ADS Chapter 567

Classified Contracts Under USAID's National Industrial Security Program

Partial Revision Date: 08/03/2021
Responsible Office: SEC/CTIS
File Name: 567_080321

Functional Series 500 - Management Services
ADS 567 - Classified Contracts Under USAID's National Industrial Security Program
POC for ADS 567: Diane Sloan, (202) 712-0990, dsloan@usaid.gov

Table of Contents

567.1 OVERVIEW 4

567.2 PRIMARY RESPONSIBILITIES 5

567.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES 6

567.3.1 Determining Contract Security Levels 6
567.3.1.1 Pre-Award Procedures 6
567.3.1.2 Security Language and Designation of Positions 7
567.3.1.3 Post-Award Procedures 7

567.3.2 Facility Clearance 7

567.3.3 Security Procedures for Registering Contracts 9

567.3.4 Security Clearance 9

567.3.5 Building and Classified Information Access for Contractor Personnel 10

567.3.6 Self-Employed Contractors (Consultants) 10

567.3.7 Subcontractors/Sub Awardees 11

567.3.8 Contract Extensions 11

567.3.9 Suspension of Physical Access for Contractor Personnel 11

567.3.10 Contract Completion 12

567.3.11 Return of Federal Identification Card (ID) FAC 12

567.4 MANDATORY REFERENCES 13

567.4.1 External Mandatory References 13

567.4.2 Internal Mandatory References 13

567.4.3 Mandatory Forms 14

567.5 ADDITIONAL HELP 14

567.6 DEFINITIONS 14

ADS 567 - Classified Contracts Under USAID's National Industrial Security Program

567.1 OVERVIEW

Effective Date: 02/26/2018

The National Industrial Security Program (NISP) serves as a single, cohesive industrial security program to protect classified information and to preserve our nation's economic and technological interests. As per Executive Order 12829, the purpose of this program is to safeguard classified information that may be released or has been released to current, prospective, or former contractors, licensees, or grantees of United States agencies (see **Executive Order (EO) 12829, National Industrial Security Program**). The NISP will provide protection of information classified under **EO 13526, Classified National Security Information, as amended**, or its successor, the **Atomic Energy Act of 1954 as amended**, and **12 FAM 570, Industrial Security Program**.

The National Security Council is responsible for providing overall policy direction for the NISP. The Director, Information Security Oversight Office (ISOO), is responsible for implementing and monitoring the NISP and for issuing implementing directives that are binding on federal agencies.

USAID utilizes contractor personnel to perform various missions and functions. USAID's National Industrial Security Program is in place to ensure contractor personnel safeguard Federal Government classified information. The program is guided by **EO 13526, Classified National Security Information**, **EO 12829, National Industrial Security Program**, the **National Industrial Security Program Operating Manual (NISPOM)**, and **Homeland Security Presidential Directive 12 (HSPD-12)**.

This ADS chapter provides the policy directives and required procedures for USAID's implementation of the NISP. It also provides policy directives and required procedures on the security requirements and language for contracts falling under the provisions of the NISP. These contracts require the contractor to obtain a Facility Clearance (FCL) and require contractor personnel to obtain security clearances in order for the contractor personnel to have access to classified information and restricted areas.

Classified assistance awards must be coordinated with the Agreement Officer (AO), Agreement Officer's Representative (AOR), and the Office of Security (SEC) and follow the procedures outlined in this ADS chapter.

This chapter does not address background investigations or the Facility Access investigative process. Security clearance actions regarding U.S. Personal Service Contractors and other categories of personnel can be found in **ADS 566, Personnel Security Investigations and Clearances**.

This chapter also does not address the badge issuance process for access to USAID facilities (see **ADS 565, Physical Security Programs (Domestic)**).

This ADS chapter does not apply to contractor personnel working under a wholly unclassified contract whereby none of the job duties under that contract will require a

security clearance. The IIS Branch does not process unclassified contracts since they do not fall under the NISP. Unclassified contracts should be coordinated with the COR and the AMS Officer.

