Functional Series 500 - Management Services
ADS Chapter 566 - U.S. Direct-Hire and PASA/RSSA Personnel Security Program

Table of Contents

Functional Series 500 - Management Services
ADS Chapter 566 - U.S. Direct-Hire and PASA/RSSA Personnel Security Program

566.1 OVERVIEW

This chapter provides the policy and procedures for personnel security investigations and issuing security clearances for **direct-hire employees**.

566.2 PRIMARY RESPONSIBILITIES

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

(1) Carrying out the responsibilities of the Senior Agency Official as delineated in Executive Order (EO) 12968 and EO 12958 **(See Mandatory References, EO 12968 and EO 12958)**; and

(2) Chairing the USAID **Security Clearance** Review Panel (SCRP).

b. The Assistant General Counsel for Ethics and Administration (GC/EA) is responsible for serving as an SCRP member.

c. The Deputy Assistant Administrator for the Bureau for Management, Office of Human Resources (DAA/M/HR) is responsible for

(1) Serving as an SCRP member;

(2) Determining the **suitability** for employment of USAID direct-hire employees;

(3) Designating the position sensitivity (public trust) level for each direct-hire position; and

(4) Determining those positions for which a **temporary security clearance** may be issued.

d. The Deputy Director of Security (DD/SEC) is responsible for

(1) Deciding the denial or revocation of eligibility for **access** to **classified national security information**; and

(2) Receiving written and hearing personal replies to decisions of ineligibility for access to classified national security information.

e. The Chief, Personnel, Information, and Domestic Security Division (SEC/PIDS) is responsible for

(1) Deciding to take **assignment restriction** actions;

(2) Deciding on the suspension of security clearances and periodically reviewing the status of suspensions;

(3) Receiving written and/or hearing personal requests to initiate denial, reduction, or revocation of eligibility for access to classified national security information; and

(4) Initiating personnel security investigations when information is uncovered bearing on an employee's suitability or continued eligibility for access to classified national security information.

f. The Assistant Inspector General for Management (AIG/M) is responsible for determining the suitability for employment of direct-hire employees assigned to the Office of the Inspector General (OIG).

g. The Security Clearance Review Panel (SCRP) is responsible for sustaining or overruling the decision to deny, reduce, or revoke an individual's eligibility for access to **classified information**.

566.3 POLICY AND PROCEDURES

566.3.1 Security Clearance and Public Trust Position Designation

All direct-hire positions in USAID are national security positions requiring either a Secret or Top Secret security clearance. The references listed under 566.4.1 establish the security clearance criteria for determining eligibility for those positions. **(See 566.4.1)**

A Top Secret security clearance is required for all officers and **employees** who are

a. Appointed by the President with the advice and consent of the Senate;

b. Appointed to a position to which the basic rate of pay is fixed according to Executive Levels I-V under 5 U.S.C. Chapter 53 subchapter 2;

c. In a position for which the basic rate of pay is equal to or greater than Level V of the Executive Schedule;

d. In the Foreign Service; or

e. General Schedule (GS) employees working in positions designated as Special Sensitive or Critical Sensitive.

The positions cited immediately above require a High public trust designation. All other positions are Noncritical-Sensitive and require a Secret security clearance and a designation of either High or Moderate public trust.

The position sensitivity of Special-Sensitive, Critical-Sensitive, or Noncritical-Sensitive will be reflected in the OF-8, Position Description, for all direct-hire positions.

The security clearance and public trust designations for each direct-hire position in USAID are cited in the USAID Staffing Pattern.

