



**Department of
Transportation**
Office of the Secretary
of Transportation

ORDER

1600.26B

Subject: DEPARTMENT OF TRANSPORTATION (DOT) FACILITIES
PROTECTION PROGRAM.

CHAPTER 1 -- GENERAL

1. PURPOSE

This Order prescribes policies to ensure an effective and efficient Facilities Protection Program for the U.S. Department of Transportation (DOT) and to implement within DOT all laws, Executive Orders, Presidential Directives, and applicable Government-wide regulations and directives pertaining to the protection of Federal facilities. It provides guidelines for each Secretarial Office and Operating Administration (OA) to establish, in collaboration with the responsible security organization, a successful risk management process with respect to the physical security of their facilities. It assigns responsibilities concerning the protection of DOT owned, leased, or occupied Federal facilities. This Order applies to DOT's administrative facilities as defined below and does not apply to operational facilities, such as those operated by the Federal Aviation Administration (FAA), as these are addressed by the National Infrastructure Protection Plan and its Transportation Sector.

2. BACKGROUND

A. DOT's mission is to serve the Nation by ensuring a fast, safe, efficient, accessible and convenient transportation system that meets the national interests of the United States and enhances quality of life for the American people. The Department plays a leadership role ensuring the Nation's transportation infrastructure remains safe, viable, and strong. The operational transportation infrastructure represents the primary components of the Transportation Sector, one of 18 sectors of the National Infrastructure Protection Plan (NIPP). DOT provides guidance over a vast array of transportation modes that are vital to supporting the day-to-day activities of all Americans. Guidelines for the protection of these modes rest with the Transportation Sector of the NIPP. Any disruption to the Transportation Sector has the potential to negatively affect national security and the Nation's economy, as well as the defense, health and safety of the Nation.

- B. DOT owns and operates facilities that vary in function and purpose; each of these physical assets is important to the overall mission of the Department. The types of facilities range from administrative offices to those that provide key infrastructure services such as air traffic control and the operation of waterways. Additionally, many DOT facilities house the Department's most important asset, thousands of DOT employees, who work daily to accomplish DOT missions. This Order provides guidelines for the protection of facilities dedicated to Administrative, Regulatory and Research (ARR) functions which are associated with the Government Facilities Sector of the NIPP.
- C. Each DOT component's infrastructure carries its own risk; thus each organization must examine its ARR facilities and use the guidance referenced in this Order to identify, assess, prioritize, mitigate, grade and regularly review the inherent risks associated with its ARR facilities. By following the risk management process outlined in the references, DOT will be able to mitigate risk at each of its ARR facilities. Stakeholders at all DOT organizations will be involved in this risk management process, including the Office of Security (M-40), Operating Administrations, Secretarial Offices, OA Security Coordinators, Facility Security Committees (FSC), the responsible security organization (in most cases the Federal Protective Service), information technology personnel and individuals assigned to DOT facilities.

3. SCOPE

- A. This Order applies Department-wide to all DOT OAs and Secretarial Offices, both at the Washington headquarters location and field facilities, excluding FAA Regional Offices, field facilities and all DOT operational facilities which are associated with the Transportation Sector. It applies to all facilities that are either DOT-owned, direct-leased, General Services Administration (GSA)-leased, or used under another form of agreement by any DOT component. These facilities and space include existing buildings, stand-alone facilities, campuses (educational and/or training facilities), individual facilities on campuses, warehouses, special-use facilities, Continuity of Operations facilities and/or Alternate Facilities. Also addressed is the physical security of child care centers located within DOT facilities. The provisions of this Order are critical and must be applied during the planning stages for new facilities, whether they are to be owned or leased, and to major modernizations at existing facilities.
- B. DOT facilities include elements that are often contained or housed within a larger facility. Specifically, this applies to multi-tenant, mixed-tenant, and mixed-multi-tenant facilities.
- C. This Order provides references for guidance on employing risk management principles to protect DOT facilities and addresses human threats to facilities. While naturally occurring threats such as earthquakes, fires, and meteorological events are generally beyond the scope of this Order, many of the protection methods

addressed by the Order, as well as the risk management process for facility oversight, will assist in risk mitigation for any naturally occurring event.

4. CANCELLATION

DOT Order 1600.26A, Department of Transportation Physical Security Program; July 25, 1990.