567.2 PRIMARY RESPONSIBILITIES

Effective Date: 02/26/2018

a. The **Director, Office of Security (D/SEC)** is the Senior Agency Official (SAO) responsible for enforcing **EO 12829**, **EO 13526**, and **HSPD-12**.

b. The **Office of Security's Counterterrorism and Information Security Division (SEC/CTIS), Information and Industrial Security Branch (IIS):**

1. Issues USAID NISP security policies and standards;

2. Liaisons with the Department of Defense, Defense Security Service (DSS) regarding the National Industrial Security Program;

3. Coordinates corrective action with contractors and/or DSS when personnel fail to comply with the security requirements of their contracts; and

4. Reviews and processes NISP requests.

c. **Bureau/Independent Offices (B/IOs)** and **USAID Overseas Mission Project Officers** are responsible for providing the security specifications to be included in contracts or assistance awards to the B/IO Contracting Officer (CO) or Executive Officer (EXO).

d. **Contracting Officers (COs)** are responsible for inserting security specifications into contracts and ensuring the contract terms abide by NISP policies and procedures as outlined in this ADS chapter.

e. **Contracting Officer's Representatives (CORs)** are responsible for assisting COs with establishing and administering security specifications for contracts. COR duties include monitoring classified contractor personnel's compliance with the security specifications included in their contracts and notifying the CO and SEC of any problems or suspected non-compliance with these contract requirements.

The COR must be familiar with the security specifications in the contracts for which they are a COR and with the USAID regulations that apply. These include **ADS 545, Information System Security**, **ADS 552, Cyber Security for National Security Information Systems** , **ADS 565, Domestic Security Programs**, and this ADS chapter (**ADS 567**).

f. **Bureau/Independent Office (B/IO) Administrative Management Specialists (AMSs)** are responsible for ensuring that Visit Authorization Letters

(VALs)/Visit Authorization Requests (VARs) are completed and delivered to SEC's International Security Program Division's Domestic Security Branch (SEC/ISP/DS).

g. Contractor Facility Security Officers (FSOs) are responsible for initiating VALs/VARs on all cleared contractor personnel who access USAID spaces in the performance of their contract.

h. Department of Defense (DoD), Defense Security Service (DSS) Industrial Security Representatives oversee cleared contractor facilities and assist the contractor management staff and FSOs in formulating their security programs and obtaining personnel security clearances and facility clearances.

567.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES

Effective Date: 02/26/2018

The USAID program, project, and acquisition workforce must consider federal security requirements at the earliest possible stage in the procurement process. This section provides the required security policies and mandatory procedures that USAID must apply in creating and administering contracts. If the terms and conditions of a grant or cooperative agreement require the recipient's employees to have unescorted access to USAID restricted space and access to classified information, as described below, the AOR must work with the AO and SEC to ensure that the award contains the necessary security requirements.

567.3.1 Determining Contract Security Levels

567.3.1.1 Pre-Award Procedures

Effective Date: 02/26/2018

The B/IO or Mission Project Officer must first determine whether contract performance will be classified, unclassified, or involve dual performance.

A contract will be classified if:

- The contractor personnel will require a security clearance, and
- The contractor personnel will require access to classified information.

If a contract is determined to be classified, it does not necessarily mean that the terms or statements within the contract are classified. It refers to the type of access that is required, access to classified information.

A contract will be dual performance if:

- Some, but not all, of the contractor personnel will require security clearances, or

- Some, but not all, of the contractor personnel will require access to classified information.

Contractor personnel working under a classified contract require a security clearance. If the contractor personnel are working under a dual performance contract and their job duties do not require a security clearance, however they require logical and/or physical access to USAID information systems and/or facilities, facility access (formerly known as employment authorization) is required. The facility access process is discussed in **ADS 566, Personnel Security Investigations and Clearances**.

567.3.1.2 Security Language and Designation of Positions
Effective Date: 02/26/2018

If a contract is determined to be classified or dual performance, the COR must obtain specific security language from the IIS Branch through **SECNISP@usaid.gov** or the **IIS Branch's MyUSAID Web site**. The COR must then provide the security language to the CO for inclusion in the contract. Without this language, contractor personnel cannot gain unescorted access to restricted space in USAID/W or have access to classified materials.

