Transportation Security Administration

OFFICE OF LAW ENFORCEMENT/ FEDERAL AIR MARSHAL SERVICE

TSA MANAGEMENT DIRECTIVE No. 2800.18
FACILITIES SECURITY

To enhance mission performance, TSA is committed to promoting a culture founded on its values of Integrity, Innovation and Team Spirit.

1. **PURPOSE:** This directive provides TSA policy and procedures for the requirements to secure TSA-controlled facilities nationwide and to protect TSA personnel, facilities and assets from unlawful acts.

2. **SCOPE:** This directive applies to all TSA facilities, employees, and contractors.

3. **AUTHORITIES:**

   A. 41 CFR Part 102-74, *Facility Management*, and Part 102-81, *Security*

   B. DHS Delegation 12000, *Delegation for Security Operations within the DHS*

   C. DHS Directive 121-01, *Office of the Chief Security Officer*

   D. DHS Directive 121-01-011, *The Department of Homeland Security Administrative Security Program*

   E. DHS Directive 121-03, *Common Identification Standard for DHS Employees and Contractors*

   F. DHS Instruction Manual 121-01-010-01, Revision #01, *Physical Security*

   G. Federal Information Processing Standards Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*

   H. Homeland Security Presidential Directive (HSPD) 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*

   I. Interagency Security Committee Publication: *Facility Security Plan: An Interagency Security Committee Guide*

   J. Interagency Security Committee Publication: *The Risk Management Process: An Interagency Security Committee Standard*

   K. TSA MD 200.3, *Headquarters Facilities Management*

   L. TSA MD 200.57, *Personal Property Management*

   M. TSA MD 2800.15, *Foreign Visitor Management*

   N. TSA MD 2800.16, *Identification Media and Access Control Program*

   O. *TSA Program Of Requirements*

4. DEFINITIONS:

A. Access: Authorization for TSA personnel and contractors who have been issued an official form of TSA identification media that permits unescorted access into TSA-controlled facilities.

B. Access Control Program: Designed to prevent loss of TSA property and material, provide for the protection of employees and contractors, as well as minimize potential breaches of security by limiting access to only those individuals possessing legitimate reasons to enter TSA-controlled facilities.

C. Access Control Officer (ACO): Employees assigned by the Designated Official of the facility to assign access privileges to personnel.

D. Accountable Property Officer (APO): The individual responsible for the accountability and control of TSA-issued property within his or her jurisdiction. The responsibility may be a collateral duty designated to an individual with a different title within the organization.

E. Designated Official (DO): The highest ranking official of the Organization/Office at a specific TSA-controlled facility. Federal Security Directors (FSDs), Supervisory Air Marshals in Charge (SACs) and equivalents serve in this capacity, following security procedures implemented by the Chief Security Officer (CSO), and ensuring that their personnel comply with standards and requirements set forth in this directive and supplementary guidance.

F. Facility Security Manager (FSM): A person assigned by the DO of a TSA facility to coordinate all security, emergency, and safety policies, guidelines, and protocols for that facility. The FSM also serves as the ACO for the facility.

G. Facility Security Plan (FSP): Document that establishes how a specific TSA facility is being protected, the TSA elements that are responsible for protection of the facility, and the specific procedures and response plans that have been established for identified incidents.

H. Federal Security Level (FSL): A five-level categorization, Level I, Lowest Risk up to Level V, Highest Risk, that designates the security level of a Federal facility and serves as the basis for implementing protective measures under Inter-Agency Security Committee (ISC) standards. The FSL is determined by the following criteria: Mission Criticality, Symbolism, Facility Population, Facility Size, and Threat to Tenant Agencies. Consideration may also be given to intangibles to allow the level to be raised or lowered one level.

I. Identification Media: Photographic access cards that identify individuals as having been authorized for both physical and logical (i.e., electronic) access to TSA-controlled facilities and property.

J. Interagency Security Committee (ISC): A committee, chaired by DHS and comprised of 54 Federal departments and agencies, whose mission is the development of security standards and best practices for nonmilitary Federal facilities in the United States.

K. Levels of Protection (LOP): Enhancements established at a Federal facility to mitigate the threats identified by the FSL and Risk Assessment.

L. National Capital Region (NCR): For the purpose of this directive, includes TSA locations and facilities, located within 50 miles of Washington, D.C., excluding Washington Area airports.

M. Personal Identity Verification (PIV) Card: A security access card used to identify the cardholder as a Federal employee or contractor. The PIV Card allows the cardholder to obtain unescorted access to TSA facilities and to gain access to TSA information systems such as email and network access when approved equipment is deployed for use throughout the agency.

N. Physical Security: For purposes of this directive, defined as that part of security concerned with measures that: provide for the individual and collective safety and well-being of personnel, as well as visitors and clients; prevent unauthorized access to a designated facility; and, protect and safeguard information, equipment, materials, and documents within the facility against espionage, sabotage, damage, theft, and/or unauthorized disclosure.

