the designated Agency's Ethics Official that the SCRP must meet to issue a decision.

- In reaching its decision, the SCRP is bound by the access eligibility policy, procedure, and standards stipulated in Parts 2 and 3 of **EO 12968** and by the **Federal Adjudicative Guidelines**.

- If the decision of the SCRP is not unanimous, the SCRP forwards the file to the Administrator. The rationale and recommended decision of each SCRP member is included in the file forwarded to the Administrator. The Administrator then makes the final decision.

The Chair of the SCRP notifies the individual, in writing, of the final decision reached by the SCRP or the Administrator.

566.4 MANDATORY REFERENCES

566.4.1 External Mandatory References

Effective Date: 09/26/2011

a. **3 FAM 4191**

b. 5 CFR 731.104

c. 5 CFR 752.404

d. 5 CFR 731.203

e. 5 USC 552

f. 5 USC 552a

g. 12 FAM 270

h. Executive Order 10450

i. Executive Order 12829—National Industrial Security Program

j. Executive Order 12968

k. Executive Order 13467

l. Executive Order 13488

m. Executive Order 13381

n. Federal Adjudicative Guidelines

o. Homeland Security Presidential Directive (HSPD) 12

p. Intelligence Community Directive (ICD) 704

q. Public Law 108-458

566.4.2 Internal Mandatory References

Effective Date: 09/26/2011

a. ADS 545, Information Systems Security

b. ADS 565, Physical Security Programs (Domestic)

c. ADS 567, Classified Contracts and Contractor Personnel Security

d. ADS 569, Counterintelligence Program

e. Public Trust Designations

f. USAID Staffing Pattern

566.4.3 Mandatory Forms
Effective Date: 09/26/2011

a. **AID Form 6-1, Request for Security Action**

b. **AID 566-8 (SCI Request)**

c. **AID Form 500-3, Record of Security Action**

566.5 ADDITIONAL HELP
Effective Date: 09/26/2011

a. **8 CFR 337.1**

b. **12 FAM 080**

c. **ADS 562, Physical Security Programs (Overseas)**

566.6 DEFINITIONS
Effective Date: 09/26/2011

The terms and definitions listed below have been incorporated into the ADS Glossary. See the **ADS Glossary** for all 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**)

adjudicative guidelines
The Government-wide Adjudicative Guidelines for Determining Eligibility for Access to Classified Information issued pursuant to Executive Order 12968. (Chapter 566)

adjudicative determination
An examination of a sufficient period of a person's life to make an affirmative decision that the person is an acceptable security risk. (Chapter 566)

appointment authority
The USAID Office of Human Capital and Talent Management (HCTM) is the hiring authority for persons occupying USAID direct-hire positions. The Assistant Inspector General for Management (AIG/M) is the hiring authority for all Inspector General direct-hire positions. The Office of Acquisition and Assistance (or designated Contracting Officer) is the hiring authority for all U.S. Personal Service Contractors or Institutional Contractors. (Chapter 566)

assignment restriction
Any factor (medical, personnel, suitability, security, marriage, cohabitation, etc.) that would render the assignment of an individual to a particular position or location as not in the best interest of the U.S. Government or USAID. (Chapter 566)

authorized requestor
Direct hire employees designated as: (1) Administrative Support Officers (AMS) in USAID/Washington; (2) Executive Officers (EXO) overseas; (3) the Office of Human Capital and Talent Management (HCTM); and (4) Office of the Inspector General (OIG/M). (Chapter 566)

classified information
See the definition for classified national security information. (Chapters **562**, 566, **567**)

classified national security information
Information that has been determined pursuant to E.O. 13526 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**)

continuous evaluation program
The uninterrupted assessment of a person for retention of a security clearance or continuing assignment to sensitive duties. (Chapter 566)

contractor
Any industrial, educational, commercial, or other entity that has been granted a Facility Clearance (FCL) by a Cognizant Security Agency (CSA). (**National Industrial Security Program Operating Manual [NISPOM]**) (Chapters 566, **567**)