Dual performance contracts must clearly state which positions/titles require a security clearance and what level of security clearance is required. If the positions/titles are not clearly stated within the contract, the contract will not be registered with IIS under the NISP. The positions/titles that do not require a security clearance do not need to be listed.

567.3.1.3 Post-Award Procedures
Effective Date: 02/26/2018

If the contract is awarded prior to the inclusion of the required security language, the CO must make a modification to ensure it is incorporated into the contract before it can be registered under the NISP. If the contract is not registered under the NISP, contractor personnel will not gain access.

567.3.2 Facility Clearance
Effective Date: 02/26/2018

If the contract is determined to be classified or dual performance, the contractor must have or be able to obtain and maintain a valid Facility Clearance (FCL) equal to the level of Secret or Top Secret, as specified in the contract. The contract must clearly state what level of FCL is needed to fulfill the contract terms. This is required to ensure classified information entrusted to the private sector is properly safeguarded.

USAID SEC will prohibit contractors without a valid FCL from having their contractor personnel gain access to USAID restricted areas and will deny the contractor personnel access to classified information. An FCL is obtained through

DSS. To obtain an FCL, the contractor must complete the following steps:

1. **Sponsorship**

   Contractors must apply for an FCL through DSS and be sponsored for an FCL by a government entity. The government entity that sponsors a contractor will be the USAID B/IO in which the contractor personnel will be working. The government entity will provide the contractor with a sponsorship letter. Additional assistance with the sponsorship letter can be obtained through **DSS' Web site**.

   USAID SEC does not sponsor contractors for an FCL or contractor personnel for security clearances, nor does it represent the contractor or contractor personnel in his/her effort to obtain such clearances from DSS. USAID SEC does not prepare documentation, other than a mandatory draft **DD 254 – Contract Security Classification Specification Form** on behalf of a company for submission of an FCL application to the DSS. Applying for an FCL is the sole responsibility of the contractor.

2. **Contract Security Classification Specification Form, DD-254**

   A **Contract Security Classification Specification Form, DD-254**, is required for all classified and dual performance contracts with USAID. The purpose of this form is to provide security classification guidance to cleared contractors and contractor personnel working under the NISP. This form specifies the classification requirements for that contract.

   DSS requires contractors to have a draft DD-254 when applying for an FCL. The COR can request a draft DD-254 from **SECNISP@usaid.gov**. SEC will be responsible for the final preparation of the draft DD-254 with the COR's assistance throughout the process.

   Block 13 of the DD-254 provides supplemental security guidance that incorporates security specifications into the contract. The security guidance attached to the DD-254 must remain with the DD-254 at all times.

   The COR must inform the IIS Branch when an FCL is issued. The IIS Branch will verify the issuance of an FCL and then issue a non-draft DD-254. The COR is responsible for immediately communicating any changes in the FCL status to the IIS Branch at **SECNISP@usaid.gov**.

3. **Submission of Request to DSS**

   The COR must ensure that the contractor submits the sponsorship letter, draft DD-254, and any additionally required paperwork to DSS.

   DSS controls the Facility Clearance process. The process of applying for an FCL and the required paperwork is detailed on the **DSS' Web site**.

Updates on where a contractor is in the FCL process should be directed to DSS through their Web site or the contractor's assigned DSS representative. USAID SEC does not control the FCL process.

567.3.3 Security Procedures for Registering Contracts

Effective Date: 02/26/2018

In order for a contract to be registered as a classified or dual performance contract, several steps must be completed.

After the award, the COR must send an electronic copy of the signed and dated contract to **SECNISP@usaid.gov** along with the Commercial and Government Entity (CAGE) code for the contractor. DSS issues a CAGE code to an entity in order to track basic facility information. The CAGE code assists the IIS Branch with verifying the FCL. The contract must clearly state the period of performance and contain one of the required security clauses; either classified or dual performance. The contract number must be included on all pages of the contract. For dual performance contracts, the specific positions/titles requiring access to classified information must be clearly stated within the contract (see **567.3.1**).

