12 FAM 370
PHYSICAL SECURITY—DOMESTIC OPERATIONS

(CT:DS-133; 05-21-2008)
(Office of Origin: DS/DO/DFP)

12 FAM 371 DOMESTIC FACILITIES PROTECTION

12 FAM 371.1 General

12 FAM 371.1-1 Policy

(CT:DS-133; 05-21-2008)

The Directorate of Domestic Operations (DS/DSS/DO) is responsible for protecting information and property, and for safeguarding employees at domestic Department facilities.

12 FAM 371.1-2 Authority

(CT:DS-133; 05-21-2008)

Omnibus Diplomatic Security and Antiterrorism Act of 1986 (Public Law 99-399).

12 FAM 371.2 Program Office

(CT:DS-133; 05-21-2008)

The Office of Domestic Facilities Protection (DS/DO/DFP) is responsible for managing the domestic facilities protection program.

12 FAM 371.3 Office Management

(CT:DS-133; 05-21-2008)

Office managers include:

- Director of the Office of Domestic Facilities Protection (DS/DO/DFP)
- Chief of the Security Support Division (DS/DFP/SSD)
- Chief of Uniformed Protection Division (DS/DFP/UPD)

12 FAM 371.4 Access Controls

(CT:DS-133; 05-21-2008)

a. Persons entering secured domestic Department facilities must:

(1) Display appropriate Department building pass identification; and

(2) Use such identification as required for entrance to the individual facility (see 12 FAM 371.5).

b. DS/DO/DFP should make access control and escort procedures readily available to the Bureau of Diplomatic Security (DS) uniformed security officers to ensure employee and visitor compliance.

12 FAM 371.5 Mandatory Use of Identification Media

(CT:DS-133; 05-21-2008)

a. The Department has a policy of mandatory use of identification media (excepting those identified in paragraph c of this section). This allows Department security personnel to readily confirm that an individual is authorized to be within a Department facility or grounds.

b. For the purpose of this section, the term "Department building pass identification" refers to any of the following:

(1) Building pass;

(2) Building identification;

(3) Visitor pass; or

(4) Identification media (i.e., smart chip badge, non-smart chip badge, visitor badge, or any other Department authorized badge issued for the purpose of gaining access to Department facilities or grounds).

c. The following persons are not required to display a valid Department

building pass identification within designated Department facilities or grounds:

(1) Authorized visitors escorted within HST by Department personnel in possession of a VIP pin;

(2) Children of Department employees (parent/guardian) under the age of 16, while under the direct control, supervision, and escort of the employee (parent/guardian);

(3) Persons entering on an emergency basis (firemen, paramedics, and police) may be admitted without pass issuance; DS is responsible for monitoring their presence. Those employees who requested such assistance are responsible for immediately informing DS of the request for such assistance.

d. Persons (excluding those listed in paragraph c of this section) within designated Department facilities or grounds must always display a valid Department building pass identification.

e. Building passes should be displayed:

(1) on the upper front torso;

(2) of the outermost garment; and

(3) with the photograph clearly visible.

f. Locally employed staff (LES) at diplomatic facilities abroad are employees of the U.S. Government and may access the Harry S Truman building (HST) and other authorized facilities during normal business hours as a nonescort required visitor under the following conditions:

(1) The LES possess and displays a valid U.S. embassy issued identification card; and

(2) The RSO or a sponsoring office (e.g., Foreign Service Institute, conference host; etc.) has pre-registered the LES using the Visitor Access Control System - Domestic (VACS-D) by:

(a) Logging onto the Department Intranet;

(b) Selecting Visitor Information in the iNet directory;

(c) Selecting Visitor Pre-Registration; and

(d) Completing and submitting the form;

(3) Outside of normal business hours LES are treated as visitors and must be escorted according to 12 FAM 371.5 i.

g. Department building pass identification must comply with Federal Information Processing Standard Publication (FIPS PUB) 201 standards and associated special publications.

h. DS uniformed security officers may challenge any person without a pass and escort the person to his or her office, workplace, security control point, or building reception area to verify that the employee is a valid pass holder. The person must fully cooperate with the uniformed security officers under these circumstances. Failure to comply may result in adverse administrative action.

i. Employees with an "E" (depicting escort authority) on their smart badge may sign visitors into Department facilities. Employees who sign in visitors must escort and control their visitor while the visitor is on Department property. Visitors from other U.S. Government agencies do not require an escort during normal business hours. If a visitor who requires an escort intentionally eludes their Department escort, the Department escort must immediately alert a DS uniformed security officer or the facility's principal unit security officer in person or by phone.

j. If an employee fails to maintain custody of an escort-required visitor, the employee's appropriate security officer must be informed and the responsible security officer must complete Form OF-0117, Notice of Security Incident (see 12 FAM 553.1).