5. REFERENCES

- A. Executive Order 12977, Interagency Security Committee, October 19, 1995.
- B. Facility Security Level Determinations for Federal Facilities: An Interagency Security Committee Standard, February 21, 2008.
- C. Use of Physical Security Performance Measures: Interagency Security Committee, 2009.
- D. Physical Security Criteria for Federal Facilities: An Interagency Security Committee Standard, April 12, 2010.
- E. Facility Security Committees: An Interagency Security Committee Standard, January 1, 2012.
- F. Security Specialist Competencies: An Interagency Security Committee Guideline, January 27, 2012.
- G. Homeland Security Presidential Directive 7, Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003.
- H. National Infrastructure Protection Plan, 2009.
- I. Transportation Systems – Critical Infrastructure and Key Resources Sector Specific Plan – as input to the National Infrastructure Protection Plan, May 2007 (FOUO).
- J. Government Facilities Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan, 2010.
- K. Department of Homeland Security Management Directive Number 11042.1, Safeguarding Sensitive but Unclassified (FOUO) Information, dated January 6, 2005.
- L. Intelligence Community Directive (ICD) 705, Physical and Technical Security Standards for Sensitive Compartmented Information Facilities (ICS-705-1) and Standards for Accreditation and Reciprocal Use of Sensitive Compartmented Information Facilities (ICS-705-2).

- M. National Security Telecommunications and Information Systems Security Instruction No. 4005, Safeguarding Communications Security (COMSEC) Facilities and Materials, August 1997.
 - N. DOT Order 1661.10, Consolidation of Physical Security Services for the Department of Transportation, Washington Headquarters Facilities; April 27, 1992.
 - O. Best Practices for Mail Screening and Handling: An Interagency Security Committee Standard, September 1, 2011.
 - P. Executive Office of the President, Office of Management and Budget, Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors, February 3, 2011.
 - Q. Homeland Security Presidential Directive 12 (HSPD-12), Policies for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004.
 - R. National Institute of Standards and Technology (NIST) Special Publication 800-116, A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems (PACS), November 2008.
 - S. Department of Transportation (DOT) Order 1681.1, DOT Implementation Policy for Identity, Credential and Access Management (ICAM) and Homeland Security Presidential Directive -12, June 23, 2011.
6. TERMS AND DEFINITIONS: See Appendix A.
7. ACRONYMS: See Appendix B.

CHAPTER 2 -- NATIONAL POLICIES AND PLANS

1. GENERAL

The information contained in this Order originates in guidance stemming from multiple Federal Directives, Orders and manuals. Described below are the two primary Presidential documents that provide guidance for the protection of Federal facilities: Executive Order 12977 (E.O. 12977) and Homeland Security Presidential Directive 7 (HSPD-7). HSPD-7 is currently under review. Its replacement, a Presidential Policy Directive, is not expected to have any significant impact on this DOT Order.

A. *E.O. 12977*, October 19, 1995

Prompted by the 1995 Oklahoma City bombing of the Alfred Murrah Federal Building, the President issued E.O. 12977 to “enhance the quality and effectiveness of security in and protection of buildings and facilities in the United States occupied by Federal employees for nonmilitary activities.” E.O. 12977 established

the Interagency Security Committee (ISC). E.O. 13286, February 28, 2003, amended E.O. 12977, designating the ISC to be chaired by the Department of Homeland Security (DHS). ISC membership consists of senior executives from Federal departments and agencies. The ISC is mandated to carry out the policies of E.O. 12977. The ISC's mission is to safeguard the Nation's Federal civilian facilities from all hazards by developing state-of-the-art security processes and standards in collaboration with public and private homeland security partners. As such, the ISC provides processes, standards and best practices to assist Federal departments and agencies in outlining their facility security management. Specifically the ISC has issued four applicable policy guidelines:

1) *Facility Security Level Determinations*, February 21, 2008

This document provides guidance, criteria and processes for determining the facility security level (FSL), a categorization based on analysis of several security-related factors. This categorization serves as the basis for implementing scalable protective measures at the facility.

2) *Use of Physical Security Performance Measures*, 2009

This document provides guidance on the requirement for all Federal agencies to assess and document the effectiveness of their physical security programs through performance measurement and testing. This standard provides additional guidance on the establishment and implementation of a comprehensive measurement and testing program.

3) *Physical Security Criteria for Federal Facilities*, April 12, 2010

This standard establishes a baseline set of physical security measures to be applied to all Federal facilities based on their designated facility security level. It also provides a framework for the customization of security measures to address unique risks at a facility. Additionally, it provides an integrated, single source of physical security standards for all Federal facilities; opportunity and guidance for flexibility and customization of these standards; and integration of new standards and concepts contained in two other key ISC documents.

4) *Facility Security Committees*, January 1, 2012

This document provides guidance on the establishment, procedures, and decision-making process of a Facility Security Committee (FSC). FSCs are required at all Federal facilities having two or more Federal entities with funding authority.

B. *HSPD-7*, December 17, 2003

Following the September 11, 2001, terrorist attacks, HSPD-7 established policy for all Federal departments and agencies to identify their critical infrastructure and

ensure these resources are protected against future terrorist attacks. HSPD-7 specifically states, “Federal departments and agencies will identify, prioritize, and coordinate the protection of critical infrastructure and key resources in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them.” The issuance of HSPD-7 prompted Department of Homeland Security (DHS) to create and publish the National Infrastructure Protection Plan (NIPP) and its ensuing sub-documents. A review of HSPD-7’s draft successor document, performed in December, 2012, indicates no likely effect on this Order.

