ADS Chapter 565

Domestic Security Programs

Partial Revision Date: 12/13/2017
Responsible Office: SEC/OD
File Name: 565_121317

Functional Series 500 - Management Services
ADS 565 – Domestic Security Programs
POC for ADS 565: Patrick (PJ) Butler, pbutler@usaid.gov

Table of Contents

ADS Chapter 565 – Domestic Security Programs

565.1 OVERVIEW

Effective Date: 12/13/2017

This chapter provides the policy directives and required procedures for the protection of USAID/Washington (USAID/W) workforce and national security information in USAID headquarters, buildings, and offsite facilities. This chapter applies to the entire USAID workforce, which for the purpose of this policy refers to individuals working for or on behalf of the Agency, regardless of hiring or contracting mechanism, who have physical and/or logical access to USAID facilities and information systems.

565.2 PRIMARY RESPONSIBILITIES

Effective Date: 12/13/2017

a. The **Director, Office of Security (D/SEC)** provides centralized security support to the Agency, with the exception of unclassified automated systems security. S/he supervises, directs, and controls all security activities relating to the programs and operations of USAID. S/he serves as the Agency's Senior Security Official and advises the Administrator and USAID senior staff on all security matters (see **ADS 101, Agency Programs and Functions** and **ADS 103, Delegations of Authority**).

b. The **Division Chief, Office of Security, International Security Programs (SEC/ISP)** implements physical security programs in USAID headquarters, buildings, offsite facilities, and overseas Missions.

c. The **Director of the Bureau for Management, Office of Management Services (M/MS)** ensures that SEC is apprised of future relocations of USAID personnel and assets and (in advance if possible) of any matters affecting the operations of physical security systems in USAID headquarters, buildings, and offsite facilities.

d. **USAID Senior SEC Managers**, **Division and Branch Chiefs** ensure staff compliance with the security policy directives and required procedures contained in this ADS chapter.

e. The **Office of Security, International Security Programs, Domestic Security Branch Chief (SEC/ISP/DS)** ensures staff compliance with the security policy directives, physical security programs, guard force, and required procedures contained in this ADS chapter and **Homeland Security Presidential Directive-12 (HSPD-12)**.

f. The Office of Security **AMS Officer** plays an integral role in ensuring workforce compliance with HSPD-12 for workforce within Office of Security. The AMS Officer, as the authorized sponsor within SEC, reviews all initial requests

submitted by personnel for a Federal Identification Card - Personal Identity Verification (PIV)/Facility Access Card (FAC). The AMS Officer also assures that departing employees are properly debriefed and return their PIV/FAC on their last day at the agency.

g. All individuals must comply with the security policy directives and required procedures contained in this ADS chapter.

565.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES

565.3.1 USAID Headquarters Building Security Standards

Effective Date: 04/16/2012

The physical security standards specified in this report apply to the USAID headquarters building (Ronald Reagan Building) and offsite locations (400 C. St. NW, Security Engineering Warehouse, Continuity of Operations (COOP) Site, Crystal Plaza Three (CP3), Washington Learning Center (WLC), Potomac Yards II, and all future work sites not yet named).

565.3.2 Designated Restricted, Unrestricted and Limited Access Areas

Effective Date: 12/13/2017

All office space within USAID/W headquarters and offsite facilities are designated as either “restricted” or “unrestricted” space. Further, spaces may also be designated as “limited access” based on mission. The Assistant Administrator (AA) or Office Director must request a change in designation from “restricted” or “unrestricted” for any office or office suite in writing to D/SEC. Subsequent approval or disapproval by Office of Security Counter Terrorism/Information Security (CTIS), or SEC/CTIS is based upon an inspection and evaluation of the space to determine and ensure full compliance with established standards. SEC/CTIS 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 ClassNet equipment. Restricted space also includes agency Sensitive Compartmented Information Facility (SCIF) areas, which are special access areas where Joint Worldwide Intelligence Communication Systems (JWICS) are stored.