12 FAM 371.6 Safeguarding and Control of Identification Media

(CT:DS-133; 05-21-2008)

a. Employees should protect their Department building pass identification against loss or theft. Employees who lose their Department building pass identification due to negligence may be subject to administrative actions.

b. Proper uses of Department building pass identification include:

(1) Display within Department facilities open to the public;

(2) Display within Department facilities or property closed to the public;

(3) Display upon the request of Federal protective officers, or other authorized individuals when entering, leaving, or while on Department property;

(4) To access Department information systems when required and in the use of Public Key Infrastructure (PKI) applications; and

(5) For identity verification at other Federal and State facilities when required.

c. Improper uses of a Department building pass include:

(1) Using another person's Department building pass identification;

(2) Permitting another person to use one's Department building pass identification;

(3) Permitting other individuals to enter/exit with the aid of one's own Department authorized identification media (commonly referred to as "piggybacking");

(4) Using Department building pass identification for a purpose unrelated to the performance of official duties;

(5) Duplicating or copying Department building pass identification;

(6) Altering or defacing Department building pass identification.

d. Employees should immediately report lost or stolen Department building pass identification to the DS Uniformed Security Services and to supervisor. Failure to report such loss may result in adverse administrative action.

12 FAM 371.7 After-Hours Access to Buildings

(CT:DS-133; 05-21-2008)

a. Employees requiring access to Department facilities after hours where the space is not accessible by use of DS access control readers will be required to sign in and out with the DS security officer.

b. Some visitors may not require an escort during normal hours, but during non-business hours all visitors must be escorted.

12 FAM 371.8 Other Controls

(CT:DS-133; 05-21-2008)

In unusual or emergency circumstances, DS may impose additional security measures or restrictions as deemed appropriate.

12 FAM 372 DS IDENTIFICATION MEDIA

12 FAM 372.1 Administration

12 FAM 372.1-1 Purpose

(TL:DS-68; 05-26-2000)

This policy applies to all elements of the Bureau of Diplomatic Security (DS) for all credentials, badges, identification pins, and any identification media developed. This policy governs the issuance, use, maintenance, safeguarding, disposal, and accountability of DS identification media.

12 FAM 372.1-2 Responsibilities

(TL:DS-68; 05-26-2000)

a. The Director of the Diplomatic Security Service (DSS) is responsible for approving DS identification media policy. The Director of Domestic Operations (DS/CIS/DO) has the authority for implementation and oversight of the DS identification media program.

b. The Director of the Office of Domestic Operations is responsible for all DS identification media. The Security Support Division, Systems Operations Branch (DS/DO/SSD), is responsible for the day-to-day operation and implementation of the identification media policy.

c. DS/DO/SSD manages all the necessary facilities and equipment to issue authorized DS media.

12 FAM 372.2 Types of Identification Media

12 FAM 372.2-1 Credentials

(TL:DS-68; 05-26-2000)

a. The two-part credential approved April 10, 1998, is the only valid credential for official use. An embossed leather case is provided for holding and displaying the credentials.

b. A DS employee will possess only one type of the DS credential at any one time. As a general rule, a DS officer will be issued the credentials for the position in which the officer is serving.

c. Credential control numbers are located on the lower right-hand corner of the bottom half of the two-part credential. Each credential will have a category prefix and chronologically ascending control numbers.

d. DS currently issues distinctive printed identification media for the following categories of personnel:

(1) Special category credentials:

- Executive Director;
- Director – The Director of DSS;
- Legal Advisor – DSS Legal Advisor;
- Public Affairs Officer – DSS PA Officer;
- Others as approved by the Director;