O. Program of Requirements (POR): A document issued by the Physical Security Section that lists the security features, equipment and processes to be noted in Security Statements of Work to be installed at TSA Facilities as determined by the CSO and the Physical Security Section.

P. Risk Assessment (RA): An Inter-Agency Security Committee (ISC) process that conducts a comprehensive review of security procedures, processes, equipment, and mitigations in place at Federal facilities. The RA determines the FSL of the facility which establishes a baseline for minimum security enhancements to be installed at the facility. It also identifies the risk level of the facility which determines the LOP. The LOP may require security enhancements above the minimum level determined by the FSL based on operational needs, equipment and/or information used or stored at the facility, and threat and risk factors identified by the RA.

Q. Special Security Officer (SSO): An individual who works under the direction of the CSO and administers the receipt, control, and accountability of Sensitive Compartmented Information (SCI). The SSO oversees SCI security functions and reporting requirements for subordinate Sensitive Compartmented Information Facilities (SCIFs).

R. TSA-controlled Facility: A building, area, room, or leased space, whether for single or multitenant occupancy, and its grounds and approaches, all or any portion of which is under the jurisdiction, custody, or control of TSA. It includes TSA-controlled commercial space shared with non-government tenants; TSA-owned contractor-operated facilities; and facilities under a management and operating contract such as for the operation, maintenance, or support of a government-owned or controlled research, development, special production, or testing establishment. For purposes of this MD and the associated handbook, the terms *TSA-controlled Facility* and *TSA Facility* may be used interchangeably.

S. TSA Personnel: Persons permanently or temporarily assigned, attached, detailed to, employed by, or under contract with TSA (including student volunteers and foreign nationals).

T. Visitors: For purposes of this directive, individuals who have not been vetted or issued a TSA PIV card who require an escort to enter TSA facilities. This includes but is not limited to custodial/janitorial/building maintenance personnel, vendors, suppliers, business representatives, state and local government employees, other Federal Government employees, the general public, and Foreign Nationals.

5. RESPONSIBILITIES:

A. The TSA Administrator is responsible for developing policies and procedures to properly secure TSA facilities in accordance with Interagency Security Committee and DHS security requirements.

B. The Assistant Administrator/Director of the Office of Law Enforcement/Federal Air Marshal Service has programmatic oversight over TSA facilities security.

C. Assistant Administrators, and equivalents, are responsible for ensuring that subordinate organizations comply with DHS and TSA policy and procedures related to securing TSA facilities.

D. The Office of Inspection (OOI) is responsible for conducting periodic reviews of facilities for compliance with DHS and TSA established policies and procedures.

E. The Office of Financial Administration (OFA) is responsible for ensuring adequate funding, allocating funds to the respective program offices, and reviewing the related office expenditures as they occur.

F. The Office of Real Estate Services (ORES) is responsible for:

(1) Coordinating with the Physical Security Section, Security Branch, Security Services and Assessments (SSA) Division, to integrate Physical Security requirements into the design and construction of new facilities; and

(2) Coordinating with the Field Support Unit, Physical Security Section, on projects including repairs, maintenance, and upgrades, at new, existing, or renovated facilities.

G. The Chief Information Officer (CIO) is responsible for the management, implementation, and usability of information and computer technologies. CIO representatives can also provide technical reviews and input on the implementation or modification of security measures that require the use of an information technology system.

H. The CSO is responsible for:

(1) Developing and implementing policies and procedures for securing TSA facilities nationwide;

(2) Implementing security-related policies, programs, directives, and training within TSA;

(3) Providing final approval authority for all security enhancements implemented at TSA facilities; and

(4) Identifying, via memorandum, one primary and one alternate to serve as the DO for each TSA controlled facility.

I. FSDs, SACs, and equivalents are responsible for:

(1) Ensuring the safety, protection, and security of all occupants of their assigned office as well as all information, resources, and property over which they have knowledge and control;

(2) Serving as DOs;

(3) Following security procedures implemented by the CSO; and

(4) Ensuring that their personnel comply with the standards and requirements set forth in this directive and additional supplemental guidance.

J. The FSM is responsible for:

(1) Developing the FSP with the approval of the DO;

(2) Administering and implementing security operations, to include the FSP, under the direction of the DO; and

(3) Serving as the ACO for the facility.

K. The Personnel Security Section, Security Branch, SSA Division, is responsible for:

(1) Managing the Personnel Security program established to ensure that only loyal, reliable, and trustworthy people are granted access to TSA Facilities, IT Systems, and classified information, or allowed to perform sensitive duties;

(2) Assessing the loyalty, reliability and trustworthiness of individuals for initial and continued eligibility for access to classified information and/or position suitability; and

(3) Conducting initial and/or periodic investigations for the purpose of determining the eligibility of employees, contractors, consultants, and other persons affiliated with the TSA, for access to facilities, IT Systems, classified information, assignment or retention in sensitive duties, or other designated duties requiring such investigation.