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. Other personnel requesting access to designated restricted space must be escorted by a cleared, authorized employee who 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 receiving a written request from the individual's AMS Officer, SEC may grant access to unrestricted areas to any authorized individual(s) who has received a favorable background investigation as determined by SEC. Authorized individuals include:

- U.S. Direct-Hire employees,
- Personal Services Contractors (PSCs),
- Cleared (under reciprocity) Foreign Nationals for HSPD-12 access,
- Participating Agency Service Agreement (PASA) personnel, and
- Institutional Contractors.

All USAID overseas Missions are designated as unrestricted and are 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 and Offsite Facilities

565.3.3.1 Authorization to Work in USAID Headquarters and Offsite Facilities

Effective Date: 12/13/2017

Only those individuals who have been the subject of a background investigation and have received a favorable review by SEC are permitted to work within USAID space and be issued a USAID headquarters Personal Identity Verification (PIV) Card or Facility Access Card (FAC) to access USAID government space.

- Individuals with a current Secret, Top Secret, or Sensitive Compartmented Information (SCI) security clearance verified by SEC are authorized to work within USAID designated restricted areas. Individuals with an appropriate HSPD-12 background investigation verified by SEC are authorized to work within USAID designated unrestricted areas.
- Visitor passes (see **565.3.4**) must not be requested or used for people to work in USAID space unless pre-approved by authorized SEC personnel. Exceptions are granted on a case-by-case basis and must be approved by the Domestic Security Branch Chief, the International Security Programs (ISP) Division Chief, or designated staff acting on their behalf.

- SEC must specifically pre-approve unescorted access to work in unrestricted areas by individuals without a security clearance on a temporary basis. This includes unescorted access by USAID Cooperating Country Nationals (CCN) and Third Country Nationals (TCNs) on temporary duty (TDY) to USAID/W headquarters, and contractor employees working temporarily in USAID space. The Bureau/Independent Office (B/IO) AMS Officer must submit a request for such authorization to SEC/ISP/DS via an email to **SECDomestic@usaid.gov** at least one full week in advance of the proposed work date. A brief and concise security plan must specify what measures have been implemented to safeguard national security information from unauthorized access by an un-cleared individual. The request must include the following information:

  1. The purpose of the visit (training, etc.);

  2. The office and location where the visitor (CCN/TCN PSC or contractor employee) will be assigned;

  3. The identity of the USAID employee who will be the primary point of contact for administrative matters pertaining to the visitor;

  4. The dates of visit; and

  5. A statement that the visitor will not have access to any classified information or to restricted space.

  SEC will base approval on its assessment of the adequacy of the proposed measures.

- Once this cursory background check has been completed, the AMS Officer for the sponsoring Bureau must submit a **565-1 Badge Request Form** to SEC/ISP/DS via **enrollmentreviewer@usaid.gov**.

565.3.3.2 Obtaining a USAID Headquarters Federal ID/Personal Identity Verification (PIV) Card or Facility Access Card (FAC), and Reissuance of Credentials

Effective Date: 12/13/2017

Individual USAID Direct-Hires, Personal Service Contractors, employees of contractors and other government entities, including Congress, who require access for more than 10 days must be sponsored by a USAID B/IO to obtain a federal ID/PIV or FAC. The sponsoring B/IO 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 565-1, Request for Federal Identification Card/Facility Access Card** to the Enrollment Reviewer at **enrollmentreviewer@usaid.gov** for quality control review. The requesting B/IO AMS Officer is responsible for determining and specifying the access level required by the individual(s). After review, the Enrollment Reviewer will forward each 565-1 form to SEC/ISP/DS for approval.

Before individuals are granted unescorted access to government facilities, all requirements of **HSPD-12** must be met. These requirements are as follows:

- Favorable adjudication of clearance or background investigation;
- Sponsorship by AMS, HCTM, or other proper authority;
- Completion of in-person enrollment/identity proofing. An employee or contractor is issued a credential only after presenting two identity source documents to the Enrollment Office, at least one of which must be a valid federal or state government issued picture identification (see HSPD-12 and reference **Form I-9, Employment Eligibility Verification**, for a complete list of acceptable documents as proof of identification);
- Attendance at an appropriate SEC security briefing; and
- Authentication by the Badge Office.