To request a change in either designation, Bureaus and Independent Offices must complete the form SF-52B, Request for Personnel Action, and send it to the Bureau for Management, Office of Human Resources, Personnel Operations Division (M/HR/POD). M/HR/POD will forward the form to the Office of Security, Personnel, Information, and Domestic Security Division (SEC/PIDS). **(See Mandatory Reference, SF-52B, also available on the USAID intranet Forms page)**

Additional instructions on public trust designations can be found in the Public Trust Designations reference in this chapter. **(See Additional Help, Public Trust Designations)**

566.3.2 Direct-Hire Personnel Security Investigations and Clearances

SEC will conduct personnel security investigations and adjudicate them to determine the **security eligibility** of USAID employees. Investigations and adjudications will be conducted in accordance with the standards issued under EO 10450 and 12968. **(See Mandatory References, EO 10450 and 12968)** The adjudicative standards in Director of Central Intelligence Directive (DCID) 1/14 also apply to Special **Sensitive positions**. **(See 566.4.1)**

No individual may be employed by USAID, detailed or assigned to a USAID-funded position, permitted access to classified information, and/or allowed unescorted access into USAID office space until

- A **personnel security investigation** is completed at the level appropriate for the position;
- A determination is made that the individual's employment is clearly consistent with the interests of national security and USAID goals; and
- A favorable access eligibility determination is issued.

(See 566.3.6 for Temporary Clearance Conditions)

Personnel security investigations are based on the position sensitivity (security clearance) and public trust designations of the position. The investigation will not be initiated until

- A completed and signed Form AID 6-1, Request for Security Action is received by SEC from the Bureau for Management, Office of Human Resources (M/HR) or Office of the Inspector General, Office of Legal Counsel and Management (OIG/LCM); and

- Completed personnel security forms are submitted along with the Form AID 6-1. **(See Mandatory Reference, AID 6-1, also available on the USAID intranet Forms page)**

The required personnel security forms are listed in the Mandatory Reference section. All forms requiring a signature must be signed. Type or print all forms with sufficient boldness and clarity to allow the information to be successfully scanned by electronic media. Forms that do not contain all the required information or are not legible will be returned to the requestor without the initiation of any investigative activity.

566.3.3 Change in Employee Position

M/HR must notify SEC prior to assigning an employee to a new position requiring a higher or lower security clearance.

- When an employee is to be assigned to a position requiring a higher or lower security clearance, M/HR/POD will forward to SEC a Form AID 6-1 indicating that a change in the employee's security clearance is necessary. **(See Mandatory Reference, AID 6-1, also available on the USAID intranet Forms page)**

- SEC will notify the cognizant Bureau Administrative Management Specialist (AMS) that the employee is not to be given a higher level access until any requisite investigation is complete and a new clearance is issued.

566.3.4 Employee Update Investigations

Employees must be periodically reinvestigated. The interval between the initial investigation and subsequent update investigations depends on the level of security clearance and public trust associated with the position (e.g., five years for Top Secret access and 10 years for Secret access).

- Employees who, after notification from SEC, fail to submit the requisite forms for their update investigation in a timely manner will be subject to security, administrative, and/or disciplinary action.

- SEC must notify employees in writing of the requirement to undergo an update investigation. Employees must complete their update security package and return it to SEC within the time frame specified on the notification.

566.3.5 Sensitive Compartmented Information (SCI) Access

Only employees in positions designated as Special Sensitive or otherwise designated as requiring Sensitive Compartmented Information (SCI) access will be granted SCI access. The Executive Secretariat (ES) is the approval authority for determining the adequacy of a justification for SCI access.

Requests for SCI access must be prepared in memorandum format and addressed to the ES through the respective Bureau Assistant Administrator or Independent Office Director. The memorandum must contain the following information:

- The employee's full name;
- Date of birth;
- Place of birth;
- Social Security Number; and
- Justification for the SCI access requirement.

Efforts must be made to keep the request unclassified. If it is classified, it must be prepared and transported in accordance with EO 12958. **(See Mandatory Reference, EO 12958)**

Both the Mission Director and the Chief of Mission must first approve requests for SCI access for personnel assigned overseas, and then forward the request to ES. ES will notify SEC when the request has been approved. SEC then initiates the necessary investigative and adjudicative action.

