ADS Chapter 567

Classified Contracts and Awards Under USAID's National Industrial Security Program

Document Quality Check Date: 11/12/2012
Full Revision Date: 05/29/2012
Responsible Office: SEC/CTIS
File Name: 567_111212

Functional Series 500 - Management Services
ADS 567 - Classified Contracts and Awards Under USAID's National Industrial Security Program
POC for ADS 567: Diane Fitzgerald, (202) 712-0894, dfitzgerald@usaid.gov

This chapter, including the title, has been modified in its entirety.

Table of Contents

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

567.1 OVERVIEW

Effective Date: 05/29/2012

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. (See **E.O. 13526, Classified National Security Information** for the protection of information classified under **EO 13526** as amended, or its successor or predecessor orders, and the **Atomic Energy Act of 1954** as amended, and **12 FAM 570**.)

The National Security Council is responsible for providing overall policy direction for the NISP. The Secretary of Defense has been designated Executive Agent for the NISP by the President. 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 uses a large number of institutional contractors and grant/cooperative agreement recipient employees to perform various missions and functions. The USAID Industrial Security Program is in place to ensure that these contract and recipient employees safeguard Federal Government classified information. The program is guided by **E.O. 13526, Classified National Security Information**, **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 National Industrial Security Program. It provides policy directives and required procedures and guidance on the security requirements and language for acquisition and assistance awards falling under the provisions of the NISP. Such contracts or assistance awards require the contractor or recipient to obtain a facility security clearance (FCL) in order for the contractor or recipient employees to have access to classified information or restricted areas.

This chapter does not address background investigations or the Facility Access investigative process. Security clearance actions regarding U.S. Personal Service Contracts and other employee categories 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).**

567.2 PRIMARY RESPONSIBILITIES

Effective Date: 05/29/2012

The following Bureaus/Independent Offices (B/IOs) have primary responsibilities for specific policy directives and required procedures within this chapter.

a. The **Director, Office of Security (D/SEC)** is the senior Agency official responsible for enforcing **E.O. 13526, Classified National Security Information** and **HSPD-12**.

b. The **Office of Security, Industrial Security Program Manager (ISPM)**

(1) Issues USAID security policies and standards;

(2) Serves as liaison to the Department of Defense, Defense Security Service (DSS) regarding the National Industrial Security Program; and

(3) Coordinates corrective action with contractors, award recipients and/or the DSS when employees fail to comply with the security requirements of their contracts or awards.

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)** and **Agreement Officers (AOs)** and Mission Executive Officers are responsible for inserting security specifications into contracts and assistance awards.

e. **Contracting Officer's Representatives (CORs)** and **Agreement Officer's Representatives (AORs)** are responsible for assisting COs and AOs (respectively) with establishing and administering security specifications for contracts and assistance awards. COR and AOR duties include monitoring classified contractors' and recipients' compliance with the security specifications included in their contracts, grants, and cooperative agreements, and notifying the contracting or agreement officer and SEC of any problems or suspected non-compliance with these contract requirements.

The COR and AOR must be familiar with the security specifications in the awards for which they are a COR or AOR and with the USAID regulations that apply. These include **ADS 545, Information System Security**, and **ADS 565, Physical Security Programs (Domestic)**, as well as ADS 567.

f. **Bureau/Independent Office (B/IO) Administrative Management Specialists (AMSs)** are responsible for ensuring that Visit Authorization Letters (VALs) are completed and delivered to SEC Domestic Security (SEC/DS).

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

h. **Department of Defense, 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: 05/29/2012

USAID program, project, and contracting personnel 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 and grants/cooperative agreements. This chapter applies to recipients of grants or cooperative agreements to the same extent as to contractors if the terms and conditions of their awards require their employees to have unescorted access to USAID restricted space and/or access to classified information, as described below.

567.3.1 Determining Contract or Award Security Levels

Effective Date: 05/29/2012

a. Pre-Award Procedures

The B/IO or Mission Project Officer must first determine whether a contract or assistance award performance will be classified.