1) *National Infrastructure Protection Plan, 2009*

The overarching goal of the NIPP is to ensure the protection of the nation’s Critical Infrastructure and Key Resources (CIKR) from terrorist activities. The CIKR of the United States consists of the assets, systems, networks, and functions that provide vital services to the Nation. Additionally, the NIPP provides guidance to strengthen national preparedness, and ensure the rapid recovery of any loss to the country’s CIKR in the event of an attack, natural disaster, or other emergency.

2) *Sector Specific Plans*

HSPD-7 identifies 18 CIKR sectors that require protective actions to prepare for, protect, or mitigate against terrorist activities. Sector Specific Plans (SSP) detail the application of the NIPP’s risk management framework to the unique characteristics and risk landscape of 18 different sectors. The SSPs provide the means by which the NIPP is implemented across all 18 CIKR sectors. One of the 18 SSPs, DHS’s Government Facilities Sector, contains provisions that serve as basis for DOT’s ARR Facilities Protection Program.

3) *Government Facilities Sector-Specific Plan (GFSSP), 2010*

The GFSSP outlines a framework of steps designed to ensure the safety and security of government facilities so that essential government functions and services are preserved without disruption. Specifically, the GFSSP includes a step-by-step framework of guidelines for the implementation of a risk management process.

4) *Transportation Systems – Critical Infrastructure and Key Resources Sector Specific Plan – as Input to the National Infrastructure Protection Plan, May, 2007*

The Transportation Systems SSP and its supporting modal implementation plans and appendices establish the Transportation Systems Sector Specific Plan’s strategic approach based on the tenets outlined in the NIPP and the principles of Executive Order 13416, Strengthening Surface Transportation Security. The Transportation Systems SSP describes the security framework that will enable sector stakeholders to make effective and appropriate risk-based security and resource allocation decisions.

2. SUMMARY

The guidance issued from the ISC's policies, coupled with the overarching guidance provided in the NIPP and its corresponding GFSSP, have been incorporated by reference into this Order to provide the Department with a comprehensive Facilities Protection Program. For a full description of the relevant ISC and NIPP guidance directing DOT's Facility Protection Program, refer to the specified references.

CHAPTER 3 -- FACILITIES PROTECTION POLICY

All DOT Operating Administrations and Secretarial Offices shall adhere to the Facilities Protection Program requirements stated in this Order. DOT components shall comply with the guidelines in this Order, as well as with any applicable regulations or standards issued as the result of laws or Executive Orders. When necessary, Operating Administrations shall issue internal guidelines to address unique circumstances with regard to the protection of their facilities in order to implement the provisions of this program. Overall, the successful protection of DOT facilities will involve sharing information, building partnerships, implementing a risk management program, and managing resources efficiently. Specifically, the Department shall:

1. Support the overarching goal of the NIPP and adhere to the standards and best practices promulgated by the ISC. The primary document that provides guidance for the DOT Facilities Protection Program is the ISC Government Facilities Critical Infrastructure and Key Resources Sector Specific Plan.
2. Ensure facility protection activities are coordinated across all DOT Operating Administrations and Secretarial Offices. This coordination shall include the sharing of information, best practices, and collaboration among all DOT components responsible for facilities protection.
3. Use the risk management framework established by the ISC and the Government Facilities SSP to provide security for DOT ARR facilities. The principles of risk management call for a proactive approach to deter threats, mitigate vulnerabilities and limit the consequences of actions that could threaten DOT facilities. Adhering to the prescribed risk management framework will help ensure DOT performs its essential functions without disruption, and makes risk-based decisions in the allocation of resources.
4. Establish and update when needed the baseline or customized level of protection (LOP) for each facility, based on its facility security level (FSL).
5. Assess risk using a method that is credible, reproducible, and defensible. The Government Facilities SSP outlines specific risk assessment methodologies and tools.
6. Test and measure the Facility Protection Program's performance to identify opportunities for continuous improvement. The protection of facilities coupled with efficient management will result in a sustainable security program.

7. Ensure the best use of appropriate technology in the protection of DOT facilities by coordination with the Office of Security (M-40) and the Office of the Chief Information Officer (S-80).

CHAPTER 4 -- RESPONSIBILITIES

1. Assistant Secretary for Administration (M-1) shall:
 - A. Issue Departmental policy for effective compliance with and implementation of this Order, thereby ensuring DOT conformance with Federal regulations, laws and policies concerning the protection of Federal facilities.
 - B. Represent the Secretary of Transportation on the ISC and provide DOT representation, as appropriate, on ISC subcommittees and working groups that have responsibility for developing national policies governing the protection of Federal facilities and employees.
 - C. Coordinate with the DOT Chief Information Officer, the DOT Chief Financial Officer and the Heads of DOT Components to ensure the requirements of HSPD-12, the Federal Identity, Credential and Access Management (ICAM) initiative and the associated DOT HSPD-12/ICAM policies are implemented for facilities subject to this Order.

