



USAID
FROM THE AMERICAN PEOPLE

ADS Chapter 565

Physical Security Programs (Domestic)

Revision Date: 09/26/2007
Responsible Office: SEC/OD
File Name: 565_092607_cd49

Functional Series 500 - Management Services
Chapter 565 - Physical Security Programs (Domestic)

Table of Contents

565.1	OVERVIEW	4
565.2	PRIMARY RESPONSIBILITIES.....	4
565.3	POLICY DIRECTIVES AND REQUIRED PROCEDURES.....	4
565.3.1	USAID Headquarters Building Security Standards	4
*565.3.2	Designated Restricted and Unrestricted Areas	5
565.3.3	Access to and Within USAID Headquarters	5
*565.3.3.1	Authorization to Work in USAID Headquarters	5
*565.3.3.2	Obtaining a USAID Headquarters Building Pass, Federal ID	6
*565.3.3.3	Use of USAID Headquarters Building Passes or Federal Credentials	7
*565.3.3.4	Access to Offices and Suites within USAID Headquarters	7
*565.3.3.5	TDY Building Passes.....	8
*565.3.3.6	Temporary Building Passes.....	9
*565.3.3.7	Access for Department of State Employees	9
*565.3.3.8	Replacement Building Passes	10
*565.3.3.9	Required Verification of Building Passes, Federal ID Card/FAC ...	10
*565.3.3.10	Return of Building Pass or Federal ID Card/FAC	10
*565.3.3.11	Confiscating Invalid Building Passes and Federal ID Cards.....	11
*565.3.4	Visitors and Guests to USAID/W	11
*565.3.5	Access to Domestic Department of State Building Facilities (Physical Access) for USAID Employees	12
*565.3.6	Use of Cameras, Photographic or Video Teleconferencing Equipment.....	12
*565.3.7	Alteration of Security Systems or Locks.....	13
*565.3.8	Safe and Door Combination Control.....	14
*565.3.9	Movement of Classified Equipment.....	14
*565.3.10	Property Passes	14
*565.3.11	Fingerprints	15

*An asterisk indicates that the adjacent material is new or substantially revised.

2

*565.3.12	Deliveries to USAID/W.....	15
*565.4	MANDATORY REFERENCES.....	15
*565.4.1	External Mandatory References	15
*565.4.2	Internal Mandatory References	16
565.4.3	Mandatory Forms	16
565.5	ADDITIONAL HELP	16
*565.6	DEFINITIONS.....	16

*An asterisk indicates that the adjacent material is new or substantially revised.

ADS Chapter 565 - Physical Security Programs (Domestic)

565.1 OVERVIEW

Effective date: 09/24/2007

This chapter provides the policy directives and required procedures for the protection of USAID/Washington (USAID/W) employees and national security information in USAID headquarters buildings.

565.2 PRIMARY RESPONSIBILITIES

Effective date: 09/24/2007

- a. The **Director of Security (D/SEC)** is responsible for physical security programs in USAID/W.
- b. The **Chief, Office of Security, Personnel, Information, and Domestic Security Division (SEC/PIDS)** is responsible for implementing physical security programs in USAID headquarters buildings.
- c. The **Director of the Bureau for Management, Office of Administrative Services (M/AS)** is responsible for ensuring that SEC is advised (in advance if possible) of any matters affecting the physical security systems in USAID headquarters buildings.
- d. **USAID Senior Managers** are responsible for ensuring staff compliance with the security policy directives and required procedures contained in this chapter.
- e. The **Unit Security Officer (USO)** in each Bureau/Independent Office is responsible for the safe and door security in his or her Bureau/Independent Office.
- f. Each **USAID employee** is responsible for complying with the security policy directives and required procedures contained in this chapter.

565.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES

Effective date: 09/24/2007

565.3.1 USAID Headquarters Building Security Standards

Effective date: 09/24/2007

The USAID headquarters building is designated as a Level IV facility as defined in the Department of Justice Vulnerability Assessment of Federal Facilities Report. The physical security standards specified in this report apply to the USAID headquarters building. (See [Department of Justice Vulnerability Assessment of Federal Facilities Report](#))

*An asterisk indicates that the adjacent material is new or substantially revised.