Supporting documentation that must be submitted for each category of personnel is as follows:

For Direct-Hire/PSC personnel: The sponsoring B/IO AMS is not required to submit any additional forms, as all Direct-Hire/PSC personnel security information is maintained by SEC. The sponsoring B/IO AMS must provide documentation if the badge has been lost or stolen to **secbadges@usaid.gov**. If the change of information is the result of a name change, a standard form 50 must be provided to SEC/Investigations at **sclearances@usaid.gov** prior to requesting a new badge. Any documents including PII must be encrypted.

For Institutional Contractor employees: Institutional contractors on unclassified contracts are not required to submit security clearance documents. For institutional contractors on classified contracts, the sponsoring B/IO AMS must coordinate with the institutional contract company's Facility Security Officer (FSO) and comply with the HSPD-12 requirements to obtain a FAC or PIV for the contractor. The FSO must submit the required security clearance verification information on a Visit Authorization Request (VAR)/Visit Authorization Letter (VAL). The sponsoring B/IO AMS office will submit the company provided

VAR/VAL which must be encrypted and will include at a minimum:

- Individual's full name,
- DOB,
- SSN,
- Dates of Visit,
- Contract Company,
- Contract Number,
- Clearance Level,
- Investigation Type,
- Investigation Conducted by,
- Investigation Granted Date, and
- Signature and Date of the FSO.

Please note: The VAR/VAL is only valid for 30 days.

For PASA personnel: The sponsoring B/IO AMS must coordinate with PASA personnel's originating agency's Facility Security Officer (FSO) and obtain an **AID Form 565-2** in order to comply with the HSPD-12 requirements to provide security clearance verification.

For Cooperating Country National (CCN) or Third Country National (TCN) personnel: The sponsoring B/IO AMS must coordinate with the originating country's Regional Security Officer (RSO) and must provide:

1. A RSO verification letter/certificate that, at a minimum, includes the following information:
    - Individual's full name,
    - DOB,
    - Clearance level (HSPD-12), and
    - Signature and date of the RSO.

Note: The verification letter or certificate must be dated within the last 30 days. If the RSO certification letter is older than 30 days, an email statement from the RSO must state that the verification is still valid. All documents containing PII must be encrypted.

2. A TDY Notification Letter that at a minimum includes the following information:

- Individual's full name,
- Bureau of Sponsorship, and
- Dates of Visit.

Pursuant to HSPD-12 policies, a cardholder must be allowed to apply for a renewal starting six weeks prior to the expiration of a valid PIV/FAC card and until the actual expiration of the card. The expired PIV/FAC card must be returned to SEC/ISP/DS for proper deactivation and destruction.

A cardholder must apply for reissuance of a new PIV card through their AMS Officer if the old PIV card has been compromised, lost, stolen, or damaged. The cardholder can also apply for reissuance of a valid PIV card in the event of an employee status or attribute change.

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

Personnel who are posted abroad whose PIV/FAC card is within three months of expiration and plan to be in the Washington, DC area either during home leave or TDY should notify their AMS Officer to arrange for a badge renewal while in the DC area. The Domestic Security Branch will accommodate individuals in this category (see **565.3.3.3**).

565.3.3.3 Use of USAID Headquarters Federal ID/Personal Identity Verification (PIV) Card or Facility Access Card (FAC)

Effective Date: 04/16/2012

All individuals within USAID headquarters and offsite locations must possess and wear a valid USAID federal ID/Personal Identity Verification (PIV) card, Facility Access Card (FAC), or visitor pass at all times, regardless of employment type.

- All individuals must wear the federal ID/PIV card or FAC on the outer garment on the upper torso front with the front of the pass clearly visible.
- The federal ID/PIV card or FAC must not be altered (e.g., affixed with stickers, pins, or other items) in any way.

- All individuals are prohibited from lending building passes or ID cards to other employees or visitors.