2. Director, Office of Security (M-40) shall:
 - A. Serve as the Executive Agent for the Assistant Secretary for Administration with respect to the Facilities Protection Program.
 - B. Administer and manage the DOT Facilities Protection Program exclusive of FAA's Regional offices, field facilities and operational transportation facilities that are specifically covered under the Transportation Sector of the NIPP.
 - C. Provide guidance to DOT component organizations to implement and maintain the Facilities Protection Program, ensuring it complies with all Government-wide security policies for the protection of sector specific government facilities.
 - D. Provide support to the Department as the subject matter expert (SME) on physical security.
 - E. Represent the Department on all applicable Federal, State, and local physical security committees. M-40 shall participate on interagency committees and working groups responsible for developing Government facilities protection policies. Additionally, when outside groups request participation of Operating Administrations and Secretarial Offices on matters involving the physical security of their facilities, M-40, as the SME, shall be consulted. M-40 shall

work with the Secretarial Office and/or OA to determine appropriate representation.

- F. Administer the Facility Protection Program at DOT headquarters facilities, Southeast Federal Center (SEFC), in Washington, DC. This Program shall also encompass the DOT offices at 55 M ST, FAA headquarters buildings 10A/B and other locations as determined by DOT. M-40 shall administer the physical security of these headquarters facilities in a manner consistent with the guidance set forth in Chapter 5 of this Order and with all applicable ISC guidance. M-40 shall function as the central point of control for protection of the headquarters buildings and shall recommend the establishment of, or changes to, policies and procedures relating to facility protection. M-40 shall consult with all applicable entities regarding new or changed security policies and shall respond to any requests from Secretarial Offices and OAs concerning security support within these headquarters facilities.
- G. Serve as DOT liaison with all other government agencies (both Federal and non-Federal) on matters involving the physical security for the headquarters facilities. M-40 shall provide a mechanism for headquarters personnel to exchange information, such as crime data and threat information, and for ideas concerning security operations and routine physical security support matters relating to headquarters facilities. M-40 shall have the authority to delegate portions of the Facility Protection Program; however, in the event of a security emergency, M-40 shall retain overall responsibility and authority, including the use of immediate action, without collaboration with other entities occupying the headquarters buildings. Upon conclusion of the security emergency, the Director of M-40 shall brief each DOT headquarters entity as appropriate.
- H. Determine the Facility Security Level for DOT SEFC, DOT offices at 55 M ST, FAA headquarters buildings 10A/B and other locations as determined by the Secretary of Transportation (S-1), consistent with ISC guidance, and adjust the FSL when the security situation dictates. Additionally, M-40 shall collaborate with each OA on the FSL for each facility not covered by the SEFC.
- I. Develop and maintain a master database for the FSL identified at each DOT facility nationwide as submitted by the OA Security Coordinators.
- J. Provide technical and policy advice as appropriate to OAs with regard to facilities protection. As necessary, collaborate with the OAs and their designated Security Coordinators on issues relating to facilities protection. When requested by the OAs, M-40 shall provide guidance and support within the mandates of this program.
- K. Provide advice and assistance to OAs' designated FSC representatives. When requested, M-40 Physical Security Specialists shall provide technical guidance through the OA Security Coordinator for security survey/assessments at OA facilities.

- L. Provide oversight of the OA responsibilities under this Order through the conduct of site visits/assessments and spot inspections as appropriate for DOT facilities. This oversight shall not be conducted in lieu of the assessments otherwise planned by the designated facility security organization, typically the Federal Protective Service (FPS), but shall complement these reviews.
- M. Provide technical support to the OAs with their identification and remediation of vulnerabilities at facilities where DOT components are in complete or primary tenancy.
- N. Support the Department's Facilities Protection Program and determine, establish and implement a method to track remediation of vulnerabilities identified at facilities where DOT components are in complete or primary tenancy. This information shall be utilized to provide input for the annual report to Congress regarding the Government Facilities Sector.
- O. Provide policy and technical advice to OAs, excluding FAA headquarters and their field sites, for the physical security and protection of special use spaces including, but not limited to, Communications Security facilities, Sensitive Compartmented Information Facilities (SCIF), any area where classified information is processed or discussed, command centers, weapons storage areas, warehouse storage areas, research and test facilities, training facilities, child care centers located within DOT facilities, academies/school campuses and other facilities as appropriate.
- P. Provide policy interpretation, technical advice and coordination among the Secretarial Offices and OAs prior to initial construction and/or significant modifications to any DOT facility. M-40 shall facilitate communication with other governmental agencies when facilities are planned and/or when significantly modified. Coordination shall be made at the earliest stages of the proposed construction/modification and prior to issuance of a Statement of Work. Plans, project drawings, and specifications shall be reviewed during the entire new construction/significant modification process.
- Q. Coordinate with OST Budget to ensure annual budget guidance provided to the Operating Administrations includes the requirement to provide support, as available, to the Department Facility Protection Program.
- R. Coordinate security measures, as necessary, with all Federal, State, and local law enforcement entities in response to demonstrations, threats, criminal investigations, or attacks against the DOT HQ Facilities (including the DOT offices at 1200 New Jersey SE, 55 M ST, FAA headquarters buildings 10A/B and other locations as determined by DOT). Additionally, collaborate with the Office of Intelligence, Security, and Emergency Response (S-60) as needed to ensure DOT's responses to security situations are effective and thorough.
- S. Review and approve physical security directives (excluding FAA) issued by the OAs implementing this Order.