If a contract is requesting Sensitive Compartmented Information (SCI) access for any contractor personnel, the positions/titles requiring such access must be clearly stated in the contract along with an unclassified justification as to why that level of access is required. The unclassified justification must express the reasons in which SCI access is required.

The IIS Branch will review the contract to ensure the aforementioned elements are included and will verify the FCL with DSS. The contractor name and address registered with DSS under the company's FCL must match the contractor name and address on the contract in order for a DD-254 to be issued. If the contractor name or address on the contract does not match the information on file with DSS for the FCL, the contract will be sent back for correction and will not be registered under the NISP. The COR should ensure the information matches in its entirety prior to submitting it to **SECNISP@usaid.gov**.

Once all information is verified, the IIS Branch will issue a complete form DD-254 to the requestor.

567.3.4 Security Clearance

Effective Date: 08/03/2021

Contractor personnel, who need access to restricted areas within USAID/W and access to classified national security information, when there is a job-related "need-to-know", must obtain and maintain a security clearance from DSS' Defense Industrial Security Clearance Office (DISCO). The COR and Facility Security Officer (FSO) must work together to submit to DSS all such security clearance requests or inquiries. For more information on this process, visit **DCSA's Web site**.

The Office of Security, Personnel Security Division (SEC/PSD) does not conduct background investigations for the adjudication of security clearances for contractor personnel (see **ADS 566, Personnel Security Investigations and Clearances**). No exceptions can be made to this rule.

In accordance with the NISP, USAID is required to use the Defense Counterintelligence Security Agency (DCSA), for security clearances for contractor personnel.

567.3.5 Building and Classified Information Access for Cleared Contractor Personnel

Effective Date: 02/26/2018

The FSO must submit a Visit Authorization Letter (VAL)/Visit Authorization Request (VAR) to the respective AMS for cleared contractor personnel to obtain a Facility Access Card (FAC). A VAL/VAR is a request that permits an employee to enter USAID office space to perform his/her job duties. The VAL/VAR includes a full identification of the visitor, including his/her security clearance level.

All VALs/VARs must meet the requirements of the **NISPOM, Chapter 6**, regarding visits. Contractor personnel must comply with security directives listed on the DD-254, Contract Security Classification Specification form, in addition to HSPD-12 requirements.

The FSO must electronically send the VAL/VAR to the USAID AMS of the B/IO that the contract personnel are working under. The AMS will then send it to the Office of Security's Domestic Security Branch, **SECDomestic@usaid.gov**, along with the **AID 565-1, Request for Federal Identification Card/Facility Access Card (FAC)** form.

The COR must coordinate with the B/IO AMS in submitting requests for USAID FACs for all contractor personnel.

See **ADS 565, Domestic Security Programs**, for more information on the badge issuance process and physical access to USAID/W facilities.

567.3.6 Self-Employed Contractors (Consultants)

Effective Date: 02/26/2018

Self-employed contractors are typically also referred to as "consultants." If the contractor personnel is paid by another contractor, the paying contractor obtains the personal security clearance through DSS for the individual actually performing the work. For consultants hired directly by USAID, SEC/PSD will process the contractor personnel's security clearance. For consultants hired by the Office of Human Capital and Talent Management (HCTM), also known as WAEs (When Actually Employed), that typically do not exceed a contract for more than 120 days, SEC/PSD will conduct the investigation (see **ADS 566, Personnel Security**

Investigations and Clearances and **Section 2-212 of the NISPOM** for additional guidance).

567.3.7 Subcontractors
Effective Date: 02/26/2018

Prime contractors are required to issue DD-254s for subcontractors. USAID SEC does not issue DD-254s for subcontractors. Prime contractor FSOs must provide the subcontractor's DD-254 to the IIS Branch through **SECNISP@usaid.gov** to demonstrate that the subcontractor has the requisite facility clearance for the level of security classification. If the prime contract is classified, then the subcontract under that same contract number will be considered a classified subcontract. If the prime contract is dual performance, then the subcontract under that same contract number may be considered classified, unclassified, or dual performance.