(2) Special agents:

- Deputy Director – The Deputy Director of DSS;
- Assistant Director – SA personnel assigned as office directors;
- Special Agent In Charge – Self-explanatory;
- Special Agent – Self-explanatory;
- Special Agent Retired – All SAs who retire in good standing;

(3) Security engineering officers:

- Assistant Director – Office director;
- Supervisory Security Engineer – Regional, division, and branch chiefs;
- Security Engineer – All other SEs;
- Security Engineer Retired – All SEs who retire in good standing;

(4) Security technical specialists;

(5) Security officers:

- Assistant Director – Office director;
- Supervisory Security Officer – Division and branch chiefs;

- Security Officer – All persons assigned to offices as security officers, specialists, WAE RSOs, and other WAE personnel as approved by the Director of DSS;
- Security Officer Retired – All SOs who retire in good standing;

(6) Special investigators:

- Supervisory Special Investigator – Division and branch chiefs;
- Special Investigator - Persons assigned to DS as SIs;
- Special Investigator Retired – All SIs who retire in good standing;

(7) Diplomatic couriers.

12 FAM 372.2-2 Badges

(TL:DS-68; 05-26-2000)

DS currently issues five types of badges approved April 10, 1998. The position title located on the bottom rocker of the badge indicates the type of badge. Badge types include: Director, Deputy Director, Assistant Director, Special Agent in Charge, Special Agent, Security Engineering Officer, Security Officer, and Diplomatic Courier. Control numbers are stamped on the back of each badge.

12 FAM 372.2-3 Security Lapel Pins

(TL:DS-68; 05-26-2000)

Security lapel pins are used by federal, state, and local law enforcement agencies involved in protective security activities. DS issues and controls DOS security pins. A specific color pin is worn on the lapel identifying the wearer as being involved with a protective detail, having access to closed areas or authorized VIP escort privileges. Types of security lapel pins are as follows:

(1) A protective security lapel pin is a specific color pin worn on the lapel identifying the wearer as being involved with a protective detail;

(2) A protective security support lapel pin is a specific color pin worn on the lapel identifying the wearer as being involved with a protective detail;

(3) The VIP escort pin is issued to a DOS employee for the purpose of escorting cabinet, congressional, or ambassador-level visitors into the Department;

(4) Special access pins are issued to DOS employees who have a need to be in an area that has been closed for security reasons, usually because of a VIP arrival or protective detail.

12 FAM 372.2-4 Media Jackets

(TL:DS-99; 06-16-2004)

a. The Diplomatic Security Service (DSS) media jacket is official Department of State equipment. For service uniformity, the new media jacket replaces all previously issued or purchased jackets that were utilized with the issued bullet resistant vest and will be the only DSS identifier jacket worn during raids and arrests. All previously existing media, raid, and/or identification jackets should be turned in through the officer's respective supervisor for disposition and/or destruction. (See 12 FAM 372.2-4, paragraph j.)

b. Use of the media jacket is mandatory for all official events where Law Enforcement Officer (LEO) public recognition and identification enhances officer safety and public awareness of the Diplomatic Security Service. The media jacket may also be worn with full identifiers displayed for events such as crime scene security and searches, and public events where DSS has official duty functions, (e.g., Presidential Inaugurations, G8 summit duty, Olympic security functions, DSS representation at National Police Week affairs, Protective Security (PRS) operations, emergency and crisis situations where DSS may be assisting other LEO organizations). Special Agents in Charge (SACs) and Agents in Charge (AIC) of protective details will provide guidance in these situations and events.

c. Diplomatic Couriers will be issued a specialized convertible (reversible) media jacket/safety vest for use while on the tarmac, under the aircraft, in aircraft movement areas, or while embarking or disembarking from the aircraft.

d. The non-expendable media jacket will be issued to the following categories of personnel:

(1) Special Agents, FS-2501 and GS-1811;

(2) Security Engineering Officers, FS-2550;

(3) Security Technical Specialists, FS-2560;

(4) Diplomatic Couriers, FS-2580;

(5) Security Specialists, GS-080 and other security skill codes; and

(6) Investigative Assistants.