- Federal ID cards must be used only for official business purposes.

- All individuals must conceal their card after departing USAID headquarters and offsite facilities.

- SEC will make exceptions to the mandatory pass rule for children under the age of 17 and those visitors attending functions whose range of movement is severely limited.

565.3.3.4 Access to Offices and Suites within USAID Headquarters, Ronald Reagan Building, and USAID Washington Facilities

Effective Date: 05/24/2012

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

The sponsoring B/IO AMS Officer must submit requests for access to office space within USAID/W to the SEC Badges mailbox: **SECDomestic@usaid.gov**. All requests must include the following:

- The individual's name,

- Door or suite number requested,

- Time of day requested (shift name), and

- The purpose of access.

Requests for access to another B/IO 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 completed.

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 7:00 p.m., five days a week, no holidays or weekends;

- Core = 8:45 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 Badges

Effective Date: 12/13/2017

Overseas Direct-Hire employees with at least Secret level security clearance on temporary duty assignment (TDY) in USAID/W may obtain a TDY badge at the 14th Street Visitor Control Desk while they await approval of permanent badge application. After verification of the individual's identity, employment status, clearance level, and sponsoring B/IO, a TDY badge will be issued for the duration of the TDY assignment.

Employees on TDY assigned to 400 C. St. NW, 2PY, CP3 or WLC are required to have their respective AMS Officer notify the Security Officer at 400 C. St. NW or 2PY 14 days prior to the employee's arrival to arrange for the issuance of a temporary badge.

CCN/TCN PSCs and USPSCs without at least a Secret level clearance must show their embassy-issued identification card at the 14th Street Visitor's Desk before being issued an un-cleared TDY badge. Foreign visitors as well as any non U.S. citizen members of the USAID workforce must have a business visa; a tourist visa will not suffice.

To expedite the verification process, the sponsoring office (normally the B/IO AMS Officer) must send an email to the Office of Security mailbox (**SECDomestic@usaid.gov**), which includes the following:

- The individual's full name,
- Start and end dates of the TDY,
- Mission location,
- Clearance level, and
- The sponsor's contact information.

TDY badges will enable individuals to proceed unescorted through the turnstiles at the 13 ½ and 14th Street lobbies into USAID space. The pass also permits the

individual 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 **565.3.3.6**. Requests to add access to a TDY badge must also include the TDY badge number (located on the front of the card).

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

The B/IO AMS Officer should request a permanent photo building pass for any employee scheduled for TDY in USAID/W for more than 10 working days. Such requests must be submitted on an **AID 565-1 form** following the procedures in **565.3.3.2**.

Any individual who is assigned to USAID/W or any of the offsite facilities for more than 30 days must obtain an HSPD-12 issued badge.

565.3.3.6 Temporary Badges

Effective Date: 12/13/2017

Individuals required to have access to USAID/W facilities who report to work without their authorized federal ID card/FAC must request a temporary badge (T-Badge). Uniformed guards are required to verify the identity of the individual before issuing the temporary badge. Temporary badges are not issued to any individual with an expired federal ID card. Unless special authorization is approved by SEC, a temporary badge will be issued for a period of one day.

Individuals required to have access to the Ronald Reagan Building must request a T-Badge from the 14th Street Visitor Control Desk.

Individuals required to have access to 400 C. St. NW must request a temporary badge from the Federal Emergency Management Agency access control desk, located at the 400 C Street lobby, upon approval by the USAID Security Officer.

Individuals required to have access to Potomac Yards II must report to the Front Desk Security Officer at Potomac Yards II to request a T-Badge. The individual will be required to contact a member of the USAID workforce to serve as an escort. The uniformed guard is required to verify the identity of the individual before issuing a temporary badge. The individual's regular federal ID card/FAC will be deactivated until the temporary badge is returned to the 14th Street Visitor Control Desk. Individuals are prohibited from using multiple badges simultaneously (i.e., temporary or TDY badge and photo HSPD-12 ID).