***565.3.2 Designated Restricted and Unrestricted Areas**

Effective date: 09/24/2007

*All office space within USAID/W headquarters is designated as “restricted” or “unrestricted” space. A change in designation for any office or office suite must be requested in writing by the AA or Office Director to D/SEC. SEC maintains a listing of all restricted and unrestricted office space.

*Designated **restricted space** is defined as an area where storage, processing, discussions, and handling of classified material may occur. Designated restricted areas are authorized for classified equipment such as stand alone computers, ClassNets, and STU/STE equipment.

*Upon request, SEC may grant unescorted access to designated restricted space to an authorized individual who has a valid national security clearance at the “Secret” level or higher. The security clearance must be properly certified to SEC in writing by the individual’s parent agency or organization. Other personnel requesting access to designated restricted space must be escorted by a cleared, authorized employee that has been granted “unescorted access” to the designated restricted area.

***Unrestricted space** is defined as an area where storage, processing, discussion, and handling of classified material are **not authorized**. Classified meetings or conversations are not authorized in designated unrestricted areas. Upon request, SEC may grant access to “unrestricted areas” to any authorized person(s) that has received a favorable background investigation as determined by SEC.

*All USAID overseas Missions are designated as unrestricted and prohibited from storage and processing of classified information. All classified information must be stored, processed, and discussed in the Controlled Access Area (CAA) inside the U.S. Embassy, as designated by the Regional Security Officer (RSO). (See [ADS 562.3.1](#))

565.3.3 Access to and Within USAID Headquarters

Effective date: 09/24/2007

***565.3.3.1 Authorization to Work in USAID Headquarters**

Effective date: 09/24/2007

*Only those individuals who have been the subject of a background investigation and have received a favorable review by SEC are permitted to work in the USAID headquarters building and be issued a USAID headquarters Building Pass or any physical access to USAID government space.

- *Only individuals with a current security clearance or appropriate background investigation verified by SEC are authorized to work within

*An asterisk indicates that the adjacent material is new or substantially revised.

USAID designated restricted areas.

- *Visitor passes are not to be requested or used for people to **work** in USAID space unless approved by SEC. Bureau/Independent Office AMS Officers must coordinate with SEC Personnel, Information and Domestic Security, Information and Domestic Security (SEC/PIDS/IDS) at least two work days in advance of a visitor's proposed work start time so that SEC has time to determine whether or not authorization for a visitor pass is appropriate. Emergencies are handled on a case-by-case basis.
- *SEC must specifically pre-approve unescorted access to restricted areas by individuals without a security clearance. This includes unescorted access by USAID Foreign Service Nationals (FSN) and Third Country Nationals (TCN) on temporary duty (TDY) to USAID/W headquarters. The Bureau/Independent Office AMS Officer must submit a request for such authorization to SEC/PIDS/IDS at least one full week in advance of the proposed work date. The coordination must include a security plan on how access by the uncleared person to national security information will be precluded. SEC will base approval on its assessment of the adequacy of the proposed measures.

***565.3.3.2 Obtaining a USAID Headquarters Building Pass, Federal ID Card or Facility Access Card (FAC)**

Effective date: 09/24/2007

*Individual USAID Direct Hires, Personnel Service Contractors, Private Industry Contractors, and other Government entities including Congress must be sponsored by a USAID Bureau/Independent Office to obtain a building pass, federal ID card, or FAC.

The sponsoring office must coordinate the request for a building pass for congressional personnel with the Bureau for Legislative and Public Affairs (LPA) and the Office of the Executive Secretariat (ES) before SEC will process the request.

*To obtain physical access to USAID/W or a federal ID card issued under [Homeland Security Presidential Directive-12 \(HSPD-12\)](#), AMS Officers must forward a completed [AID Form 500-1](#) to the "SEC Badges" (SECBadges@usaid.gov) mailbox. (See [AID Form 500-1](#)) It is the responsibility of the requesting Bureau/Independent Office AMS Officer to determine and specify the access level required by the individual(s).

*Before individuals are granted unescorted access to government facilities, all requirements of [HSPD-12](#) must be met. Requirements include, but are not limited to the following:

*An asterisk indicates that the adjacent material is new or substantially revised.

- *Successful adjudication of clearance or background investigation;
- *Sponsorship by AMS, M/HR, or other authorized individual(s);
- *Completion of in-person enrollment/identity proofing;
- *Attendance at appropriate SEC security briefing; and
- Authentication by the Badge Office.