A contract or assistance award will be classified if:

- The contractor or recipient employees will require unescorted access to USAID restricted space within USAID/W, and/or
- The contractor or recipient employees will require access to classified information.

Contractor or recipient employees working under a classified contract or assistance award require a security clearance. If the contractor or recipient employees are not working under a classified contract or assistance award, they will need a Facility Access (formerly known as Employment Authorization) and therefore would not fall under this ADS chapter. The Facility Access process is discussed in **ADS 566, Personnel Security Investigations and Clearances**.

If a contract or assistance award is determined to be classified, it does not mean that the terms within the contract or assistance award are classified. It focuses on the type of access that is required: access to classified information or restricted space.

b. Security Language

If the B/IO or Mission Project Officer determines a contract or assistance award to be classified, the COR or AOR must obtain specific security language from the Industrial Security Program Manager (ISPM) through **SECNISP@usaid.gov** and must then provide it to the CO or AO for inclusion in the contract or assistance award. Without this language, contractor and recipient employees cannot gain unescorted access to restricted space in AID/W nor have access to classified materials.

c. Post-Award Procedures

If the contract is granted prior to the inclusion of the required security language clause, an amendment/modification must be made to ensure it is incorporated into the contract or assistance award.

567.3.2 Facility Clearance

Effective Date: 05/29/2012

a. According to the NISPOM, if the contract or assistance award is determined to be classified, the contractor or recipient must have or be able to maintain a valid Facility (Security) Clearance (FCL) equal to the level of Secret or Top Secret, as specified in the contract or award. This is required to ensure classified information entrusted to the private sector is properly safeguarded. Exceptions to this must be approved by SEC in coordination with the CO/AO and requiring office and will be granted on a case-by-case basis.

USAID SEC will prohibit a contractor or award recipient without a valid Facility Clearance from gaining access to USAID restricted space and will deny the contractor or recipient employees access to classified information. An FCL is obtained through the Defense Security Service (DSS).

To obtain an FCL, the contractor or recipient must complete the following steps:

1) Sponsorship

Contractors or recipients must be sponsored for a Department of Defense (DoD) facility security clearance by a Government entity and apply for one through the DSS. The Government entity that sponsors a contractor or recipient will be the USAID B/IO through which the contractor or recipient employee will be working. The Government entity will provide the contractor or recipient with a sponsorship letter.

USAID SEC does not sponsor contractors or recipients for an FCL or personnel security clearance, nor does it represent the contractor or recipient employee in his/her effort to obtain such clearances from the 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 or recipient.

2) Contract Security Classification Specification Form, DD254

The DSS requires contractors or recipients to have a draft DD 254 when applying for an FCL. The COR or AOR can request the form from **SECNISP@usaid.gov** and must assist SEC in preparing it. The COR or AOR must inform the ISPM when an FCL is issued. The Industrial Security group will issue a non-draft DD 254 when the DSS grants the contractor or recipient an FCL.

Block 13 of the DD 254 provides supplemental security guidance that incorporates security specifications into the contract or award. The COR or AOR is responsible for immediately communicating any changes in the FCL status to the ISPM.

3) Submission of Request to DSS

The contractor or recipient must submit the sponsorship letter, 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, **http://www.dss.mil/isp/fac_clear/fac_clear_check.html.** An example of the sponsorship letter is also included on this Web site.

567.3.3 Security Procedures for Acquisition and Assistance Awards

Effective Date: 05/29/2012

After the award, the COR or AOR must send an electronic copy of the contract or assistance award document to **SECNISP@usaid.gov** along with the Commercial and Government Entity (CAGE) code for the contractor or recipient. The CAGE code is provided by DSS when an FCL is issued.

The ISPM will review the contract or assistance award to ensure the correct security language is included and will verify the FCL with the DSS. Once verified, the ISPM will issue a complete form **DD 254** to the COR or AOR for modifying into the contract.