The employee is granted SCI access only after a favorable adjudication and an appropriate briefing.

SEC must debrief personnel no longer requiring SCI access.

566.3.6 Temporary Clearance Request

a. Application

The requirement for completion of a personnel security investigation prior to hiring may, in specific situations, be waived via a Temporary Clearance. The Temporary Eligibility Standards issued under EO 12968 will only be applied to

- USAID direct-hire positions determined to be eligible for a Temporary Clearance by the Deputy Assistant Administrator for the Bureau for Management, Office of Human Resources (DAA/M/HR); or

- OIG positions designated by the Assistant Inspector General for Management (AIG/M).

(See Mandatory Reference, EO 12968)

b. Conditions

A Temporary Clearance may be requested if the following conditions are met:

- A completed AID Form 6-1 and a complete set of personnel security forms are submitted to SEC with an annotation indicating that this is a Temporary Clearance Request. **(See Mandatory Reference, AID 6-1, also available on the USAID intranet Forms page)**

- The request is endorsed by the Deputy Assistant Administrator for the Bureau for Management, Office of Human Resources (DAA/M/HR) or the Assistant Inspector General for Management (AIG/M) for OIG positions.

c. Issuance

The following steps must be completed before a Temporary Clearance can be issued:

- The request must include sufficient information and justification to support a finding that accelerated employment is necessary in the national interest and is based on operational requirements justifying the risk of employing the individual prior to the completion of the personnel security investigation;

- The AID Form 6-1 and all the other required papers and forms must be completed and received by SEC;

- SEC must approve the request.

SEC will then issue a certification of security clearance to the employee, containing the following notation:

"TEMPORARY CLEARANCE AUTHORIZATION - This security clearance/employment authorization is temporary. Retention of this clearance/authorization is contingent upon a favorable adjudication by SEC of the completed security investigation as required by Executive Order 12968."

(See Mandatory Reference, EO 12968) Employment of the individual is authorized only upon receipt of this certification.

d. Withdrawal

SEC must notify DAA/M/HR or AIG/M in writing if the Temporary Clearance/Authorization must be withdrawn due to a subsequent determination of ineligibility.

In this event, action must be taken to immediately physically remove the person from the work force.

The notification will advise that the investigation must proceed further or be completed prior to a decision to grant the clearance or initiate the clearance denial process.

566.3.7 Participating Agency Employees Assigned to USAID Under a PASA or RSSA

Before a Participating Agency may assign an employee to work in USAID space or under USAID direction pursuant to a Participating Agency Service Agreement (PASA) or a Resources Support Services Agreement (RSSA), the Participating Agency must complete an investigation of the employee and issue a personnel security clearance at the required level.

After assignment to USAID, employees of Participating Agencies are subject to the same security requirements as USAID direct-hire personnel.

Under the proposed PASA/RSSA agreement, the parent agency's security office must certify the candidate's security clearance on the AID Form 2-5, Participating Agency Certification of Candidate's Security Clearance and Duration of Assignment, and forward the certification to SEC. **(See Mandatory Reference, AID 2-5, also available on the USAID intranet Forms page)**

566.3.8 Marriage or Cohabitation With Non-U.S. Citizens

Individuals who intend to marry or cohabit with non-U.S. citizens must comply with the requirements of 3 FAM 4100, Appendix B (old 3 FAM 629). **(See Mandatory Reference, 3 FAM 4100, Appendix B)**

In USAID this policy (3 FAM 4100) applies to all direct-hire positions, i.e., Foreign Service, General Schedule, and Administratively Determined.

Upon completion of the investigation of the intended spouse or cohabitant, SEC will assess the impact of the marriage or cohabitation on the clearance holder's continued eligibility for access to classified information.

The determination of continued eligibility for access is based on EO 10450, as amended, and EO 12968. **(See Mandatory References, EO 10450, as amended, and EO 12968)**

Additional guidance is provided in the Mandatory Reference document, Employee Marriage to or Cohabitation With Non-U.S. Citizens.