Contracting Officer (CO)
A person representing the U.S. Government through the exercise of his or her delegated authority to enter into, administer, and terminate contracts and make related determinations and findings. This authority is delegated by one of two methods: to the individual by means of a "Certificate of Appointment", SF 1402, as prescribed in FAR 1.603-3, including any limitations on the scope of authority to be exercised, or to the

head of each contracting activity (as defined in AIDAR 702.170), as specified in AIDAR 701.601. (**Chapter 300, 302, 304, 309, 331, 566, 621**)

credentials
Reliable forms of identification for employees, USPSC's and institutional contractors who access Federal facilities and Federal information systems. (Chapter 566)

direct-hire employee
Refers only to U.S. citizens employed as direct-hire (general schedule Civil Service) and excepted service (non-career and Foreign service), expert, consultant or Advisory Committee Member serving without compensation working for USAID. This category, for the purposes of security clearances, also refers to temporary and intermittent employment (i.e. interns-paid and unpaid) who are not hired under contract and "When Actually Employed" (WAE) employees. (Chapter 566)

dual citizenship
Dual citizenship is the simultaneous possession of two citizenships. For security clearance purposes, it typically involves a person holding US citizenship and that of another country. (Chapter 566)

electronic questionnaires for investigations processing (e-QIP)
The e-QIP system is an e-Government solution. Instead of distributing paper forms to prospective applicants and subjects of investigation, applicants will be required to use the e-QIP system to complete investigative forms on-line. The e-QIP system automates the Federal Government's hiring process, so that applicants fill out the Standard Forms on OPM's secure website and submit the information to OPM's server, where it remains. Meanwhile, the applications are transferred from OPM to the relevant Federal agencies. (Chapter 566)

facility access
(Formerly known as "Employment Authorization")
A determination based on investigative action that an individual is eligible to occupy a non-sensitive position. Facility Access grants an individual access to Sensitive But Unclassified Information (SBU) at the discretion of the holder of the SBU material. Facility Access also grants the individual access to USAID sensitive information technology systems at the discretion of the responsible system administrator. SEC has the authority to withdraw facility access at any time and such action is not subject to appeal. (Chapter 566)

fitness
The level of character and conduct determined necessary for an individual to perform work for or on behalf of a Federal agency as an employee in the excepted service (other than a position subject to suitability) or as a contractor employee. A favorable fitness determination is not a decision to appoint or contract with an individual. (Chapter 566)

fitness determination

A decision by an Agency that an individual has or does not have the required level of character and conduct necessary to perform work for or on behalf of a Federal agency as an employee in the excepted service (other than a position subject to suitability) or as a contractor employee. A favorable fitness determination is not a decision to appoint or contract with an individual. (Chapter 566)

institutional contractor
An individual who performs work for on or behalf of any Agency under a contractor and who, in order to perform work specified under the contract, will require access to space, information, information technology systems, staff or other assets of the Federal Government. Such contracts, include, but are not limited to services contracts, contracts between any non-Federal entity and any agency, and sub-contracts between any non-Federal entity and another non-Federal entity to perform work related to the primary contract with the agency. (Chapter 566)

national security position
Any position which requires the incumbent to have access to classified information. (Chapters **562**, 566, **567**) National security positions require the submission of an SF-86 form.

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. (**Chapter 545, 566, 569, 573**)

non-sensitive position
Any position in USAID that does not fall within the definition of a sensitive position (special-sensitive position, critical-sensitive position, or noncritical-sensitive position). (Chapters **562**, 566, **567**)

Personal Identity Verification (PIV)
A PIV card is a smart card issued by the Federal Government and contains the necessary data for the cardholder to be granted access to Federal facilities and information systems and assure appropriate levels of security for all applicable Federal applications. A PIV card requires the completion of National Agency background Check with Inquiries (NAC-I) for issuance. (**Chapter 545, 566**)

