

12 FAM 440 POST SECURITY FUNCTIONS

*(CT:DS-123; 12-13-2006)
(Office of Origin: DS/MGT/PPD)*

12 FAM 441 FACILITY ACCESS

12 FAM 441.1 Identification Cards

(CT:DS-123; 12-13-2006)

- a. Post personnel must be assigned a post identification (ID) card. The regional security officer (RSO) may approve the issuance of post ID cards to other personnel, as appropriate.
- b. All personnel at Foreign Service missions, annexes, and facilities that have public access control points staffed by Marine security guards (MSGs) or other security personnel must present identification cards to gain access to the facility. All individuals must wear identification cards in plain view at all times while inside a facility.
- c. Posts with automated access control systems (AACs) must comply with AACs standards found in 12 FAH-6 H-538.
- d. Temporary identification, such as visitor stickers, identification cards, or badges, will be issued to all visitors prior to entering the general work area (GWA) or controlled access area (CAA) of any Foreign Service mission, annex, or facility. Visitors must wear this temporary identification in plain view at all times while in the facility. Admitting offices must escort those visitors who do not have appropriate security clearances. (See 12 FAM 445.1 for handling exceptions.)
- e. Posts must establish and implement measures to safeguard identification cards, badges, passes, and other identification media. (See 12 FAM 445.2 and 12 FAH-6 H-538.5-3.d. for safeguards.)
- f. *Post ID cards must be compliant with Federal Information Processing Standards Publication (FIPS PUB) 201 standards and associated Special Publications.*

12 FAM 441.2 After-Hours Access to Chancery and Consulate Buildings

(CT:DS-123; 12-13-2006)

- a. In addition to showing proper identification, all employees must sign a register when entering or leaving a chancery or consulate building outside of regular working hours.
- b. Uncleared personnel, including Foreign Service nationals (FSNs), third-country nationals (TCNs), U.S. citizens, contractors, and interns, may work after hours in chancery or consulate general work areas (GWAs) and public access areas (PAAs) when the cleared U.S. supervisor authorizes the work and obtains written approval from the regional or post security officer (RSO or PSO).
- c. Uncleared authorized personnel entering and/or remaining in the chancery or consulate must be escorted in accordance with 12 FAH-6 H-311.8 *and* H-314.8.

12 FAM 442 MEMBERS OF HOUSEHOLD

(CT:DS-123; 12-13-2006)

(State)

(Applies to Foreign Service Employees)

- a. 3 FAM 4180 defines members of household ("MOHs") as persons who have accompanied or join a State Department employee assigned abroad and who the employee has declared to the Chief of Mission (COM) are part of his or her household, who will reside at post with the employee, and who are other than legitimate domestic staff. MOHs do not include those persons who are "family members" or "eligible family members (EFM)."
- b. When an employee declares a person as an MOH to the COM, the employee must provide such biographic data to the regional security officer (RSO) on the MOH as may be necessary to conduct appropriate investigative activities. In the case of U.S. citizens, this will be data sufficient for conducting a National Agency Check and, if an expatriate, appropriate records checks with the host government. If a non-U.S. citizen, a background investigation commensurate with that accorded to locally engaged staff will be conducted. Should unfavorable information be developed as a result of investigative activities, the RSO must inform the Chief of Mission immediately and recommend further steps based upon these findings. MOHs are not exempt from 12 FAH-6, Employee and Visitor Access Restrictions. If results of records checks or other investigative actions are favorable, the post may issue photo identification that permits access to post facilities for MOHs to attend activities, events, and programs open to EFMs as described in 3 FAM 4180. Unescorted access to residential compounds is also permissible.
- c. Employees should encourage their MOHs to attend unclassified security

briefings at post.

- d. RSOs should inform employees that security criteria outlined in [3 FAM 4180](#) and personnel considerations that may be pertinent under [3 FAM 2440](#) (COM authority for involuntary curtailment) may also have applicability regarding an employee's relationship with an MOH.

12 FAM 443 SECURITY CLEARANCES

12 FAM 443.1 Personnel Assigned on Permanent Change of Station (PCS) Orders or Locally Hired

(CT:DS-123; 12-13-2006)

- a. Except as provided in paragraph e *below*, all U.S. citizen-U.S. Government employees either assigned through permanent change of station (PCS) or locally hired must hold a Top Secret clearance issued by their parent agency if they:
 - (1) Work within a controlled access area; or
 - (2) Require unescorted access to a controlled access area.