Temporary badges are not intended for any hiring mechanism waiting for approval of clearance, contract extension, or completion of pre-employment requirements. On a case-by-case basis, SEC/ISP/DS will consider special circumstances for access to designated for unrestricted space. The B/IO AMS

Officer must submit a request for such authorization to SEC/ISP/DS via an emailed memo to **SECDomestic@usaid.gov** at least one week in advance. The memo must contain a brief explanation of circumstances, a point of contact, and desired work location. The Domestic Security Branch Chief or appointed representative will not grant approvals for access of more than 10 working days.

565.3.3.7 Procedures for Distinguished Visitor Visits

Effective Date: 12/13/2017

USAID employees who expect to receive Distinguished Visitor (DV) visits by heads of state/government, reigning royalty, or cabinet-level guests must submit the following information to the respective SEC and LPA email mailboxes noted below at least 72 hours prior to the visit to ensure compliance with protocols regarding processing and access. The USAID employee sponsoring the visit must send an email to **SECDV@usaid.gov** and **SpecialEvents@usaid.gov** and include the following information:

- Identity of the designated escort officer and their contact information (limit three visitors per escort officer);
- Sponsoring Bureau or Office, telephone number, and the name(s) and title(s) of each member of the DV delegation (including prefix, full name, and title);
- Prefixes, names, and titles of any other accompanying U.S. Government personnel; and
- Date, time, and meeting room.

The individual sponsoring the visit must inform the DV that U.S. citizens on official diplomatic business must present an un-expired official government passport and business visa at sign-in to the RRB front desk. Access will be denied if the visitor fails to provide an official government passport with a business visa. The only acceptable visa is a business visa (tourist visa is not acceptable).

On the day of the visit, the employee who will serve as the escort must re-confirm two hours prior to the visit to **SpecialEvents@usaid.gov**. A DV escort badge will be subsequently issued to the escort, who must sign out the badge at the 14th Street Visitor Control Desk, after confirmation has been received from **SECDV@usaid.gov** and **SpecialEvents@usaid.gov**.

LPA will determine if the visitors fall within the accepted categories for DV protocol. LPA handles logistics (flags, photos, gifts, escorts, internal press coverage, etc.), as appropriate to the rank of the guest. DVs and guests of the Administrator will be afforded expedited sign-in and security screening, provided that guests are pre-registered in the Visitor Registration System (VRS) and

notification of the DV visit is received a minimum of 72 hours in advance. Foreign visitors must present a passport and U.S. citizens must present a valid (un-expired) government issued ID card (such as a passport or driver's license).

SEC will determine what visitors, if any, will be granted an exception to bypass security. All visitors to USAID will present proper identification and be screened with the exception of the following:

- Presidents, Prime Ministers, or Heads of State;
- DVs who rate an armed protection detail (Secret Service, State Department Diplomatic Security Service or other federal agency);
- Sworn law enforcement officers; or
- Other special circumstances approved by SEC on a case-by-case basis.

When a security screening exception is granted, the principal, any authorized armed security detail personnel, and federal HSPD-12 ID card holders will not be screened. All other personnel in their party will be signed in at the registration desk and screened.

Security screening is independent of DV level or protocol status. A visitor may be extended protocol for DV level 2 or 3 by LPA as a guest of the Administrator, and the visitor and delegation will be screened for the safety and security of the Administrator and the Agency. Additional exceptions to security screening must be approved by D/SEC, the Administrator, or the Deputy Administrator. LPA personnel may sign for elevator keys in order to facilitate holding an elevator for DV, if needed.

565.3.3.8 Replacement of Federal Identification PIV/FAC Badges

Effective Date: 12/13/2017

Individuals must immediately report any lost, compromised, or possibly stolen federal PIV or FAC badge to their AMS Officer, or immediate supervisor, and the SEC Main Desk at (202) 712-0990. The individual may request a replacement badge by completing the **AID 565-1 form**. The AMS Officer must submit the **AID 565-1 form** electronically to the SEC Badges mailbox (**SECDomestic@usaid.gov**). Individuals must wait a minimum of five working days for authorization for a replacement badge. SEC will issue a temporary badge in the interim.