All requests for physical access or the issuance of a federal ID card are reviewed and subject to approval by SEC.

***565.3.3.3 Use of USAID Headquarters Building Passes or Federal Credentials**

Effective date: 09/24/2007

*All individuals within the USAID headquarters building must possess and wear a valid USAID building pass, federal ID, Facility Access (FAC) card, or visitor pass at all times.

- *All employees must wear the pass, federal ID card, or FAC on the outer garment on the upper torso front with the front of the pass clearly visible.
- *The building pass, federal ID, or FAC card must not be altered (e.g., affix stickers, pins, or other items) in any way.
- *Employees are prohibited from lending building passes or ID cards to other employees, visitors, or other individuals.
- *Federal ID cards must be used only for official business purposes.
- SEC will make exceptions to the mandatory pass rule for small children and those visitors attending functions whose range of movement is severely limited.

***565.3.3.4 Access to Offices and Suites within USAID Headquarters**

Effective date: 09/24/2007

Authorized personnel may have access to rooms/suite entry door within USAID headquarters only after coordination/endorsements from their servicing AMS Officer, the AMS officer of the space in question, and SEC.

*Requests for access to office space within AID/W must be submitted by the Bureau/Independent Office AMS Officer to the "SEC Badges" (SECBadges@usaid.gov) mailbox. All requests must include the following:

*An asterisk indicates that the adjacent material is new or substantially revised.

- The employee's name,
- Door or suite number requested,
- Time of day requested (shift name), and
- The purpose of access.

*Requests for access to another Bureau/Independent Office space must also include approval from the AMS Officer of the space in question. SEC will notify the AMS Officer when the requested access changes are complete.

Hours of access to suite entry doors and turnstiles within USAID are defined as follows:

Always = 24 hours a day, seven days a week, holidays included;
Flex = 6:30 a.m. to 6:30 p.m., five days a week, no holidays or weekends;
Core = 8:30 a.m. to 5:30 p.m., five days a week, no holidays or weekends; and
Vendor = 7:30 a.m. to 3:30 p.m., five days a week, no holidays or weekends.

Access to freight elevators, GSA doors, and specific secured areas is granted on a case-by-case basis. To obtain access, follow the same procedures (above) for requesting access to a door or suite. Access to these areas may require additional time for approval and processing.

***565.3.3.5 TDY Building Passes**

Effective date: 09/24/2007

*Employees on Temporary Duty Assignment (TDY) in USAID/W headquarters may obtain a TDY badge at the 14th Street Visitor Control Desk. After verification of the individual's identity, employment status, clearance level, and sponsoring Bureau/Independent Office, a TDY badge will be issued for the duration of the TDY assignment.

*FSN employees must show their embassy-issued identification card at the 14th Street Visitor Control Desk before being issued an uncleared TDY building pass.

*To expedite the verification process, the sponsoring office (normally the Bureau/Independent Office AMS Officer) must send an e-mail to the "SEC Security" (SECSecurity@usaid.gov) mailbox which includes the following:

- The employee's name,
- Start and end dates of the TDY,

*An asterisk indicates that the adjacent material is new or substantially revised.

- Mission location,
- Clearance level, and
- The sponsor's contact information.

*TDY passes will enable employees to proceed unescorted through the turnstiles at 13 ½ and 14th Street lobbies into USAID space. The pass also permits the employee to enter USAID space that is approved for the clearance level of the TDY pass holder. AMS Officers may request that additional access be added to the TDY badge by following the procedures in **565.3.6**. Requests to add access to a TDY badge must also include the TDY badge number (located on the back of the card).

*Employees must return all TDY passes to the Visitor Control Desk upon completion of the TDY assignment.

*The Bureau/Independent Office AMS Officer may request a permanent photo building pass for any employee scheduled for TDY in USAID/W for more than five working days. Such requests must be submitted on an [AID 500-1](#) and sent electronically to the "SEC Badges" (SECBadges@usaid.gov) mailbox. All requests for physical access to government space are subject requirements of [HSPD-12](#).

***565.3.3.6 Temporary Building Passes**

Effective date: 09/24/2007

*Employees who report to work without their authorized building pass or federal ID card/FAC may request a temporary building pass (T Badge) from the 14th Street Visitor Control Desk. The uniformed guard is required to verify the identity of the employee before issuing the temporary badge. Temporary badges are not issued to any individual with an expired or otherwise invalid building pass or federal ID card. Unless special authorization is approved by SEC, a temporary pass will be issued for a period of one day.