- T. In order to ensure the continued professional proficiency of all SME's, M-40 shall advise DOT components on qualification training and provide guidance on courses offered by the Federal Law Enforcement Training Center, United States Department of Agriculture Graduate School, Office of Director for National Intelligence, or other training providers so that all DOT personnel engaged in facility protection are properly qualified.
 - U. Establish, lead, and provide focus to a working group comprised of Security Coordinators appointed by OAs. This group shall function as a forum to receive security policy guidance/direction and to exchange information concerning lessons learned and issues related to the implementation of DOT and national level security policies by the OAs and Secretarial Offices.
 - V. Lead the implementation of HSPD-12/ICAM requirements with respect to the physical security of DOT facilities (excluding FAA). M-40 shall ensure that risk assessments are performed, and that the recommended mitigations are consistent with the requirements of HSPD-12/ICAM.
 - W. Coordinate with S-60 on counterintelligence activities that have an impact on DOT facilities.
3. Director, Office of Intelligence, Security, and Emergency Response (S-60) shall:
- A. Coordinate with M-40 to ensure all counterintelligence aspects of facility security plans and programs, specifically those related to protecting DOT from espionage, sabotage, and subversion, are carefully monitored. Coordinate with FAA to ensure all counterintelligence aspects of their facility security plans and programs, specifically those related to protecting the FAA from espionage, sabotage and subversion, are carefully monitored.
 - B. Establish, maintain and monitor an information sharing program among the OAs, M-40 and Secretarial Offices concerning threats, vulnerabilities and consequences.
4. Chief Information Officer (S-80) shall:
- A. Coordinate and provide guidance to M-40, OAs and Secretarial Offices to identify and mitigate risks associated with information technology assets, including Critical Infrastructure and Key Resources (CIKR) housed within DOT facilities. Additionally, coordinate with these DOT components as required by NIST P 800-116, HSPD-12 and DOT Order 1681.1 regarding risk assessments for PIV physical access controls and the requirements for implementing such systems in DOT owned and leased facilities.

- B. Coordinate with M-40 in developing and providing policy and guidance to OAs and Secretarial Offices in the implementation of HSPD-12/ICAM requirements that pertain to the physical security of DOT facilities.

5. Operating Administrations (except FAA) shall:

- A. Establish a Facility Protection Program consistent with the policies promulgated in this Order and any supplementary facility protection policies and procedures issued by the Office of the Assistant Secretary for Administration (M-1) and M-40.
- B. Appoint a Federal employee to serve as their organization's Security Coordinator. This individual shall be a senior level manager and have the authority to make decisions and speak on behalf of his/her organization on all matters related to the physical security of the OA's facilities and personnel located in field and regional offices as well as in the DOT headquarters facilities in Washington, DC. Due to circumstances that may require time sensitive critical decisions, this individual must have the authority to act on behalf of their administration's interests. A copy of each appointment letter shall be forwarded to the Director, M-40, no later than 30 days after the effective date of this Order and shall be updated annually or with the occurrence of personnel changes.

The OA shall make an appointment for the following position:

1) OA Security Coordinator (SC)

The OA SC shall:

- a. Upon appointment by the Head of the Operating Administration, serve as a liaison between the coordinator's organization and M-40, and assist M-40 and the organization in implementing the policies and guidance promulgated in this Order. When facility security issues are identified, the SC shall collaborate with M-40 personnel.
- b. Provide representation on the M-40 sponsored DOT Security Working Group. The OA's SC shall be the primary point of contact for passing information on security issues as well as policies/directives from the Interagency Security Committee.
- c. Ensure a Site Security Representative (SSR) is appointed at each OA ARR location. This appointment will generally be identified as an additional duty for the SSR. The SSR shall be the primary point of contact on security issues for these field offices. In facilities with minimal staffing, the SSR may be located at a Regional location with responsibilities for multiple smaller locations.