The Top Secret clearance must be based upon a Single Scope Background Investigation (SSBI) that meets the requirements of Standard B of the Investigative Standards for Background Investigations for Access to Classified Information as promulgated by the Assistant to the President for National Security Affairs or, in the case of temporary access at the Top Secret level, the Investigative Standards for Temporary Eligibility for Access.

- b. All U.S. citizen-U.S. Government employees not working within a controlled access area nor requiring unescorted access to a controlled access area must possess a security clearance appropriate for the level of classified material to which they have access. They must also have been the subject of an investigation appropriate for the sensitivity of the position they are occupying and the area to which they are assigned.
- c. The regional security officer (RSO) or post security officer (PSO) serves as the central repository at post for clearance data.
- d. It is the responsibility of the individual agencies represented at post to provide clearance data on their PCS personnel to the RSO or PSO. The options for providing this data are:
 - (1) The agency representative provides the data to the RSO or PSO;
 - (2) The agency headquarters provides the data to the RSO or PSO by official communiqué; or

- (3) The agency headquarters provides the data to the Department, Bureau of Diplomatic Security, Office of Personnel Security and Suitability (DS/SI/PSS), for transmission to post.
- e. For all new construction or major renovations involving controlled access areas, security clearance requirements are specified in 12 FAH-6 sections H-311.14, H-312.14, H-313.14, and H-314.14.

12 FAM 443.2 Temporary Duty Personnel

(CT:DS-103; 09-16-2004)

- a. All agencies that initiate travel messages and travel authorizations for the temporary duty (TDY) assignment of their personnel (both employees and contractors) to a mission abroad, must include in the travel message and in the travel authorization the level of security clearance. In cases of TDY travel from one mission to another mission abroad, the sending post is responsible for providing verification of the security clearance level.
- b. Temporary duty personnel for whom clearance has not been provided to the post will not be given unescorted access to U.S. Government facilities or access to classified or controlled information. Address requests for security clearance verification to DS/SI/PSS with an information copy to the regional bureau and, in the case of other agency personnel, to the appropriate agency.
- c. The RSO serves as the control officer for the visits of short-term (TDY) personnel on various security-related matters, e.g., emergency security support teams (see 12 FAM 444). Except in countries that are clearly on record as rejecting the accreditation of personnel assigned TDY for short periods or where attempted notification could cause other complications, the RSO will request that the chief of mission or principal officer notify the host country's foreign ministry of the impending visit of all security-related TDY visitors and request temporary accreditation for the duration of the visit.

12 FAM 444 EMERGENCY SECURITY SUPPORT

12 FAM 444.1 Policy

(CT:DS-103; 09-16-2004)

DS provides rapid operational response in emergency situations where specially trained teams of DS officers are required to supplement available overseas post or domestic office resources. Most often the team deployment will be in response to either a terrorist incident, or to an immediate threat of terrorist or criminal activity. The team may also be activated for natural

disasters and other unusual events.

12 FAM 444.2 Implementation

(CT:DS-103; 09-16-2004)

- a. DS/DSS/IP/RD determines the scope and work priorities of all emergency support missions. The Office of Mobile Security Deployment (DS/T/MSD) is the DS office that provides support to posts for emergency situations and provides training to U.S. Government personnel and dependents at posts abroad.
- b. DS/T/MSD dispatches personnel and equipment quickly. To minimize the drain on post resources, the team will be as self-sufficient as possible. Posts are to arrange, to the extent possible, airport visas for team members and unimpeded entry and transportation of equipment to the mission. The team and equipment should be en route to a post within 24 hours of a decision to deploy.

12 FAM 445 IDENTIFICATION MEDIA EXCEPTIONS AND SAFEGUARDS

12 FAM 445.1 Exception to Required Identification

(CT:DS-103; 09-16-2004)

- a. There are certain areas of Department missions, annexes, and facilities where implementing this mandatory policy would inhibit operational effectiveness. Information resource centers (IRCs) and publicly accessible libraries maintained by Public Affairs Offices, and portions of the consular sections are examples of these areas. In these specific instances the regional or post security officer, in coordination with the chief of mission, decides which areas are exempt from this policy. This policy is primarily to enhance the post's security posture, and posts should carefully weigh this in determining whether to make an exception for a specific area or section.
- b. In the event a post determines an exception to this policy is required, for a specific area or section, the post security officer must provide a detailed explanation to the Assistant Director for International Programs (DS/DSS/IP). The PSO report must indicate the specific exception and the reason behind the exception.