*The employee's regular building pass or federal ID card/FAC will be deactivated until the temporary pass is returned to the 14th Street Visitor Control Desk. Employees are prohibited from using multiple building passes simultaneously (i.e., temporary or TDY pass and photo building pass).

***565.3.3.7 Access for Department of State Employees**

Effective date: 09/24/2007

*Department of State employees visiting USAID may request a temporary building pass at the 14th Street Visitor Control Desk. Unless authorized by SEC, all temporary building passes for Department of State employees are valid for a period of one day and must be returned at the conclusion of the visit.

*An asterisk indicates that the adjacent material is new or substantially revised.

***565.3.3.8 Replacement Building Passes**

Effective date: 09/24/2007

*Employees must immediately report any lost or stolen building pass, federal ID card, or FAC to the AMS Officer and the SEC Main Desk at (202) 712-0990. The employee may request a replacement badge by completing the [AID 500-1](#). The [AID 500-1](#) must be submitted electronically to the “SEC Badges” (SECBadges@usaid.gov) mailbox by the AMS Officer. Employees must wait a minimum of five working days for authorization for a replacement badge.

*Employees requesting replacement federal ID cards are subject to all requirements for enrollment, identify proofing, and authentication under the [HSPD-12](#) program.

***565.3.3.9 Required Verification of Building Passes, Federal ID Card/FAC**

Effective date: 09/24/2007

*Uniformed guards are required to positively identify the employee by examining the photograph on the front of the badge. All employees must cooperate with the identification process. If the employee does not resemble the photograph on the badge, the uniformed guard may request the employee report to the Badge Office for an updated photograph. Employees who do not comply will have their building badge access suspended until a replacement badge is obtained.

***565.3.3.10 Return of Building Pass or Federal ID Card/FAC**

Effective date: 09/24/2007

An employee must return their building pass or federal ID card/FAC when

- *An employee or contractor leaves the Agency, or
- *An employee is no longer working under the employment mechanism in which they applied for and received the building pass or federal ID card/FAC.

*All cards must be returned to SEC upon departure.

- *USDH Employees - are required to return their identification cards to SEC during the mandatory security debriefing and employee “check out” procedures.
- *PSC Employees, Uncleared Institutional Contractors and Detailees - the Agency Sponsor (Bureau/Independent Office AMS Officer) is responsible for collecting the identification cards from employees at the conclusion of the contract or detail.

*An asterisk indicates that the adjacent material is new or substantially revised.

- *Cleared Institutional Contractors – the Facility Security Officer (FSO) for the parent company is responsible for returning the card to SEC at the conclusion of the contract or when the employee is no longer working under the mechanism in which the card was issued.

***565.3.3.11 Confiscating Invalid Building Passes and Federal ID Cards**

Effective date: 09/24/2007

*The security officers posted at the USAID turnstiles will confiscate any expired or invalid building pass or federal identification card/FAC. The Bureau/Independent Office AMS Officer must complete a new [AID 500-1](#) to request re-issuance of the card or pass.

***565.3.4 Visitors and Guests to USAID/W**

Effective date: 09/24/2007

*All visitors and guests requiring access to the USAID headquarters (Ronald Reagan Building (RRB)/Washington, D.C.) must present a valid identification with photograph (driver's license, U.S. Government-issued ID card, U.S. passport, State Department building pass, or USAID-issued building pass) to the USAID uniformed guard(s) before they may enter USAID space in the RRB.

*Additionally, visitors and guests, excluding Department of State employees with proper State issued identification, will be subject to metal detection and package screening before entering USAID space.

*When uncleared individuals, such as building construction contractors, are required to enter or remain in the building after working hours, the direct-hire employee from the sponsoring Bureau/Independent Office authorizing the work must arrange for an escort and obtain SEC concurrence. Such individuals must

- *Sign in and out on the appropriate register designated by SEC,
- *Wear visitor's passes for the duration of the visit, and
- *Surrender visitor's pass at the 14th Street Visitor Control Desk when leaving USAID space for the day.

*The Bureau/Independent Office escort is responsible for ensuring visitors comply with appropriate sign in/sign out procedures.