- d. Provide guidance and technical assistance to the SSR in order to address all protection issues at ARR facilities where the coordinator's organization is the primary tenant.
- e. Assist the organization to implement the risk management process outlined in the ISC references in this Order at all ARR facilities.
- f. Ensure through the SSR at ARR facilities where the OA is the primary tenant accomplishment of the following:
 - i) Identify the facility's baseline level of protection (LOP).
 - ii) Identify and assess the risks to the facility.
 - iii) Determine if the baseline LOP mitigates the assessed risks.
 - iv) Provide operating procedures for proposed countermeasures.
 - v) Provide a cost estimate for proposed countermeasures.
- g. Allocate and monitor funds that used for facility security protection within their OA.
- h. With support from M-40, determine the FSL for each of their ARR facilities. Prepare and submit an annual report to M-40 identifying the FSL for each facility. Conduct facility security assessments, fund, and implement security countermeasures required to mitigate security vulnerabilities at each facility the OA owns, direct leases, leases through GSA, or uses by another form of agreement.
- i. Maintain reports, files, and records concerning the implementation and management of the Facility Protection Program for all facilities in which the OA has a presence. The OA SC shall ensure all required reports and documentation from local Facility Protection Programs, including documentation of transmittal to the local security organization, are provided to M-40.
- j. Coordinate with M-40 prior to initial construction and/or significant modifications to any DOT facility. Coordination shall be made at the earliest stages of the proposed construction/modification and prior to issuance of a Statement of Work. Plans, project drawings, and specifications shall be reviewed during the entire construction/modification process.
- k. Coordinate with M-40 and S-80 for guidance with the implementation of HSPD-12/ICAM physical security requirements within DOT facilities.

- l. Coordinate with M-40 prior to issuance of new or revised policies that implement the organization's Facilities Protection Program.
- m. Ensure a sufficient number of qualified personnel are appointed to implement and manage the Facilities Protection Program within their organization.
- n. Ensure personnel assigned duties associated with the implementation of the Facilities Protection Program receive proper training, including refresher training as necessary, so that they have the skills and knowledge necessary to effectively implement policies and procedures for the protection of Federal facilities and personnel. Consult with M-40 as necessary regarding training opportunities.
- o. Ensure performance appraisals of all employees whose duties involve the management and implementation of the Facilities Protection Program include this function as a performance measure.
- p. Support the establishment of a Facility Security Committee (FSC) in a multi-tenant facility where the OA is a tenant. The Security Coordinator shall provide guidance and assistance to the OA representative appointed to the local FSC. GSA-leased offices located in a commercial building may require modification to the lease in order to fulfill this FSC requirement. If modifying the lease to accomplish this requirement is necessary, the modification shall be done as soon as is practical but no later than the next regularly scheduled lease renewal. In those locations where the OA is the primary tenant, the senior on-site OA official shall be designated the FSC chairperson. In those locations, the Security Coordinator shall provide guidance and assistance to the chairperson.

Where required, the OA SC shall make appointments for the following two positions.

i) Facility Security Committee Chairperson

The FSC Chairperson shall:

- (a) Follow guidance provided in appropriate ISC directives, by their assigned OA and from M-40.
- (b) Be familiar with the ISC document entitled "Facility Security Committees, An Interagency Security Committee Standard", as issued in June 2009, and any subsequent revisions or other ISC policies pertaining to FSCs.
- (c) Convene, schedule and draft the agenda for all FSC meetings. Meetings shall be held in accordance with ISC guidelines.

- (d) Document and distribute to committee members the minutes of all FSC meetings.
- (e) Maintain all FSC records.
- (f) Coordinate as necessary any interaction with outside organizations.
- (g) Assign tasks to FSC members for drafting of plans and other facility protection activities.
- (h) Serve as the point of contact for the FSC between meetings.
- (i) Call for votes on issues before the FSC.
- (j) Represent and cast votes on behalf of his or her organization.
- (k) Consult as necessary with his or her Security Coordinator and/or M-40 on matters before the FSC.
- (l) Provide an annual report to M-40 summarizing the efforts of the FSC.

ii) Facility Security Committee Representative

The FSC Representative shall:

- (a) Follow guidance provided in appropriate ISC directives and from M-40.
- (b) Represent the interests and cast votes on behalf of his or her organization.
- (c) Attend the facility's FSC meetings as scheduled by the FSC chairperson.
- (d) Cast votes on agenda items that have been designated by the FSC as decision items.
- (e) Be familiar with the ISC document entitled "Facility Security Committees, An Interagency Security Committee Standard", as issued in June 2009, and any subsequent revisions or other ISC policies pertaining to FSCs.
- (f) Consult as necessary with his or her Security Coordinator and/or M-40 on matters before the FSC.