Individuals must submit a written statement to their AMS Officer and immediate supervisor detailing the facts and circumstances of the loss, theft, or compromise, including all actions taken to recover the badge. The individual and their immediate supervisor must sign the written statement. This statement must

be attached to the **AID 565-1 form** when submitted to the SEC Badges mailbox for lost badge replacement.

Individuals requesting replacement due to physical damage or a malfunctioning federal PIV or FAC badge are subject to all requirements for enrollment, identity proofing, and authentication under the **HSPD-12** program.

565.3.3.9 Required Verification of Federal ID (PIV) Card/Facility Access Card (FAC)

Effective Date: 04/16/2012

Uniformed guards are required to positively identify individuals with badges 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 access suspended until a replacement PIV/FAC badge is obtained.

565.3.3.10 Return of Federal ID (PIV) Card/Facility Access Card (FAC)

Effective Date: 12/13/2017

An employee must return their federal ID PIV card or FAC at the end of the day when:

- An employee who leaves the agency or contractor whose performance period, access, or contract has ended; 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 federally issued ID cards must be returned to SEC prior to an employee's departure, regardless of hiring mechanism or whether the employee resigns, completes a detail, is terminated, or when access to USAID facilities has been revoked or is no longer needed.

- **U.S. Direct-Hires and PSCs**: Must return their identification cards to SEC during the mandatory security debriefing and employee "check out" procedures (see **ADS 568, National Security Information Program**).
- **Uncleared institutional contractors and detailees**: The Agency sponsor (B/IO AMS Officer) is responsible for collecting the identification cards from these individuals at the conclusion of the contract or detail.
- **Cleared institutional contractors**: The Contracting Officer's Representative (COR) is responsible for ensuring that the FSO for the

parent company returns 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.

USAID badges may be returned via mail to:

USAID/SEC/ISP/DS
RRB Room B. 2.6-32A
1300 Pennsylvania Avenue, N.W.
Washington, DC 20523

565.3.3.11 Confiscating Invalid Federal ID Cards

Effective Date: 04/16/2012

The security guards posted at USAID/W facilities will confiscate any expired or invalid federal ID card/FAC. Individuals requiring access to these facilities whose badge has been confiscated must notify the USAID Security Badge Office to report the circumstances. These individuals may request the issuance of a T-Badge. The B/IO AMS Officer must complete a new **AID 565-1** to request re-issuance of a new card.

Security officers at the Ronald Reagan Building USAID turnstiles and at 400 C. St. NW are authorized to confiscate any expired federal ID card/FAC. The security officers at 2PY are authorized to confiscate any expired federal ID Card/FAC and will return the card to USAID SEC.

565.3.3.12 Random Security Screening

Effective Date: 12/13/2017

The security guards posted at USAID/W facilities will conduct random security screenings of USAID employees and visitors in the interest of public safety. Each randomly selected employee will be required to process through existing security screening to be checked for prohibited and/or illegal items. An employee's failure to cooperate will result in denial of entry into the facility. Employees who attempt to access federal facilities after access has been denied are subject to arrest or apprehension for unlawful entry. Prohibited items include:

- Guns and firearms;
- Bladed, edged, or sharp objects;
- Club-like items and striking devices;
- Explosives;
- Incendiaries; and

- Disabling chemicals or other dangerous items.

565.3.3.13 Unprofessional Behavior in USAID Space
Effective Date: 12/13/2017

Federal Protective Service (FPS) has law enforcement jurisdiction at the Ronald Reagan Building and other Washington area facilities. Local law enforcement agencies may respond as necessary.

Employees who exhibit unprofessional behavior towards USAID security officers will be reported to the Office of Security and may be provided with verbal or written warnings, referred to law enforcement, or may be instructed to leave the facilities. Failure to comply with orders, unlawful entry, as well as aggressive, threatening or violent actions towards USAID security officers will be immediately referred to the respective site federal law enforcement officers. USAID staff and visitors are charged with following U.S. Code Title 41 CFR 101-20.302 and 41 CFR 101-20.305, which prohibits unlawful entry or disturbances on federal property. Staff may face further administrative disciplinary action depending on the frequency or severity of the offense(s).