566.3.9 Non-Duty Status

When an employee is placed on non-duty status by M/HR, his or her security clearance must be administratively (without prejudice) withdrawn.

The **appointment authority** (M/HR, Mission, Contracting Officer) must notify SEC when an employee is placed on non-duty status and give the reason for the action.

The employee will be required to surrender to SEC any USAID or Department of State ID cards and building passes, non-tourist passports, and all U.S. Government keys.

If an employee is placed on Leave Without Pay (LWOP) status for less than 30 days, the security clearance will remain in effect. The employee may retain ID cards and building passes.

The appointment authority must notify SEC at least 60 days before the employee's planned return to duty status. SEC will then review the employee's security record and advise the appointment authority when eligibility for access can be restored.

566.3.10 Participation in a Drug or Alcohol Rehabilitation Program

Supervisors must immediately notify the appointment authority when an employee participates in a drug or alcohol rehabilitation program. The appointment authority must notify SEC of the employee's participation in such a program.

566.3.11 Suitability Determinations

Appointment authorities (M/HR and OIG/LCM) determine the employment suitability and qualifications of individuals occupying direct-hire positions in their organization.

If a security investigation uncovers significant adverse information bearing on an individual's suitability for employment, SEC must make this information available to the appropriate appointment authority.

The determination of eligibility for access to classified information will be held in abeyance until the suitability decision is made.

566.3.12 Personnel Security Clearance Access Restriction, Suspension, Denial, and Revocation

Procedural due process must be provided to employees and applicants when actions are taken to suspend, deny, or revoke a security clearance. (See **566.3.12.2.b** for more details)

566.3.12.1 Personnel Security Clearance Access Restriction

a. Conflict of Interest

If circumstances develop that create the potential for a conflict of interest between the employee and national security interests, access restrictions will be applied.

Examples of such circumstances are marriage or cohabitation with a non-U.S. citizen, membership in foreign business associations, or foreign relatives. **(See Additional Help, Access Restriction Criteria)**

If there is a conflict of interest, the employee must be excluded from assignments that create conflict. Employees are expected to recuse themselves from such assignments.

b. Waivers

Certain circumstances may justify a waiver to an access restriction.

- When considering a waiver, HR, SEC, and the affected Bureau/Office must take into account the duties and scope of responsibility of the individual employee and the identity of the foreign country and its relationship with the United States.

- In addition the Mission Director and Chief of Mission (if the position is an overseas assignment), or the Assistant Administrator or Director of an Independent Office (if the position is in USAID/W), must take into consideration all pertinent circumstances.

c. Access Restriction Procedures

The employee's access to national security information will be restricted if the Chief, SEC/PIDS determines that such action is warranted.

- When access restrictions must be imposed, SEC will notify the appointment authority, the head of the office of assignment, and the employee in writing of the access restrictions, the reasons for the action, and the time period for the restrictions.

- Such restrictions must specify the subject matter or specifically designated projects/documents, or other conditional or probationary terms of clearance. The time period may be indefinite or may depend on sufficient resolution of the precipitating issues to permit the restoration of full access eligibility.

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

a. Suspension

The Chief, SEC/PIDS 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 appointment authority, the head of the office of assignment, and the individual in writing of the suspension and the reasons for the action.

The Chief, SEC/PIDS 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. Procedural Due Process

Procedural due process must be provided to employees and applicants when actions are taken to deny, reduce, or revoke a security clearance.