CHAPTER 5 -- DOT FACILITIES PROTECTION PROGRAM

1. GOALS

The goals of the DOT Facilities Protection Program are as follows:

- A. Create a long term Facilities Protection Program. The guidance contained in this Order shall be observed as more than simply a singular event. The goal of this Order is to present and implement principles of long term risk management with respect to facility protection within the Government Facilities Sector. DOT can achieve a successful and enduring Facilities Protection Program by:
 - 1) Highlighting an awareness of facility protection throughout DOT and its Operating Administrations.
 - 2) Utilizing education, training, and exercise programs in the administration of facility security.
 - 3) Pursuing research and development initiatives, as well as the use of new and emerging technologies, to improve the protective capabilities of DOT facilities.
 - 4) Developing data systems and continuous improvement processes in order to continually refine the risk management process.
 - 5) Collaborating with other Federal departments and agencies (e.g., through interagency committees and working groups) on physical security issues impacting the Government Facilities Sector.
- B. Foster collaboration among all DOT organizations in order to ensure DOT has a comprehensive facilities protection plan.
- C. Integrate facility protection with DOT's mission statement.
- D. Implement a risk management process that will create a system of identifying and mitigating risks.
- E. Use DOT resources as efficiently as possible to address countermeasures necessary for the LOP. DOT shall achieve efficiency by implementing:
 - 1) Resource management techniques
 - 2) Resource allocation techniques
 - 3) Risk management techniques
 - 4) Performance measurement techniques

2. RISK MANAGEMENT BACKGROUND

Risk management is a comprehensive approach to allocating resources for the protection of a facility, assets, and occupants to achieve an acceptable level of risk. Risk management decisions are based on the application of risk assessment, risk mitigation, and when necessary, risk acceptance. References identified in this Order provide guidance on the usage of a risk management process, as mandated by the ISC for DOT to use in protecting its facilities. The NIPP and the GFSSP provide the outline for an effective risk management process. Specifically, the following six activities are included in the GFSSP's risk management framework which is hereby incorporated into DOT's Facilities Protection Program:

A. Set Goals and Objectives

Define specific outcomes, conditions, end points or performance targets that will result in an enhanced state of protection of facilities.

B. Identify Assets, Systems, and Networks

Determine and identify elements of the Government Facilities Sector (GFS) that, if damaged, will negatively impact the defense, economy, health, safety or psyche of the Nation.

C. Assess Risks

Risk assessment is a step within the risk management process. Risk assessment includes: identifying potential threats, recognizing vulnerabilities that exist on the facility site, and evaluating the consequences that could result from the execution of the potential threat. The results or risk assessments are used to provide reliable and comprehensive data to decision makers in their choice of risk mitigation procedures.

D. Prioritize

The process of prioritization involves aggregating and analyzing the risk assessment results. This process identifies the areas that face the highest risk and criticality to the mission. Assets will be categorized as low, medium, high, or critical. This prioritization will assist all responsible DOT entities in the planning, management, and resource allocation of risk mitigation tools.

E. Implement Programs

Program implementation is the means by which the risk to facilities is mitigated. Protective programs include methods that deter threats, reduce vulnerabilities, and minimize consequences.

F. Measure Effectiveness

The final step in the risk management framework is to measure the performance of protective programs over time. By measuring the progress of protective programs results can be quantified, and feedback can be provided in order to improve program activities and assist in new resource allocation determinations. This final step of measuring progress leads directly into the risk management feedback loop so as to achieve continuous improvement to enhance the protection of the nation's CIKR.

These risk management guidelines are documented in both the NIPP and GFSSP, and the ISC has used them in establishing a specialized risk management process for the physical security of all Federal facilities.

ASSISTANT SECRETARY FOR ADMINISTRATION


Signature


Date

APPENDIX A: Terms and Definitions

The definitions provided below are derived primarily from Interagency Security Committee (ISC) publications.

Administrative, Regulatory and Research (ARR) Facility: A dedicated facility responsible for day-to-day administrative, regulatory and research functions. It is NOT an operational facility that is part of the Nation's transportation infrastructure. For purposes of this Order, protection guidelines for ARR facilities are derived from the Government Facilities Sector of the National Infrastructure Protection Plan.

Baseline Level of Protection (LOP): The set of physical security measures identified in this document for each FSL which must be implemented unless a deviation (up or down) is justified by a risk assessment.

Building: An enclosed structure (above or below grade).

Campus: Two or more Federal facilities located on one site and typically sharing some aspects of the environment, such as parking, courtyards, private vehicle access roads, or gates and entrances to connected buildings. A campus may also be referred to as a "Federal center" or "complex."

Consequence: The level, duration, and nature of the loss resulting from an undesirable event.

Customized LOP: The set of physical security measures deviating from the baseline LOP, developed as the result of the risk-based analytical process.

Existing Facility: A facility that has already been constructed or for which the design and construction effort has reached a stage where design changes may be cost prohibitive.

Facility: Space built or established to serve a particular purpose. The facility is inclusive of a building or suite and associated support infrastructure (e.g., parking or utilities) and land.

Facility Security Committee (FSC): A committee consisting of representatives of all Federal tenants in the facility, generally responsible for addressing building-specific security issues and approving the implementation of security measures and practices. In the case of new construction or pending lease actions, the FSC will consist of the local security organization, the design team, and the planned tenants. The FSC was formerly known as the Building Security Committee.

Facility Security Level (FSL): A categorization based on the analysis of several security-related facility factors, which serves as the basis for the implementation of physical security measures specified in ISC standards.