*USAID employees who escort or approve the admittance of an individual are responsible for the individual's compliance with the pass requirements and his or her prompt departure from the building immediately following completion of their business. Visitors must be escorted by the escort official or sponsor at all times while in USAID space during the duration of their visit, with the exception of visits to common area restrooms.

*An asterisk indicates that the adjacent material is new or substantially revised.

***565.3.5 Access to Domestic Department of State Building Facilities (Physical Access) for USAID Employees**

Effective date: 09/24/2007

*Access to domestic Department of State facilities may be added to Federal ID or [Facility Access Cards](#). SEC only sponsors access to Main State (HST Building) on Federal ID cards. All other requests for access to State facilities must be requested directly from the State Department sponsor or Unit Security Officer by the employee or Bureau/Independent Office AMS Officer.

***565.3.6 Use of Cameras, Photographic or Video Teleconferencing Equipment**

Effective date: 09/24/2007

*The use of cameras or photographic equipment is not permitted within the USAID portion of the Ronald Reagan Building (RRB). This restriction does not apply to the public portion of the USAID Public Information Center on the Mezzanine level. A camera is defined as any personally owned still, motion, or video recording device, including cell phones with a camera feature and cameras attached to computer equipment.

*Requests to waive the camera restriction may be granted on a case-by-case basis by SEC for special occasions and ceremonies. The request must be sent to the "SEC Security" (SECSecurity@usaid.gov) mailbox at least two full business days prior to the day of the planned use. The request must include the following:

- *The identity of the person bringing the camera;
- *The make and model of the camera;
- *A description of where the photographs will be taken; and
- *The intended subject and purpose of the photographs.

*SEC will provide guidance on inspecting the location prior to the event to ensure that no classified or sensitive but unclassified (SBU) information is visible. The requestor is responsible for completing the inspection prior to the arrival of guests.

*Members of visiting official delegations and credentialed media representatives may bring cameras into USAID space after approval from LPA and coordination with SEC. The event sponsor must coordinate with LPA's Press Office no less than one full business day before the planned event. LPA will notify SEC when the request has been approved.

*An asterisk indicates that the adjacent material is new or substantially revised.

*In cases where advance notification is not possible, (e.g., a breaking news story) LPA must contact SEC directly by calling SEC's Main Desk at (202) 712-0990 to coordinate and authorize camera usage.

*The installation and/or use of video teleconferencing equipment, Web cameras, or other devices which transmit audio or video is prohibited unless approved in advance by SEC. All requests for exception must be presented to SEC in writing. Written requests must be directed to the attention of the SEC's Chief, Personnel, Information and Domestic Security Division. Requests must include the following:

- *A description of the equipment, including all specifications;
- *The location where the equipment will be installed;
- *The proposed uses for the equipment;
- *A point of contact;
- *A security plan (if inside a designated restricted area); and
- *Approval from M/CIO, where applicable.

*Employees are responsible for ensuring that visitors understand and comply with USAID's camera use policy.

***565.3.7 Alteration of Security Systems or Locks**

Effective date: 09/24/2007

*Unauthorized modifications (i.e., propping open doors) or other action(s) without written consent from SEC which may adversely affect the operation of the USAID headquarters physical security measures/system will result in SEC recommending the Agency take appropriate disciplinary action against the responsible violator.

*Employees are not permitted to attach any device(s) or modify any aspect of USAID's access control system, including card readers, motion detectors or alarms. Bureau/Independent Offices are prohibited from securing the services of any security contractor to alter the Agency's access control system or install or alter any locks, even when part of a construction project. Written authorization from SEC must be obtained before any part of the USAID building, the building's security system, or any security locking device used for the protection of National Security Information is modified or disengaged.

*An asterisk indicates that the adjacent material is new or substantially revised.

***565.3.8 Safe and Door Combination Control**

Effective date: 09/24/2007

*SEC maintains a master listing of all USAID safe combinations and Unican door combinations. The Unit Security Officer (USO) in each Bureau/Independent Office will maintain a list of the security container (safe) combinations and Unican door combinations in a safe for his or her Bureau/Independent Office. The USO must ensure that no unauthorized person gains access to these combinations.