565.3.4 Visitors and Guests to USAID/W
Effective Date: 12/13/2017

USAID employees who expect to receive visitors at USAID/W are required to register their sponsorship of the visitor at the USAID Security Desk. Procedures for Distinguished Visitor visits are noted in **565.3.3.7**. Employees can access the system via AIDNET by clicking the Visitor Registration System icon and accessing the system. When a visitor checks in at the USAID Front Desk and furnishes a valid, government-issued photo identification (driver's license, U.S. Government-issued ID card, U.S. passport, State Department ID), a personalized visitor's pass will be issued to the visitor. The pass will note the visitor's name, date of visit, and the sponsor's name. The USAID sponsor will be automatically notified of the visitor's arrival by email and also receive telephonic notification to provide an escort.

Non-U.S. citizens must be pre-registered at least five days in advance in order to process the request. They must furnish a valid foreign passport upon arrival when checking in.

USAID employees at 400 C. St. NW may notify the 400 C. St. NW security officer of visitors and provide their names in advance to facilitate their access. This information will be subsequently forwarded to FEMA and the front desk to facilitate the process. Employees expecting to receive groups of five or more visitors are required to notify the 400 C. St. NW USAID security officer at least two days in advance to allow sufficient time to process their screening access.

All visitors and guests must present valid (un-expired) identification before they

may enter USAID space in the Ronald Reagan Building or any USAID offsite facility.

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 un-cleared 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 B/IO authorizing the work must arrange for an escort and obtain SEC concurrence. These individuals must:

- Sign in and out on the appropriate register designated by SEC,
- Wear a visitor's pass for the duration of the visit,
- Surrender the visitor's pass at the 14th Street Visitor Control Desk when leaving USAID space for the day at the Ronald Reagan Building, and
- Surrender visitor's pass at the Front Visitor's Desk when leaving USAID space for the day at 400 C. St. NW.

The B/IO 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 for the duration of their visit, with the exception of visits to common area restrooms.

Employees who fail to comply with escort procedures and policy will be cited for each violation. When an employee is cited three times for not following the established escort procedures and policy, SEC will revoke their escort privileges. The employee will be required to surrender their current badge annotated with the "E" designation on the front of the badge, and they will then be reissued a replacement badge with no escort privileges. Violations of a security regulation may lead to disciplinary and adverse actions under **ADS Chapter 487, Disciplinary and Adverse Actions Based upon Employee Misconduct – Civil Service** and **ADS Chapter 485, Disciplinary Action – Foreign Service**.

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

Effective Date: 12/13/2017

Access to domestic Department of State facilities may be added to federal ID cards or FACs. SEC only sponsors access to Main State (HST Building) on federal ID cards for Direct-Hire employees and PSCs. The employee or B/IO AMS Officer must send all other requests for access to state facilities directly to the Department of State sponsor or Unit Security Officer.

565.3.6 Use of Cameras, Photographic or Video Teleconferencing Equipment, Personal Digital Assistants (PDAs), Smartphones, Tablets, Wireless Radio-Frequency (RF), Recording Devices and Bluetooth Devices

Effective Date: 12/13/2017

The use of cameras, recording devices, or photographic equipment is not permitted within restricted space in the USAID portion of the Ronald Reagan Building and offsite facilities. 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 Badge Office mailbox (**SECDomestic@usaid.gov**) 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 48 hours before the planned event. LPA will notify SEC when the request has been approved.

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 or record 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, Counterintelligence and Information 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 use 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.

The transport and/or use of cameras, recording devices, personal digital assistants (PDAs), tablets, smartphones, and any other type of camera are prohibited in Sensitive Compartmented Information Facility (SCIF) areas. The use of Bluetooth devices within USAID facilities is also prohibited.