(1) Procedural due process for denying, reducing, or revoking an individual's clearance eligibility requires that the Chief, SEC/PIDS send a letter to the individual. The letter must

a. Provide, within the limits of the law, a comprehensive and detailed explanation of the basis for the conclusion to deny, reduce, or revoke clearance eligibility;

b. Include a copy of the documents, records, and reports upon which the conclusion to deny, reduce, or revoke access eligibility is based. Materials not releasable under the Privacy Act, as amended, or the Freedom of Information Act (5 U.S.C. 552a or 5 U.S.C. 552) cannot be provided **(See Mandatory References, 5 U.S.C. 552a and 5 U.S.C. 552);**

c. Inform the individual of the right to be represented by counsel or other representative at his or her own expense;

d. Advise the individual of the opportunity to reply in writing and/or person within 30 days to the Chief, SEC/PIDS to present any relevant documents, materials, and information for a review of the conclusion. If the individual meets with the Chief, SEC/PIDS in person, a written summary or recording of the appearance will be made part of the individual's security file;

e. Advise that if the conclusion is unchanged after the individual has submitted a written reply and/or has presented information in person, or upon expiration of the 30-day time period, a recommendation for the action (denial, reduction, or revocation) will be made to the Deputy Director of the Office of Security (DD/SEC) to render a decision. The recommendation to the Deputy Director will include the complete investigative file; and

f. Advise that the Deputy Director will notify the individual in writing of the decision.

If the conclusion reached by the Chief, SEC/PIDS 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 is unchanged, the investigative file will be forwarded to the DD/SEC with a recommendation that considers the written and/or oral information provided by the individual.

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

If the DD/SEC agrees with the conclusion, the Deputy Director will send a letter to the individual that

a. Advises the individual of the decision to deny, reduce, or revoke access eligibility;

b. Advises 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;

c. Advises 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

d. Advises that the decision of the SCRP will be provided in writing.

(3) Security Clearance Review Panel

- If the individual appeals the decision, 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 Resources (DAA/M/HR) and the Assistant General Counsel for Ethics and Administration (GC/EA) 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 Adjudicative Guidelines cited in 566.4.1. **(See Mandatory References, EO 12968** and **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

a. Adjudicative Guidelines for Determining Eligibility for Access to Classified Information; Investigative Standards for Background Investigations for Access to Classified Information; and Investigative Standards for Temporary Eligibility for Access, issued under EO 12968 in March 1996.

b. 5 CFR 731, Suitability

c. Executive Order (EO) 10450 of April 27, 1953, "Security Requirements for Government Employment"; as amended by EO 10491 of October 13, 1953, EO 10531 of May 27, 1954, EO 10548 of August 2, 1954, EO 10550 of August 5, 1954, and EO 11785 of June 4, 1974, as they relate to the USAID personnel security program

d. EO 12958, "Classified National Security Information," of April 17, 1995

e. EO 12968, "Access to Classified Information," of August 2, 1995

f. 3 FAM 4100 Appendix B (old 3 FAM 629), Employee Marriage Equivalent Bonds, and Cohabitation

g. The Freedom of Information Act, 5 U.S.C. 552

h. Section 587(b) of the Fiscal Year 1999 Omnibus Appropriations Bill (Pub. L. 105-277)

i. The Privacy Act of 1974, 5 U.S.C. 552a

566.4.2 Internal Mandatory References

a. AID Form 2-5, Participating Agency Certification of Candidate's Security Clearance and Duration of Assignment (also available on the USAID intranet Forms page)

b. AID Form 6-1, Request for Security Action (also available on the USAID intranet Forms page)

c. Employee Marriage to or Cohabitation With Non-U.S. Citizens

d. Personnel Security Forms

e. SF-52B, Request for Personnel Action (also available on the USAID intranet Forms page)

566.5 ADDITIONAL HELP

a. Access Restriction Criteria

b. Public Trust Designations

566.6 DEFINITIONS

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

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)

appointment authority
The USAID Human Resources office (HR) is the appointment authority for persons occupying USAID direct-hire positions; the Assistant Inspector General for Resource Management (AIG/RM) is the appointment authority for all Inspector General direct-hire foreign service positions; OPIC for all OPIC direct-hire and contractor personnel; and TDA for all TDA direct-hire and contractor personnel. (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)