e. The Office of Training and Performance Support (DS/T/TPS) will issue the media jacket to Special Agents, Security Engineering Officers and Security Technical Specialists upon graduation from respective basic training courses. Upon determination of need, the remaining DSS security positions identified in 12 FAM 372.2-4, paragraph d will be issued media jackets through the officer's respective supervisor.

f. The same intent of rules that govern the use and protection of official DSS identification media, (i.e. credentials, badges and PRS ID pins) will apply to the media jacket. The media jacket is not authorized for personal off duty use outside of recognized LEO or other authorized functions. The media jacket must be kept clean and serviceable at all times. Each DSS officer issued the media jacket is responsible for the serviceability and ordinary care of the jacket.

g. DSS personnel who lose or have their media jackets stolen, must report it appropriately to the Defensive Equipment and Armored Vehicle Division (DS/PSP/DEAV) or the Office of Diplomatic Courier Service (DS/C/DC), through their immediate supervisor as soon as possible.

h. Requests for replacement DSS media jackets must be submitted via memorandum, through the responsible office director, to DS/PSP/DEAV. Requests for replacement of the specialized convertible media jacket/safety vest for the Diplomatic Couriers must be submitted to DS/C/DC. The request must include the following information: name, position title, grade, skill code, clearance level, and an explanation of the circumstances surrounding the incident.

i. DSS personnel upon termination, resignation, suspension or retirement must surrender their media jackets, through their respective supervisor, to DS/PSP/DEAV or DS/C/DC, as appropriate.

j. DS/PSP/DEAV or DS/C/DC will determine the serviceability of the media jackets and take appropriate action regarding the disposition and/or destruction of the jackets. Both offices will ensure that a complete audit trail for the receipt, storage, issuance, and destruction of media jackets is maintained at all times.

12 FAM 372.3 Use of DS Identification Media

12 FAM 372.3-1 Methods of Use

(TL:DS-68; 05-26-2000)

Identification media must be used only for official business. DS personnel must introduce and identify themselves verbally while displaying their credentials. Generally, credentials will not be relinquished to the person(s) for whom they are being displayed.

12 FAM 372.3-2 Restrictions and Proscriptions

(TL:DS-68; 05-26-2000)

a. DS identification media shall not be used for personal advantage or gain, for personal business, or to avoid responsibility and/or culpability in matters of regulation or law.

b. The unlawful purchase, reproduction, duplication, or altering of DS identification media is prohibited and is a violation of title 18 U.S.C. section 701. Authorization by the Director of DS/CIS/DO is required for the purchase, reproduction, duplication or alteration of DS identification media.

c. Misuse or the failure to follow the restrictions and proscriptions concerning reasonable and proper use of DS identification media may result in adverse administrative action.

12 FAM 372.4 Issuance and Control

12 FAM 372.4-1 Eligibility for Issuance

(TL:DS-68; 05-26-2000)

a. Initial DS special agent, criminal investigator, security engineer, security technical specialist, security specialist and diplomatic courier identification media are issued by Office of Professional Development Security (DS/EX/PLD) upon graduation from respective training courses. These media can only be requested for career Foreign Service or Civil Service employees specifically hired and trained to serve in the following position titles and skill codes:

   (1) Special Agent, FS-2501;

(2) Criminal Investigator, GS-1811;

(3) Security Engineering Officer, FS-2550 or GS equivalent;

(4) Security Technical Specialist, FS-2560;

(5) Security Specialists, GS-080 and other security skill codes; and

(6) Diplomatic Courier, FS-2580.

b. Other DS civil servants, persons on detail or contractors are issued DS identification media when it is essential to the performance of their DS responsibilities. Personnel who may qualify are those who are serving in support positions involving protective security, EOD and weapons training, or in internal inspections, surveys, and investigations. They may be career civil servants on detail from other agencies or DS contract employees. Special investigator credentials are issued to persons who are conducting personnel security investigations. Only upon determination of need and or proper justification will the Director of the Office of Domestic Operations approve requests for DS identification media. The Office of Domestic Operations will forward any special situations not covered above to the Director of DSS for final determination.