12 FAM 445.2 Safeguards

(CT:DS-103; 09-16-2004)

- a. Use a security container with an S&G security padlock to secure blank cards, badges, and passes. Only personnel responsible for managing the program are allowed access to this container.
- b. Post security must account for all cards, badges, and passes by serial number.
- c. A card, badge, or pass log must reflect the name, office, status (level of clearance), and expiration date for each card, badge, or pass issued. The log is a permanent part of the regional or post security office files.
- d. The issuing officer must issue written instructions with each card, badge, or pass issued. The instruction must address the proper use and safeguarding of the identification media, specifically stressing the security precautions concerning the wearing of the identification media outside of the facility.
- e. Involved employees must report the circumstances surrounding lost or stolen cards, badges, or passes to the regional or post security officer who will record the circumstances.

12 FAM 446 UNCLASSIFIED OFFICE FACILITY LOCK AND LEAVE (L&L) POLICY

12 FAM 446.1 Policy

(CT:DS-123; 12-13-2006)

- a. This L&L policy supplements 12 FAH-5, Physical Security Handbook, and 12 FAH-6, OSPB Security Standards and Policy Handbook, and addresses the minimum requirements and procedures for securing *U.S. diplomatic facilities* (including commercial office space) *against the crime threat where no classified material is stored, discussed, or processed and without 24-hour presence inside the building*. Risk management may dictate technical and physical security enhancements beyond the minimum requirements.
- b. *The L&L policy provides protection to unclassified office facilities based on high-value assets and risk management as determined by the parent agency and agreed to by the regional security officer (RSO). High-value assets are defined as items whose compromise or loss will severely impact post operations (personnel or payroll data, safes containing funds, etc.)*
- c. *At posts where U.S. Marines or other cleared U.S. presence are able to respond on a 24-hour basis to any alarmed condition or incident outside the main chancery, but on the post compound, buildings on the post*

compound with high-value assets are not considered L&L facilities within the context of this policy.

- d. Classified facility L&L standards are addressed in 12 FAH-6 H-910.*
- e. The DS Lock and Leave Application Guidelines for L&L Facilities, which are available separately by DS/C/ST, will prescribe the methodologies and equipment used to implement this policy.*

12 FAM 446.2 Designation of Unclassified Lock and Leave Office Facilities

(CT:DS-123; 12-13-2006)

- a. Upon completion of new construction or major renovation, accreditation and commissioning process of unclassified new office buildings (NOBs) and newly acquired buildings (NABs) designated by the parent agency to possess high-value assets, DS and OBO will issue a notice of substantial compliance and certification of occupancy to officially designate the new facility as an unclassified L&L office facility.
- b. Existing unclassified L&L office facilities with high-value assets, as determined by the parent agency and agreed to by the RSO, will require an initial inspection by the servicing ESC/ESO. A report of the inspection will be provided to DS/PSP/PSD and DS/ST/OSB for approval. Existing unclassified L&L office facilities with major security issues will require a team survey to identify security deficiencies and solutions in accordance with paragraphs d, e, and f below.*
- c. Prior to a new unclassified office facility achieving L&L status, a team survey of the site must be performed in accordance with paragraphs d, e, and f below and survey recommendations implemented.*
- d. The survey team will be composed of at least one member each from DS/PSP/PSD, DS/ST/FSE, the servicing ESC/ESO, OBO, and tenant agencies, as applicable. The team will work in close cooperation with post management and the RSO/PSO.*
- e. The survey report represents the risk managed security solutions required to provide an acceptable level of protection for the high-value assets. As such, it should detail the underlying basis for recommended security improvements and, to retain value over time, document any assumptions made by the authors regarding risk managed decisions. Therefore, the survey report will include, at a minimum, the following information:*
 - (1) A compilation of *general* post information *and specifications*;
 - (2) Site information pertinent to the decision process; (e.g., location of local police stations; *list of neighboring structures*; history of *security* incidents; political significance of site; building setback

from surrounding roads; perimeter structures; and existing security measures);

NOTE: *Risk decision factors (e.g., are historical security incidents representative of the future or is change likely; a list of security incident scenarios considered during the survey; team judgments on the relative likelihood of those scenarios occurring; assumptions made, and recommendations, if any, on what assumptions may change and warrant future monitoring).*