567.3.4 Security Clearance

Effective Date: 05/29/2012

Contractor or recipient employees who need access to restricted space within USAID/W and/or access to National Security Information when there is a job-related "need-to-know" must obtain a security clearance from the DSS' Defense Industrial Security Clearance Office (DISCO). The COR, AOR, and Facility Security Officer (FSO) must work together to submit to the DSS all such security clearance requests or inquiries.

USAID SEC/PS does not conduct background investigations for the adjudication of security clearances for contractor or recipient employees. These investigations are

conducted by the DSS. The cleared contractor must have a designated FSO. The FSO must submit requests for personnel security clearances to DSS. (See **Federal Register – Vol. 58 No. 5 Section 202**)

567.3.5 Building and Classified Information Access for Contract and Recipient Employees

Effective Date: 05/29/2012

The FSO must submit a Visit Authorization Letter (VAL) to his/her respective AMS for an employee to obtain a building access badge. A VAL is a request that allows an employee to enter USAID office space to perform his/her job duties. The VAL includes a full identification of the visitor, including his/her security clearance level.

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

The FSO must submit a Joint Personnel Adjudication System (JPAS) Summary Sheet on all cleared employees to the Administrative Management Specialist (AMS). The JPAS Summary Sheet is contained in the JPAS system, which can be accessed by FSOs through the DSS. The FSO must electronically mail the VAL and the JPAS Summary Sheet to the USAID AMS with whom they have been working. The AMS will then send it to the SEC Badges Mailbox, **SECDomestic@usaid.gov**, along with the AID 500-1, Request for Federal Identification Card/Facility Access Card (FAC), form. **[Note: This form is available on the Office of Security intranet Web site.]**

The COR and AOR must coordinate with the B/IO AMS in submitting requests for USAID Facility Access Cards (FACs) for all contractor or recipient employees.

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

567.3.6 Self-Employed Contractors (Consultants)

Effective Date: 05/29/2012

For the purpose of the industrial security program, self-employed contractors are typically also referred to as “consultants.” If the individual is paid by another contractor, the paying contractor obtains the personal security clearance through the Defense Security Service (DSS) for the contractor actually performing the work.

For individuals contracted directly by USAID, excluding PSCs, SEC/PS will process the contractor employee’s security clearance. (See **ADS 566** for additional guidance) Consultants or experts that USAID hires through OHR under Federal personnel regulations are not covered by this guidance.

567.3.7 Subcontractors/Subrecipients

Effective Date: 05/29/2012

Prime contractors or recipients issue DD 254s for subcontractors or subrecipients. Prime contractor/recipient FSOs must provide the subcontractor's/subrecipient's DD 254 to the USAID ISPM to demonstrate that the subcontractor/subrecipient has the requisite facility clearance for the level of security classification. If the prime contract or award is classified , then the subcontract/subrecipient under that same contract/award number will be considered a classified subcontract or sub-award. A prime contractor or recipient cannot subcontract or sub-award any part of a classified contract or award to a company or recipient that does not have a facility clearance. Excluded from this are subcontracts or procurements of commercial goods or services unless they require access to classified information and/or restricted space.

If the subcontractor/subrecipient DD 254 is not shared with the USAID ISPM, the subcontractor/subrecipient employees will not obtain access to USAID facilities or a Facility Access Card (FAC).

567.3.8 Suspension of Contractor Physical Access

Effective Date: 05/29/2012

SEC may suspend physical access to USAID offices when there are grounds to question an employee'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/AOR,
- The CO/AO, and
- DSS, if applicable.

DSS reserves the right to suspend security clearances issued by them in accordance with DSS policies and procedures.

567.3.9 Contract/Assistance Award Completion

Effective Date: 05/29/2012

The COR or AOR must notify the ISPM when the contract or assistance award is either completed (final delivery of goods or services), or the period of the contract or assistance award ends or is terminated, whichever occurs first. The ISPM will coordinate with the COR or AOR to ensure contractor or recipient access to Agency information and facilities is terminated (see **12 FAM 575.5**).

At the point the contractor or recipient employee no longer requires a USAID-issued badge, the COR or AOR is responsible for ensuring that the FSO for the parent company returns the badge to SEC at the conclusion of the contract or award or when the employee is no longer working under the mechanism in which the badge was issued.