12 FAM 372.4-2 Requesting Procedures

(TL:DS-68; 05-26-2000)

a. All requests for reactivation and/or replacement of DS identification media must be submitted by a supervisor through the responsible office director via memorandum to the DS/CIS/DO Office Director. The request must include the following information: name, position title, grade/contract equivalent, skill code, clearance level, type of credential required, and a justification of need.

b. Nonstandard, unique or honorific requests for issuance of DS identification media will be considered on a restrictive case-by-case basis. Such requests will be sent to the DS/CIS/DO Office Director who, in turn, recommends approval/disapproval to the Director of DSS for the final decision. The request must include the following information: name, position title, type of credential required, and a justification of need.

c. DS identification media must be kept clean and serviceable at all times. Worn or damaged media must be replaced as soon as possible. Standard replacement of outdated or damaged credentials may be done in person at the Systems Operations Branch in Main State.

d. For personnel located outside the Washington, D.C. area or at overseas posts, all requests for replacement of DS identification media must be sent to the DS/CIS/DO Office Director. Include two color photos of the head, approximately 1 x 1¼" with a light blue background. The request must include the name, position title, grade/contract equivalent, skill code, clearance level, type of credential required, and a justification of need. The request may be sent via certified mail or the diplomatic pouch system. When the recipient receives replacement identification media, old credentials should be cut in half and returned to the Systems Operations Branch via certified mail or the diplomatic pouch system. It is incumbent upon the recipient of the credential to request a replacement when major changes in appearance occur, such as shaving or growing a beard.

12 FAM 372.4-3 Outside Agencies or Organizations Request for DS Identification Media

(TL:DS-68; 05-26-2000)

DS/CIS/DO may honor requests from other federal, state, and local law enforcement agencies for examples of DS identification media. Only photographic reproductions of DS identification media will be provided. All requests for examples of DS identification media must be made in writing on agency letterhead, expressing the need, and addressed to the Director of the Office of Domestic Operations.

12 FAM 372.5 Protection and Use

12 FAM 372.5-1 Safeguarding and Carrying DS Identification Media

(TL:DS-68; 05-26-2000)

a. DS personnel are responsible for safeguarding their issued media at all times. Media not being routinely used or carried should be secured in a GSA-approved container within U.S. Government-controlled space.

b. While armed or performing official duties, employees must keep their issued DS identification media on their persons.

c. DS identification media shall not be left in unattended vehicles, unless secured in the trunk.

d. Persons being issued DS identification media have the choice of a badge

clip and single-fold credential case or a combined badge and credential case.

12 FAM 372.5-2 Lost or Stolen DS Identification Media

(TL:DS-68; 05-26-2000)

a. DS personnel who lose or have their identification media stolen, must report it to DS/DO/SSD via phone, and to their immediate supervisor as soon as possible. The verbal report must be followed by a memorandum, through their supervisor, to the Director of the Office of Domestic Operations explaining circumstances surrounding the incident. DS/CIS/DO will forward a copy to the Branch Chief of DS/ICI/PR to determine if an inquiry should be initiated.

b. If one protective security pin is lost, the entire set must be replaced because they are numbered. A memorandum to the Director of DS/CIS/DO must be sent with the remaining pins. Remaining pins will be destroyed and the DS/DO/SSD identification media custodian will record the number and type of the lost pin in the replacement report and identification media log.

c. An employee whose negligence results in the loss or theft of DS identification media is subject to discipline up to and including separation for cause.

12 FAM 372.5-3 Disposition, Termination, Resignation, Suspension or Retirement

(TL:DS-68; 05-26-2000)

a. DS personnel upon termination, resignation, suspension or retirement must surrender their DS identification media to the Systems Operation Branch. At that time, the DS/DO/SSD identification media custodian will sign a departing employee checkout sheet. Should the employee be in the field, the employee's supervisor is responsible for obtaining the identification media directly from the employee prior to the employee separating from the Department of State. The identification media may be hand carried or sent via registered mail to the Systems Operation Branch.

b. Employees on leave without pay or administrative nonduty status, with or without pay, must surrender their credentials to their supervisor. If the employee does not return to duty within 30 days, the supervisor shall forward the DS identification media to the Systems Operation Branch.