L. The Physical Security Section, Security Branch, SSA Division, is responsible for:

(1) Conducting Risk Assessments (RAs) and FSL determinations for all TSA-controlled facilities in accordance within ISC at directed intervals;

(2) Maintaining a current real property inventory of all TSA-controlled facilities that includes FSL designations;

(3) Developing operational procedures for securing TSA facilities;

(4) Developing FSP guidance and instruction for TSA-controlled facilities;

(5) Ensuring written FSPs are maintained for each TSA-controlled facility designated, at a minimum, as "For Official Use Only (FOUO)";

(6) Following a risk management process to ensure achievable LOP are identified for each TSA-controlled facility based on FSL determinations and in accordance with published ISC standards, including the *Design Basis Threat Report*, and DHS and TSA Policies;

(7) Ensuring that each TSA-controlled facility follows baseline physical security measures commensurate with the appropriate determination and in accordance with published ISC standards;

(8) Establishing a Program of Requirements (POR), in coordination with the TSA Office of Real Estate Services, to prescribe the necessary security devices for new TSA facilities;

(8) Providing security for the rooms and areas where IT systems are stored or housed within the NCR and as implemented at TSA facilities nationwide;

(9) Providing day-to-day oversight for the operations of the TSA contracted security guards at TSA facilities nationwide;

(10) Conducting Closed Storage and Classified Briefing Room surveys to certify space used for Homeland Security Data Networks (HSDN) and Security Terminal Equipment (STE) processing and usage, and for classified Briefings up to the Secret Level;

(11) Projecting and planning resources, to include funding and people, to allow for the installation of new security countermeasures as well as the operation maintenance, repair and replacement of existing security countermeasures; and

(12) Developing Statements of Work (SOWs) for all security enhancements at TSA Facilities.

M. ACOs, or the responsible program officials are responsible for:

(1) Maintaining a security clearance equal to, or above, the highest level of classified material handled and stored at their respective location. Special Security Officers (SSOs) and Facility Security Managers (FSMs) at locations with a Sensitive Compartmented Information Facility (SCIF) will need clearance at the Top Secret (TS)/SCI level;

(2) Implementing access control requirements within their areas of responsibility;

(3) Providing for the protection of employees, contractors, and visitors, as well as minimizing potential breaches of security by limiting access to only those individuals needing to enter the facility; and

(4) Ensuring that individuals who enter open storage areas for classified information or other sensitive areas are briefed and clearly understand access control procedures and measures to protect classified national security information.

N. APOs are responsible for:

(1) Managing tasks associated with the accountability of identification and access control media (PIV cards or similar cards) issued to personnel in accordance with procedures promulgated by their respective Organizational Element (OE) Issuing Office; and

(2) Maintaining local records for the storage, issuance, control, accountability, retention, return, destruction, or disposition of PIV cards and access control media (i.e. keys, access control cards) under their area of responsibility, and complying with audits and inspections, as required, by this and other TSA and/or DHS directives.

O. TSA employees and contractors are responsible for:

(1) Complying with all requirements for the proper use, display, and control of TSA-issued property, IT Systems, information, and any other types of access control media in accordance with standards and requirements established by this directive and supplementary guidance materials;

(2) Remaining vigilant and challenging any person that is not readily recognized within the facility and when entering the TSA-controlled facility; and

(3) Remaining with their guests at all times and ensuring their guests are not allowed access to sensitive areas, discussions, information, or equipment while visiting the TSA-controlled facility.

6. POLICY:

A. Physical security programs shall be administered within each TSA-controlled facility based on this directive, and the guidance set forth herein, to ensure the protection of TSA employees, visitors and assets. These programs shall be administered by the DO and FSM and monitored to ensure their integrity. At a minimum, the physical security program must include:

(1) A physical security assessment to determine the security level of the facility and to determine the minimum-security safeguards required for protecting TSA personnel and assets;

(2) Periodic reassessments to ascertain whether the security program meets pertinent Federal and departmental standards or regulations;

(3) FSPs that specify the physical security practices implemented at each TSA facility;

(4) A comprehensive and continuing awareness and education effort to gain the interest and support of employees, contractors, consultants, and visitors; and

(5) Procedures for taking immediate, positive, and orderly action to safeguard life and property during an emergency.

7. **PROCEDURES:** Reference the *Facilities Security Handbook* for additional responsibilities and for information needed to implement the requirements contained within this directive.

8. **APPROVAL AND EFFECTIVE DATE:** This policy is approved and effective the date of signature unless otherwise specified.

APPROVAL

Signed October 30, 2017

Roderick Allison
Assistant Administrator/Director for
Office of Law Enforcement/Federal Air Marshal Service

Date

EFFECTIVE

Date

Distribution: Assistant Administrators and equivalents, Managers and Supervisors, BMO Directors, Federal Security Directors, Supervisory Air Marshals in Charge, Property Management Division, Accountable Property Officers

Point-of-Contact: Chief - Physical Security Section- Security Branch, psssecurity@tsa.dhs.gov (571) 227-3933 or pssfield@tsa.dhs.gov, 571-227-2195