Federal Departments and Agencies: Those executive departments enumerated in 5 U.S.C. 101 and DHS, independent establishments as defined by 5 U.S.C. 104(1), Government corporations as defined by 5 U.S.C. 103(1), and the U.S. Postal Service.

Federal Facilities: Leased and owned facilities in the United States (inclusive of its territories) occupied by executive branch Federal employees for nonmilitary activities.

Federal Protective Service (FPS): FPS is responsible for providing security and law enforcement services to Federal buildings owned or leased by the General Services Administration (GSA), as well as to other properties, as authorized, where security is not provided by other means.

Interagency Security Committee (ISC): The ISC is a Federal Government committee established by E.O. 12977 dated October 19, 1995. The ISC is comprised of 21 primary member agencies and over 80 associate member agencies. The ISC is responsible for the development of physical security policies and standards for the protection of all Federal facilities excluding the Department of Defense. DOT is a member agency of the ISC.

Level of Protection (LOP): The degree of security provided by a particular countermeasure. Levels of protection used in this Standard are Minimum, Low, Moderate, High, and Very High.

Level of Risk: The combined measure of the threat, vulnerability, and consequences posed to a facility from a specified undesirable event.

Major Modernization: The comprehensive replacement or restoration of virtually all major systems, tenant-related interior work (such as ceilings, partitions, doors, floor finishes, etc.), and building elements and features.

Multi-Tenant Facility: A facility that includes tenants from multiple Federal departments and agencies but no non-Federal tenants.

Mixed-Multi-Tenant Facility: A facility that includes tenants from multiple Federal departments and agencies as well as one or more non-Federal tenants.

Mixed-Tenant Facility: A facility that includes one Federal tenant as well as non-Federal tenants, including commercial and State/local government tenants.

Occupant: A Federal employee or Federal contract employee who is permanently or regularly assigned to the building and displays the required identification badge/pass.

Operational Facility: A dedicated facility responsible for the day-to-day operation of a particular asset or system (i.e. Metro Transit station). For purposes of this Order, protection guidelines for these facilities are derived from the Transportation Sector of the National Infrastructure Protection Plan.

Risk: A measure of potential harm from an undesirable event that encompasses threat, vulnerability, and consequence.

Risk Acceptance: The explicit or implicit decision not to take an action that would affect all or part of a particular risk.

Risk Assessment: The process of evaluating credible threats, identifying vulnerabilities, and assessing consequences.

Risk Management: A comprehensive approach to allocating resources for the protection of a facility to achieve an acceptable level of risk. Risk management decisions are based on the application of risk assessment, risk mitigation, and—when necessary—risk acceptance.

Risk Mitigation: The application of strategies and countermeasures to reduce the threat of, vulnerability to, or consequences from an undesirable event.

Security Coordinator: This individual shall be a senior level manager appointed by the OA and has the authority to make decisions and speak on behalf of his or her organization on all matters related to the physical security of their facilities and personnel located in field and regional offices as well as the DOT headquarters facilities in Washington, DC. Due to circumstances that may require time sensitive critical decisions, these individuals must have the authority to act on behalf of their administration's or office's interests.

Security Organization: The Government agency or an internal agency responsible for providing security services to a particular DOT facility. In a multi-Tenant facility, the security organization may be from another Federal entity.

Suite: One or more contiguous rooms occupied as a unit.

Threat: The intention and capability of an adversary to initiate an undesirable event.

Undesirable Event: An incident that has an adverse impact on the operation of the facility or mission of the Agency.

Vulnerability: A weakness in the design or operation of a facility that an adversary can exploit.

APPENDIX B: Acronyms

The following acronyms are used in this Order:

ARR – Administrative, Regulatory and Research

CIKR – Critical Infrastructure and Key Resources

COMSEC – Communication Security

DHS – Department of Homeland Security

DOT – Department of Transportation

E.O. – Executive Order

FAA – Federal Aviation Administration

FOUO – For Official Use Only

FPS – Federal Protective Service

FSC – Facility Security Committee

FSL – Facility Security Level

GFSSP – Government Facilities Sector Specific Plan

HSPD – Homeland Security Presidential Directive

ICAM – Identity, Credential and Access Management

ICD – Intelligence Community Directive

ICS – Intelligence Community Standard

ISC – Interagency Security Committee

LOP – Level of Protection

M-1 – DOT's Office of the Assistant Administrator for Administration

M-40 – DOT's Office of Security

NIPP – National Infrastructure Protection Plan

NIST – National Institute of Standards and Technology

OA – Operating Administration

PIV – Personal Identity Verification

S-60 – DOT's Office of Intelligence, Security, and Emergency Preparedness

SCIF – Sensitive Compartmented Information Facility

SEFC – Southeast Federal Center

SME – Subject Matter Expert

SSP – Sector Specific Plan

U.S.C. – U.S. Code