567.4 MANDATORY REFERENCES

567.4.1 External References

Effective Date: 05/29/2012

a. 12 FAM 260, Counterintelligence

b. 12 FAM 570, Industrial Security Program

c. 12 FAM 573.2-1, Self-Employed Contractors

d. 12 FAM 577, Clearance Processing

e. Atomic Energy Act of 1954

f. E.O. 13526, Classified National Security Information

g. 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

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

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

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

k. http://www.dss.mil/isp/fac_clear/fac_clear_check.html
(This Web site provides procedures on obtaining a facility clearance.)

l. The National Industrial Security Program Operating Manual (NISPOM)

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

567.4.2 Internal Mandatory References

Effective Date: 05/29/2012

a. ADS 302, USAID Direct Contracts

b. **ADS 565, Physical Security Programs (Domestic)**

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

d. **ADS 569, Counterintelligence Program**

567.4.3 Mandatory Forms
Effective Date: 05/29/2012

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

b. **AID Form 500-1, Request for Issue (or Reissue) of Building Pass**

c. **AID 500-3, Security Investigation and Clearance Record**

d. **DD 254, Contract Security Classification Specification**

e. **FD-258, Fingerprint**

f. **Standard Form 85P, Questionnaire for Public Trust Positions**

567.5 ADDITIONAL HELP
Effective Date: 05/29/2012

a. National Industrial Security Program (NISP) Related Questions - **SECNISP@usaid.gov**

b. **Statement of Work Security Clause for Classified Contracts**

567.6 DEFINITIONS
Effective Date: 05/29/2012

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**)

Agreement Officer (AO)
A person with the authority to enter into, administer, terminate and closeout assistance agreements, and make related determinations and findings on behalf of USAID. An Agreement Officer can only act within the scope of a duly authorized warrant or other valid delegation of authority. The term "Agreement Officer" includes persons warranted

as "Grant Officers." It also includes certain authorized representatives of the Agreement Officer acting within the limits of their authority as delegated by the Agreement Officer. (Chapters **303**, **304**)

A person representing the U.S. Government through the exercise of his/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**, **306**, **331**)

Agreement Officer's Representative (AOR)
The individual who performs functions that are designated by the Agreement Officer, or is specifically designated by policy or regulation as part of the administration of an assistance award (grant or cooperative agreement). (Chapter 567)

classified award
Contracts, grants, or cooperative agreements with positions requiring access to classified information and/or designated Restricted Space. These procedures are applicable to licensees, grantees, and certificate holders to the extent legally and practically possible within the constraints of applicable law and the Code of Federal Regulations. (Chapters **562**, 567)

classified national security information (classified information) Any data, file, paper, record, or computer screen containing information associated with the national defense or foreign relations of the United States and bearing the markings: Confidential, Secret, or Top Secret. (Chapters **545**, **552**, and **568**)

Information that has been determined pursuant to **E.O. 13526, Classified National Security Information** 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)

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)

contractor employee
Refers only to U.S. citizens employed as an independent contractor, fellow, institutional contractor, or any other category of individual, not a direct-hire, potentially requiring a security clearance to work on USAID information or material or have unescorted access in USAID space. (Chapter 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. (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)

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**)

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. (Chapters **562**, **566**, 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)

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

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

institutional contractor employee
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 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. (Chapters **566**, 567)

recipient
An organization receiving direct financial assistance (a grant or cooperative agreement) to carry out an activity or program. (Chapters **303**, **304**, **305**, 567)

recipient employee
An individual that is working for a recipient. (Chapter 567)

restricted space
An area where storage, processing, discussions, and handling of classified material is authorized. (Chapters **565**, 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. (Chapters **562**, **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. (Chapters **566**, 567)

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

USAID/W
Refers to all Washington, D.C. office locations, including but not limited to the Ronald Reagan Building, SA-44, and Potomac Yards II. (Chapter 567)

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

567_091416