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 EO 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)

direct-hire employee
Refers only to U.S. citizens employee 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. (Chapters 562, 566, 567)

employee
U. S. citizen employee of USAID, both direct-hire and contractors. (Chapters 562, 566, 567)

national security position
Any position which requires the incumbent to have access to classified information. (Chapters 562, 566, 567)

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)

nonsensitive 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)

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
The designations of position 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 risk designations are used in conjunction with security clearance requirements to determine the investigative requirements for the position. Positions involving high degrees of public trust, e.g., those with broad policy making authority or fiduciary responsibilities, trigger a more thorough investigation than do positions requiring only the finding that an applicant or an incumbent has the requisite stability of character to hold Federal employment. The three public trust risk designation levels are high, moderate, and low.

a. High Risk: A position that has potential for exceptionally serious impact involving duties especially critical to the agency or a program mission of the agency with broad scope of policy or program authority such as:

(1) policy development and implementation;

(2) higher level management assignments;

(3) independent spokespersons or non-management positions with authority for independent action;

(4) significant involvement in life-critical or mission critical systems; or

(5) relatively high risk assignments associated with or directly involving the accounting, disbursement, or authorization of disbursement from systems of dollar amounts of $10 million per year or greater, or lesser amounts if the activities of the individual are not subject to technical review by higher authority to ensure the integrity of the system.

(6) positions in which the incumbent is responsible for the planning, direction, and implementation of a computer security program; has a major responsibility for the direction and control of risk analysis and/or threat assessment, planning, and design of the computer system, including the hardware and software; or, can access a system during the operation or maintenance in such a way, and with the relatively high risk for causing grave damage or realize a significant personal gain;

b. Moderate Risk: A position that has the potential for moderate to serious impact involving duties of considerable importance to the agency or a program mission of the agency with significant program responsibilities and delivery of customer services to the public such as:

(1) assistants to policy development and implementation;

(2) mid-level management assignments;

(3) non-management positions with authority for independent or semi-independent action;

(4) delivery of service positions that demand public confidence or trust; or

(5) positions with responsibility for the direction, planning, design, operation, or maintenance of a computer system and whose work is technically reviewed by a higher authority at the high risk level to ensure the integrity of the system. Such positions may include but are not limited to:

(a) access to and/or processing of proprietary data, Privacy Act of 1974, and Government-developed privileged information involving the award of contracts;

(b) accounting, disbursement, or authorization for disbursement from systems of dollar amounts of less than $10 million per year; or

(c) other positions as designated by the agency head that involve degree of access to a system that creates a significant potential for damage or personal gain less than that in high risk positions.

c. Low Risk: Positions that have the potential for impact involving duties of limited relation to the agency mission with program responsibilities which affect the efficiency of the service. It also refers to those positions that do not fall within the definition of a high or moderate risk position. (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 USAID standards (authority #16) and may be permitted access to classified information at the specified level. (Chapters 562, 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)**
A category of unclassified official information and material that is not national security information, and therefore is not classifiable, but nevertheless requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. The term includes data whose improper use or disclosure could adversely affect the ability of the Agency to accomplish its mission, proprietary data, records requiring protection under the Privacy Act, and data not releasable under Sections 552 and 552a of Title 5 of the Freedom of Information Act.

SBU information includes, but is not limited to, information received through privileged sources and certain personnel, medical, personnel, commercial, and financial records, 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 individual privacy, Federal programs, or foreign relations. (source: 12 FAM 540)

Examples of SBU include travel of agency employees to or through a high or critical terrorist threat environment; investigatory records compiled by an agency conducting lawful national security intelligence investigation (source: FOIA); and candid assessments of situations in a host country which could cause embarrassment if made public. Material of this type, which requires protection and limited dissemination, shall be designated by any official having signing authority for the material. (Chapters 545, 552, 562, 566, 567)

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. (Chapters 562, 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_042502_w120502