- (3) Detailed description of the building's structural limitations and composition, with emphasis on exterior walls, doors, and windows;
- (4) Floor layout drawings, including areas of special interest (e.g., proposed L&L and bypass door locations; public access control (PAC) location; systems interface cabinet (SIC) room; proposed technical equipment layout; description of typical personnel traffic flow; *description of probable paths, routes, and entry locations of intruders*; and applicable high-value item locations, etc.);
- (5) List of *technical and physical security hardware* required to bring the building into compliance with the L&L policy;
- (6) Full description of the proposed L&L door and bypass door (i.e., type, existing hardware, swing, etc.) as defined in *12 FAM-5, Appendix G*;
- (7) *If the survey team determines that digital video recorder (DVR) and closed circuit television (CCTV) coverage is required, then CCTV coverage and DVR recording will include all normal points of entry or exit to the area protecting the high-value items, the L&L perimeter door, the exterior of the bypass door, and any other points of entry or exit likely (realistically) to be used by an intruder to gain access to the high-value items. Additionally, DVR equipment will be installed in the Security Interface Cabinet (SIC) room and powered by an uninterruptible power supply (UPS). The required duration of backup supplied by the UPS should consider factors relevant to the likely security incidents and the availability/reliability of local power, whether or not a backup generator is in use at the facility. Any additional CCTV coverage recommended by the team should be supported by narration explaining the purpose of the camera view and the necessity, if any, of recording the view.*
- (8) Post-specific alarm response procedures (e.g., post personnel, guards, *local* police, 24-hour remote monitoring, etc.);
- (9) *Post L&L operation management plan for a particular building; and*
- (10) *Proposed action offices/agencies to implement the*

recommendations.

- f. *A copy of the L&L survey report will be retained by the servicing ESC/ESO and RSO/PSO, and a copy will be forwarded to DS/PSP/PSD and DS/ST/OSB via electronic or other means. DS/PSP/PSD will provide copies to OBO and tenant organizations, as appropriate, and confirm that responsible parties have implemented changes prior to designation as an L&L facility.*

12 FAM 446.3 Physical Security Requirements

(CT:DS-123; 12-13-2006)

- a. Each L&L office facility will have only one door, designated the L&L door, for use after *normal business* hours. This door will be the last point of exit/initial point of entry of *an* L&L building. *As an alternative, to facilitate the use of the public access area by local guards after normal business hours, the interior hard-line door between the public access area and the general work area may be designated and equipped as the L&L door. Restroom facilities should be available to local guards or procedures implemented to relieve guards for appropriate breaks.* Locking hardware for this door is identified in 12 FAH-5, Physical Security Handbook, as SHW-18 (opaque door) or SHW-18A (transparent door).
- b. All exterior forced-entry (FE) doors must have the door manufacturer's threshold plate installed and be in accordance with the manufacturer's specifications.
- c. *Facilities with non-FE exterior doors will be secured with a DS-approved 1-inch throw deadbolt or equivalent locking device.*
- d. In the eventuality of an electrical or mechanical lockout of the L&L door, a separate door equipped with bypass hardware *will be provided. The L&L bypass door hardware requirements consist of forced-entry locks with external keyways, a locked and alarmed DS-approved key container located adjacent to the bypass door that, in addition to keys, contains a switch to temporarily disable electrical or electro-mechanical locks on the bypass door.*

12 FAM 446.4 Technical Security Requirements

(CT:DS-123; 12-13-2006)

- a. *All unclassified office facilities* with high-value assets will require the installation of a separate DS-approved *intrusion detection* alarm system (IDS) dedicated to L&L for the purpose of monitoring designated alarm points. *The system must adhere to the following requirements:*
 - (1) *The IDS control panels, L&L access control system panels, keypads*

used for programming either system and any associated power supplies must be located in the SIC room. Additionally, all IDS control panels must be protected by a volumetric sensor and configured so that the IDS panel protects itself. If a SIC room does not exist, one of appropriate size must be constructed to house the equipment. The room must provide the necessary electrical service, cooling, and ventilation. Walls must be constructed floor to ceiling using 3/4 inch plywood plus sheetrock. The SIC room door will be solid core wood or hollow metal and be equipped with the SHW-17 hardware in accordance with 12 FAH-5, Appendix G;

- (2) The SIC room door must be monitored by the *IDS*.
- (3) *Power for the technical security systems must be regulated and supported by battery backup or UPS system. The required duration of backup supplied by the UPS should consider factors relevant to the likely security incidents and the availability/reliability of local power whether or not a backup generator is in use at the facility;*
- (4) *The IDS will be deployed as the dedicated alarm system for building or facility alarms; SIC rooms; and other areas as required;*
- (5) A dedicated power supply with a backup battery of at least 6.5 AH must be provided for the L&L door when utilizing SHW-18 or SHW-18A hardware. *The required duration of backup supplied by the UPS should consider factors relevant to the likely security incidents and the availability/reliability of local power;*
- (6) *At minimum, a door contact and one DS-approved detection technology will be used to protect all ingress and egress points of the area to be protected (generally the suites within the building);*
- (7) *All building exterior doors and interior building doors of offices under control of the U.S. Government containing high-value items must be monitored by the IDS;*
- (8) All alarm devices will be configured as separately identifiable alarm points;
- (9) *Volumetric protection will be provided for office areas containing high-value assets at critical and high crime threat posts. Office facilities at low and medium crime threat posts that do not meet exterior forced-entry protection for walls, doors, and windows, which are accessible without climbing tools or within 16 feet above a publicly and easily accessible surface, also require volumetric protection for office areas containing high-value assets;*
- (10) All volumetric detectors must be tamper alarmed. *Tampers shall report as separate alarm points;*
- (11) *IDS will have two methods of reporting all system events, such as*

real-time printer, alarm panel down-loadable event memory, or other DS-approved methods;