Personal Service Contractor (PSC)
This term refers to a type of contractor who provides specialized technical assistance in designing and managing programs, primarily in the field. They can be locally recruited or internationally recruited. (**Chapter 545, 566**)

personnel security investigation

Inquiries designed to develop information pertaining to an individual for use in determining whether the employment, assignment to duties, or retention in employment of that individual is clearly consistent with the interests of national security and USAID goals and objectives. (Chapters 566, **567**)

public trust risk designations/public trust positions
The designations of positions indicating the potential for action or inaction by the incumbent of the position to affect the integrity, efficiency, and effectiveness of Government operations. Public Trust positions require the submission of an SF-85P form. (Chapter 566)

reciprocity
The recognition and acceptance of all security clearance background investigations and determinations completed by an authorized investigative or adjudicative agency of the federal government without further investigation or adjudication. (Chapter 566)

security clearance
A certification that a U.S. citizen, who requires access to information classified at a certain level, has been found security eligible under federal standards and may be permitted access to classified information at the specified level. (Chapters **562**, 566)

Security Clearance Review Panel (SCRP)
Panel consisting of the Director of Security, Deputy Assistant Administrator for Human Capital and Talent Management (DAA/HCTM) and the designated Agency's Ethics Official that addresses the appeal of a denial or revocation of a security clearance. (Chapter 566)

security eligibility
A security status based on favorable adjudication of a required personnel security investigation; it indicates that an individual is deemed trustworthy for employment in a sensitive position, and may be granted a clearance for access to classified information up to the level of eligibility if required in the performance of official duties. (Chapters **562,** 566, **567**)

Sensitive But Unclassified information (SBU)
SBU describes information which warrants a degree of protection and administrative control that meets the criteria for exemption from public disclosure set forth under Sections 552 and 552a of Title 5, United States Code: the Freedom of Information Act and the Privacy Act, 12 FAM 540-Sensitive But Unclassified Information, (TL;DS 61;10 01 199), 12 FAM 541 Scope, (TL;DS 46;05 26 1995). SBU includes, but is not limited to:

- Medical, personnel, financial, investigatory, visa, law enforcement, or other information which, if released, could result in harm or unfair treatment to any individual or group, or could have a negative impact upon foreign policy or relations; and

- Information offered under conditions of confidentiality which arises in the course of a deliberative process (or a civil discovery process), including attorney-client privilege or work product, and information arising from the advice and counsel of subordinates to policy makers. (Chapters **107**, **545**, **552**, **562**, 566, **567**)

Sensitive Compartmented Information (SCI)
All information and materials bearing special intelligence community controls indicating restricted handling within present and future intelligence community collection programs and their end products for which intelligence community systems of compartmentation have been or will be formally established. (Chapter 566)

sensitive positions
Any position in USAID the occupant of which could bring about, because of the nature of the position, a material adverse effect on the national security. There are three types of sensitive positions each of which requires access to classified information:

a. Critical-Sensitive Position: Any position in USAID, the duties of which include, but are not limited to: positions with public trust risk designations of high with access to any level classified information: positions with a requirement for access to Top Secret information: positions having investigative or security functions, or service on personnel security boards.

b. Noncritical-Sensitive Position: Any other sensitive position in USAID that does not fall within the definition of a critical-sensitive position. The duties of a noncritical-sensitive position include, but are not limited to access to national security information and material up to, and including, Secret.

c. Special-Sensitive Position: Any position in USAID, the duties of which are determined to be at a level higher than "critical sensitive" because of the greater degree of damage that an individual by virtue of occupancy of the position could effect to the national security, or because the duties may entail access to sensitive compartmented information. (Chapters **562**, 566, **567**)

suitability
Suitability refers to the basic standard (in EO 10450) requiring that an individual's appointment to or retention in the Federal Service must promote the efficiency of the Service. Suitability is only applicable to direct-hire employees (**Chapter 414, 566**)

temporary facility access
A determination that an individual is eligible to occupy a non-sensitive position. SEC grants temporary facility access pending a more in-depth personnel security investigation. (Chapters 566, **567**)

temporary security clearance

A certification based on partial investigative action that a U.S. citizen, who requires access to information classified at a certain level, has been found security eligible under USAID standards (authority #16) and may be permitted access to classified information at the specified level. The temporary clearance may be withdrawn at any time. If withdrawn, the individual will be advised of the issue requiring resolution, however the individual has no right to appeal the decision. The clearance will remain temporary until the personnel security investigation is completed and favorably adjudicated at which time the temporary designation is withdrawn. (Chapter 566)

566_092622