The credentials will be retained during the period of nonduty status. This policy does not apply to DS training assignments.

c. A tenured employee in good standing who retires from DS may request his or her identification media as memorabilia. The media must be clearly altered by perforating the annotation "retired" across both halves of the credential or encasement of the identification media. The request will be submitted in writing by an employee's supervisor and forwarded to the Director of Domestic Operations. Persons who retire may receive encased credentials and badge and the retired credentials and badge at no cost. Protective Security lapel pins may not be retained.

d. A tenured employee in good standing who resigns from DS may request his or her identification media as memorabilia. The media must be clearly altered by perforating the annotation "void" across both halves of the credential or encasement of the identification media. The request will be submitted in writing by an employee's supervisor and forwarded to the Director of Domestic Operations. Persons who resign are responsible for the cost of the encasement of the credentials and badge. Protective security lapel pins may not be retained.

12 FAM 372.6 Special Requirements

12 FAM 372.6-1 Ownership and Surrender

(TL:DS-68; 05-26-2000)

a. DS identification media is the property of the U.S. Government and is provided to the employee for the convenience of the Government. At no time does the employee possess property rights to DS identification media. See 12 FAM 372.5-3, paragraphs c and d, for exceptions to this policy (i.e., retirement and resignation).

b. Any DS supervisor may direct a subordinate employee to surrender his or her official DS identification media (e.g., badge, credentials, DS lapel pins, and Department building pass identification cards, if applicable). The Director, Deputy Director, Executive Director, and Office Director of Domestic Operations may direct any employee to surrender said media.

c. Failure to comply may result in charges of insubordination under Department regulations, as well as violations under various federal statutes concerning the theft or misuse of official U.S. Government identification media.

12 FAM 372.6-2 Current DS Identification Media

(TL:DS-68; 05-26-2000)

Only current samples of DS printed identification media are provided to other federal, state and local law enforcement agencies for reference and the establishment of bona fides. Therefore, it is important that all DS personnel possess current identification media. As a rule, identification media will be updated every five years from the date of issue. Before an overseas assignment, employees should ensure that their DS identification media are current for the duration of the tour.

12 FAM 372.7 Organization and Accountability

12 FAM 372.7-1 Right to Audit or Recall

(TL:DS-68; 05-26-2000)

The Director of the Office of Domestic Operations may audit, inspect, recall, withdraw or direct the exchange of DS identification media.

12 FAM 372.7-2 Design and Production

(TL:DS-68; 05-26-2000)

DS/CIS/DO is responsible for periodic changes and improvements to DS identification media. Suggestions for design changes or improvement should be sent to the Director of Domestic Operations. After the Director of DSS approves changes, the Systems Operations Branch initiates necessary contracts or obligations for the procurement of the various DS identification media.

12 FAM 372.7-3 Safeguarding, Destruction, and Internal Audit

(TL:DS-68; 05-26-2000)

a. DS/DO/SSD maintains supplies of various DS identification media. All blank DS identification media must be safeguarded at the same level of protection as Secret national security information.

b. DS/DO/SSD ensures that a complete audit trail for the receipt, storage, issuance, destruction, and retirement of DS identification media is maintained at all times. A destruction receipt containing media type and control number will document the destruction of obsolete or damaged

media. One member of DS/DO/SSD and another member of DS will witness the destruction. DS/DO maintains destruction receipts as a permanent record.

c. The Director of Domestic Operations shall annually, or more frequently if deemed appropriate, request an audit of identification media procedure records and accountability.

d. DS/CIS/DO shall prepare a report on a semi-annual basis for the Director of DSS and other senior DS management, which reflects statistics on the number, type, and category of DS identification media issued, replaced, lost or stolen.

12 FAM 372.7-4 Systems Operations

(TL:DS-68; 05-26-2000)

a. The Systems Operation Branch manages the DS identification media program. On a daily basis, the Systems Operation Branch will handle inquiries, approve requests, maintain record keeping, conduct identification media issuance, and submit reporting requirements.

b. The Director of DS/CIS/DO shall determine the record keeping requirements for the Systems Operation Branch, such as computer databases, electronic media backups, and/or collateral hard copy files.

12 FAM 373 THROUGH 379 UNASSIGNED