A prime contractor cannot subcontract any part of a classified contract to a contractor that does not have a valid facility clearance. Excluded from this are subcontracts or procurements of commercial goods or services unless they require access to classified information and restricted areas. Security requirements flow down to the subcontractor and therefore are applicable to all contractor personnel under the subcontract.

If the subcontractor DD-254 is not provided to SEC NISP, the subcontractor employees will not be registered through USAID's NISP and contractor personnel will not obtain access to USAID facilities or a FAC.

567.3.8 Contract Extensions
Effective Date: 02/26/2018

When a contract or award is extended, the CO or COR must send the signed extension paperwork to **SECNISP@usaid.gov** for review. The SEC NISP team will review the paperwork to verify it is signed, verify the company's Facility Clearance to ensure its status has not changed, verify that the name of the company and address registered with DSS match the modification, and issue an updated DD-254 reflecting the new period of performance. The new period of performance must be clearly stated in the signed extension paperwork. Letters of intent to extend are not accepted as contract extensions.

567.3.9 Suspension of Physical Access for Contractor Personnel
Effective Date: 02/26/2018

SEC may suspend physical access to USAID offices when there are grounds to question an individual's continued access eligibility.

When SEC suspends an individual's physical access, SEC must notify the following, in writing, of the suspension and the reasons for the action:

- The individual,

- The COR,
- The CO, and
- DSS, if applicable.

DSS reserves the right to suspend security clearances issued by them in accordance with DSS policies and procedures. The COR is responsible for informing the IIS Branch through **SECNISP@usaid.gov** of any suspensions of contractor personnel (see **ADS 565, Domestic Security Programs,** for additional information on suspension of physical access to USAID facilities).

567.3.10 Contract Completion

Effective Date: 02/26/2018

The COR must notify the IIS Branch when the contract is either completed (final delivery of goods or services) or the period of the contract ends or is terminated, whichever occurs first. The COR must coordinate with the IIS Branch and the AMS Officer or Executive Officer to ensure contractor access to Agency information and facilities is terminated (see **ADS 306mah**).

At the point the contractor personnel no longer requires a USAID-issued badge, the COR is responsible for ensuring the badge is returned to SEC at the conclusion of the contract or when the individual is no longer working under the mechanism in which the badge was issued, whichever occurs first.

567.3.11 Return of Federal Identification Card (ID) FAC

Effective Date: 02/26/2018

CORs are responsible for ensuring departing contractor personnel's Federal ID FACs are returned when:

- That individual leaves the Agency,
- That individual is no longer working under the hiring mechanism in which they applied for and received the FAC, and
- At the conclusion of the contract or when the individual is no longer working under the contract in which the card was issued.

Contractor personnel may not retain their FAC when changing contracts or hiring mechanisms without confirmation from SEC. CORs must coordinate with SEC to ensure the contractor personnel's contract information is updated and that the FAC reflects the proper clearance level of their new contract or position.

For departing contractor personnel, the COR in Washington must return the FAC(s) to SEC within two (2) business days after receipt of the FAC(s) from the contractor personnel. If SEC is closed for the day, CORs may turn in PIVs/FACs to

the guards at the Ronald Reagan Building's 14th Street Guard Desk. The COR in Washington must also return the remote authentication token, along with any USG furnished equipment to the B/IO AMS in which the contractor personnel was assigned, within two (2) business days of receipt from the contractor personnel.

See **ADS 565, Domestic Security Programs** for more information on the return of PIVs/FACs.

567.3.12 Separation from USAID (Debriefings)
Effective Date: 02/26/2018

SEC must provide a security debriefing to all contractor personnel who were granted access to Sensitive Compartmented Information (SCI) through USAID. All contract personnel who received an SCI indoctrination and signed a Form 4414 SCI Nondisclosure Agreement through SEC are required to meet with a member of the IIS Branch to receive a security debriefing, sign the debriefing section of the Form 4414, and turn in their FAC reflecting their SCI access. CORs are responsible for ensuring the contractor personnel complete this process prior to separating from USAID.