- (12) The L&L alarm system must be *armed and disarmed using* personal identification numbers (PIN) *that are unique to each individual user. The alarm system keypad* must be located on the interior wall adjacent to the L&L door, positioned to preclude visual compromise from the building exterior *and protected by a volumetric detection device;*
 - (13) The assignment of PIN pad numbers must be random in nature and consist of five or more digits/characters;
 - (14) *The L&L alarm system keypad status indicator must display system activity and/or errors. All such activity must be acknowledged and/or cleared by a user with the appropriate permission level;*
 - (15) The alarm system must have date and time stamping that can be used to determine *when an intrusion occurred;*
 - (16) *A keypad must be installed within the SIC Room (one for each IDS control panel) for system programming. Alarm system keypads not located within the SIC Room must be configured so that they cannot be used to program or re-program the system.*
- b. *Wiring for all Technical Security Systems must be fully contained within ferrous metal electrical conduit installed in accordance with the National Electrical Code or local electrical code, whichever is most stringent.*
 - c. A test of the L&L technical security system must be performed *on a bi-annual basis* and after the occurrence of any suspected *unauthorized intrusion*. Inspection should include all exterior door-locking systems and walk test of alarm system (i.e., to include all applicable doors, volumetric detection devices). The test must be performed by technically competent *DS-authorized personnel*.

12 FAM 446.5 Operational Security Requirements

(CT:DS-123; 12-13-2006)

- a. Post management and the RSO/PSO will develop a standard operating procedure (SOP) plan for securing the building in accordance with the L&L policy. *(See Recommended Procedures for Securing Lock and Leave Facilities.)*
- b. The RSO/PSO will establish appropriate post specific methods and procedures for *notification and/or response to any L&L alarm events or anomalies with technical security systems*.
- c. After each L&L alarm activation, *the RSO/PSO, or a designated trained* cleared U.S. citizen will log the time and date *of the discovery and retain*

applicable event records. Unexplained findings will be immediately reported to the RSO for appropriate action *and the servicing ESC/ESO.*

- d. All malfunctions and anomalies of the L&L systems will be reported immediately to the RSO *for analysis and resolution.*
- e. *When exiting the L&L office facility:*
 - (1) *The designee, a cleared U.S. citizen as determined by the RSO or the PSO, responsible for lock down must ensure that the building is void of all personnel.*
 - (2) All exterior FE doors (with the exception of the L&L doors) will be internally secured *by engaging the* forced-entry locks;
 - (3) Entries into a L&L log book (or equivalent DS-approved *logging and/or access control* methodology) must be made upon initial lockup or opening *for all after business hours* entry or departure; and
 - (4) The L&L alarm system must be activated via a PIN pad or other DS-approved device prior to exiting the building.
- f. The RSO/PSO *must* control and maintain the L&L door combination, *exterior key container combination and all access control and IDS system access codes in DS-approved secure containers.*
- g. *The non-FE L&L bypass doors must have a DS-approved 1-inch deadbolt lock with external keyway.*
- h. *Emergency exit doors that are also used as bypass doors must be fitted with DS-approved hardware as instructed in the DS Lock and Leave Applications Guide for Unclassified Posts.*
- i. Removable lock cores of all exterior doors *must be periodically inspected and replaced if there is any evidence of tamper.*
- j. *The following key controls apply:*
 - (1) The external removable cores of the forced-entry locks on the L&L bypass door *and SIC room* must be keyed differently with no master or grandmaster key;
 - (2) The facility bypass door keys are to reside in a locked and tamper-alarmed DS-approved depository container located adjacent to the *bypass door.* It will be anchored or imbedded securely to the *hard-line wall; and*
 - (3) Keys to the *SIC room* will be tracked during *business* hours and secured at the end of each workday by the *RSO/PSO.* *Only cleared U.S. citizens are allowed unescorted access to the SIC room and possession of its keys.*

12 FAM 447 THROUGH 449 UNASSIGNED