Only SEC personnel may change door and safe combinations, unless SEC grants an exception due to exigent circumstances. When an individual having knowledge of a safe combination changes employment with the respective Bureau/Independent Office, the USO must notify SEC and arrange to have the combination(s) changed.

*The USO must notify SEC immediately if a Bureau/Independent Office safe combination is **believed to have been** compromised. The reporting Bureau/Independent Office must provide relevant information concerning the incident to permit an investigation and, arrange to have the affected combination changed.

***565.3.9 Movement of Classified Equipment**

Effective date: 09/24/2007

*Secure equipment used to store or process classified information (e.g., safes and stand alone computers) must not be moved without prior notification to and approval from SEC. Secure communication equipment, e.g. (STU/STE) and ClassNet workstations may be moved only after proper coordination and approval from Bureau for management, Information Resources Management, Telecommunications and Systems Infrastructure (M/IRM/TSI).

***565.3.10 Property Passes**

Effective date: 09/24/2007

*Employees leaving USAID space with sealed packages, boxes, luggage or government equipment must provide the uniformed guard with a valid property pass signed by their designated AMS Officer or his/her designee. Employees/contractors removing personal property such as laptop computers, monitors, luggage, etc. that might appear to be government equipment must be able to prove ownership and be in possession of a properly completed USAID property pass.

USAID's contracted uniformed guards are required to review all property passes to ensure the following:

- *The pass was signed by an authorized individual,

*An asterisk indicates that the adjacent material is new or substantially revised.

- *The description of material/articles match the items being removed, and
- *The property pass is properly dated.

*The AMS Officer is responsible for designating individuals within the Bureau/ Independent Office with the authority to sign property passes. A signed designation must be sent to the Chief, SEC/PIDS/IDS and AMS Officers must update the designation as changes occur. SEC maintains a copy of the listing of approved individuals authorized to sign property passes at USAID's 13 ½ Street and 14th Street guard post.

***565.3.11 Fingerprints**

Effective date: 09/24/2007

*Employees or prospective employees requesting fingerprints for the purpose of a personnel security clearance or periodic reinvestigation may schedule an appointment directly with the B2 Badge Office. (Note: USAID's Badge Office will not fingerprint institutional contractors to support investigations by other federal agencies/departments.

***565.3.12 Deliveries to USAID/W**

Effective date: 09/24/2007

Uniformed guards assigned to USAID will inspect all deliveries, including courier mail and packages, parcels, bags, flowers, prior to allowing these items to be introduced into the USAID space. In unusual or emergency circumstances, SEC may impose temporary restrictions on hand-carried items to ensure that materials are not introduced into or removed from USAID space.

*All deliveries must be scheduled in advance through Bureau for Management, Administrative Services, Facilities Management Division (M/AS/FMD) for forwarding to the RRB loading dock for screening. Deliveries are not accepted at the general entrances to the Ronald Reagan Building.

***565.4 MANDATORY REFERENCES**

Effective date: 09/24/2007

***565.4.1 External Mandatory References**

Effective date: 09/24/2007

- a. [Department of Justice Vulnerability Assessment of Federal Facilities Report](#), issued June 28, 1995
- b. [Presidential Directive, Subject: Upgrading Security at Federal Facilities](#), issued June 28, 1995
- c. [41 CFR 101-20.103, Physical Protection and Building Security](#)

*An asterisk indicates that the adjacent material is new or substantially revised.

- d. [12 FAM 500, Information Security](#)
- *e. [Homeland Security Presidential Directive-12 \(HSPD-12\), August 27, 2004](#)
- *f. [Federal Information Processing Standards, Personal Identity Verification \(PIV\) of Federal Employees and Contractors \(FIPS 201\), March 2006](#)

***565.4.2 Internal Mandatory References**

Effective date: 09/24/2007

- *a. [ADS 562](#)

565.4.3 Mandatory Forms

Effective date: 09/24/2007

- a. [AID Form 500-1, Request for Federal Identification Card/Facility Access Card](#)

565.5 ADDITIONAL HELP

Effective date: 09/24/2007

***565.6 DEFINITIONS**

Effective date: 09/24/2007

***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 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.

*An asterisk indicates that the adjacent material is new or substantially revised.

(Chapters 545, 552, 562, 566, 567, 569)

***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. (Chapter 565)

***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 565)

***restricted space**

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

***unrestricted space**

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

565_092607_w100407_cd49