565.3.7 Alteration of Security Systems or Locks

Effective Date: 04/16/2012

Unauthorized modifications (i.e., propping open doors) or other action(s) without written consent from SEC, which may adversely affect the operation of the physical security measures/system at USAID headquarters and offsite facilities, 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. B/IOs 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 a building's security system, or any security locking device used for the protection of National Security Information, is modified or

disengaged.

565.3.8 Door Combination Control
Effective Date: 04/16/2012

SEC maintains a master listing of all USAID and Unican door combinations. The AMS Officer in each B/IO will maintain a list of the Unican door combinations in a safe for their B/IO. The AMS Officer must ensure that no unauthorized person gains access to these combinations.

Only authorized SEC personnel may change door combinations, unless SEC grants an exception due to exigent circumstances. When an individual having knowledge of a door combination changes employment with the respective B/IO, the AMS Officer must notify SEC and arrange to have the combination(s) changed.

The AMS Officer must notify SEC immediately if a B/IO safe combination is believed to have been compromised. The reporting B/IO must provide relevant information concerning the incident to permit an investigation and arrange to have the affected combination changed.

565.3.9 Fingerprints
Effective Date: 12/13/2017

Employees or prospective employees requesting fingerprints for the purpose of a personnel security clearance may request to schedule an appointment by submitting a request directly to the **SECDomestic@usaid.gov** mailbox. The employee must specify the reason why the fingerprints are needed and indicate if s/he has initiated the process required for completing the e-QIP (Electronic Questionnaire for Investigations Processing). Fingerprints are done only for selective hiring mechanisms that require a clearance or HSPD-12 access investigation by the USAID Personnel Security Division. Employees must be able to furnish a valid government-issued photo identification card (state-issued driver's license or U.S. Passport) in order to be fingerprinted. Fingerprinting appointments are scheduled Monday through Friday according to the availability of the fingerprinting specialist.

USAID's Badge Office will not fingerprint institutional contractors on classified contracts to support investigations by other federal agencies/departments.

565.3.10 Deliveries to USAID/W Facilities
Effective Date: 12/13/2017

Uniformed guards at all USAID/W buildings will not accept any packages under any circumstances.

All deliveries to the loading docks at the Ronald Reagan Building and USAID/W

facilities must be scheduled in advance through the Bureau for Management, Office of Management Services, Headquarters Management Division (M/MS/HMD) to arrange for mandatory screening upon arrival at the building's loading dock. Deliveries are not accepted at the general entrances.

565.4 MANDATORY REFERENCES

565.4.1 External Mandatory References

Effective Date: 04/16/2012

a. 12 FAM 500, Information Security

b. 12 FAM 683, Personal Digital Assistants

c. 41 CFR 101-20.103, Physical Protection and Building Security

d. Federal Information Processing Standards, Personal Identity Verification (PIV) of Federal Employees and Contractors (FIPS PUB 201-2), August 2013

e. Form I-9, Employment Eligibility Verification

f. Homeland Security Presidential Directive-12 (HSPD-12), August 27, 2004

g. Interagency Security Committee Standard: Physical Security Criteria for Federal Facilities, April 12, 2010

h. Interagency Security Committee: Use of Physical Security Performance Measures, 2009

565.4.2 Internal Mandatory References

Effective Date: 04/16/2012

a. ADS 101, Agency Programs and Functions

b. ADS 103, Delegations of Authority

c. ADS 545, Information Systems Security

d. ADS 552, Cyber Security for National Security Information (NSI) Systems

e. ADS 561, Security Responsibilities

f. ADS 566, Personnel Security Investigations and Clearances

g. **ADS 568, National Security Information Program**

565.4.3 Mandatory Forms
Effective Date: 04/16/2012

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

565.5 ADDITIONAL HELP
Effective Date: 12/13/2017

There are no Additional Help documents for this chapter.

565.6 DEFINITIONS
Effective Date: 12/13/2017

See the **ADS Glossary** for all ADS terms and definitions.

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.

Information that has been determined pursuant to Executive Order (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.

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**, **565** and **568**)

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**)

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**)

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

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

565_022019