567.4 MANDATORY REFERENCES

567.4.1 External Mandatory References
Effective Date: 02/26/2018

a. **Atomic Energy Act of 1954**

b. **EO 13467, "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information," of June 30, 2008**

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

d. **Federal Register – Volume 58 No. 5 – Friday, January 8, 1993 Presidential Documents**

e **The Freedom of Information Act, 5 USC 552**

f. **The Defense Security Service – Facility Clearance Branch**

g. **The National Industrial Security Program Operating Manual (NISPOM)**

h. **The Privacy Act of 1974, 5 USC 552a**

567.4.2 Internal Mandatory References
Effective Date: 02/26/2018

a. **ADS 302, USAID Direct Contracting**

b. **ADS 565, Domestic Security Programs**

c. **ADS 566, Personnel Security Investigations and Clearances**

d. **ADS 569, Counterintelligence Program**

567.4.3 Mandatory Forms
Effective Date: 02/26/2018

a. **AID Form 565-1, Request for Federal Identification Card/Facility Access Card**

b. **DD-254, Contract Security Classification Specification**

567.5 ADDITIONAL HELP
Effective Date: 02/26/2018

a. For National Industrial Security Program (NISP) related questions contact: **SECNISP@usaid.gov**

b. **Statement of Work – Security Classification Specification for Classified Contracts**

c. **Statement of Work - – Security Classification Specification for Dual Performance Contracts**

567.6 DEFINITIONS
Effective Date: 02/26/2018

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**)

classified contract
Contracts with positions requiring access to classified information and/or designated restricted space. These procedures are applicable to licensees, grantees, and certificate holders to the extent legally and practically possible within the constraints of applicable law and the Code of Federal Regulations. (**Chapter** **562** and **567**)

classified national security information (classified information)
Information that has been determined pursuant to EO 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.

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.

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

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**)

cleared 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)) (**Chapter 567**)

cognizant security agencies (CSAs)
Agencies of the Executive Branch that have been authorized to establish an industrial security program to safeguard classified information when disclosed or released to U.S. industry. (**Chapter 567**) (**NISPOM**)

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. (**Chapters 302**, **331**, **567**)

contracting officer's representative (COR)
The individual who performs functions that are designated by the Contracting Officer, or is specifically designated by policy or regulation as part of contract administration. (**Chapter 567**)

contractor personnel
An individual who performs work for or on 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 567**)

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, 567**)

dual performance award/contract
Contracts with some positions requiring access to classified information and/or designated restricted space while other positions do not require access to classified information and/or designated restricted space. These procedures are applicable to licensees, grantees, and certificate holders to the extent legally and practically possible within the constraints of applicable law and the Code of Federal Regulations. (**Chapter 562** and **567**)

entity eligibility
According to the National Industrial Security Program Operating Manual (NISPOM), an administrative determination that, from a national security standpoint, an entity is eligible for access to classified information at the same or lower classification category as the clearance being granted. (**Chapter 567**)

facility access
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 567**)

facility access card (FAC)
An identification card issued to employees, detailees, or contractors who do not qualify for a federal ID card or who do not represent USAID to other agencies. (**Chapter 567**)

federal credential
A standardized form of identification as prescribed by Homeland Security Presidential Directive (HSPD) 12 that (1) is issued based on sound criteria for verifying an individual employee's identity; (2) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (3) can be rapidly authenticated electronically; and (4) is issued only by providers whose reliability has been established by an official accreditation process. (**Chapter 565** and **567**)

need-to-know
A determination made by a possessor of classified information that a prospective recipient, in the interest of national security, needs 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**)

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. (**Chapter 566** and **567**)

restricted space
An area where storage, processing, discussions, and handling of classified material is authorized. (**Chapter 565** and **567**)

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**, **567**)

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 545**, **552**, **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, 567**)

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. (**Chapter 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** and **567**)

unrestricted space
An area where storage, processing, discussion, and handling of classified material is not authorized. (**Chapter 565** and **567**)

USAID/W
Refers to all Washington, DC office locations, including but not limited to the Ronald Reagan Building, SA-44, Crystal City Plaza 3, and Potomac Yards II. (**Chapter 567**)

visit authorization letter (VAL)/visit authorization request (VAR)
A request by a contractor to enter a USAID facility to perform services. (**Chapter 567**)

567_080321