Department of the Interior
Departmental Manual

Effective Date: 08/13/2013
Series: Law Enforcement and Security
Part 444: Physical Protection and Building Security
Chapter 1: Physical Security Program Requirements

Originating Office: Office of Law Enforcement and Security

444 DM 1

1.1 **Purpose**. This chapter establishes the minimum physical security requirements necessary to safeguard Department of the Interior (DOI) personnel, resources, and facilities. Related policies are provided in the following Parts of the Departmental Manual (DM):

A. 444 DM 2 - DOI National Critical Infrastructures and Key Resources.

B. 352 DM 10 – Aircraft and Aviation Facility Security.

C. 441 DM - Personnel Security and Suitability.

D. 442 DM - Classified National Security Information Program.

E. 375 DM 19 - Information Security Program.

1.2 **Scope.** This policy applies to all DOI bureaus and offices. It is applicable to all structures, buildings, dams, grounds, real property, and/or office space (hereafter referred to as facilities) occupied by a DOI bureau/office component, whether owned, leased, or controlled by DOI and it applies to all persons entering in or on such property.

1.3 **Authorities**.

A. *Federal Security Level Determinations for Federal Facilities – An Interagency Security Committee Standard*. On March 10, 2008, the Department of Homeland Security (DHS), Interagency Security Committee (ISC) issued the standard for determining the appropriate level of security at Government facilities. It defines the criteria and process to be used in determining the Facility Security Level (FSL) of a Federal facility, and includes a categorization that serves as the basis for implementing protective measures.

B. *Physical Security Criteria for Federal Facilities – An Interagency Security Committee Standard*. On April 12, 2010, the DHS ISC issued the standard for determining the minimum security requirement at each Federal facility. This document establishes a baseline set of physical security measures to be applied to all Federal facilities at each Facility Security Level. These minimum requirements replace the recommended minimum security standards

contained in the U.S. Department of Justice study entitled, *Vulnerability Assessment of Federal Facilities*, that was implemented for all Federal facilities by Presidential Memorandum, dated June 28, 1995. The DOI has adopted the minimum security standards as reflected in the ISC document *Physical Security Criteria for Federal Facilities;* and these standards should be adhered to by all bureaus/offices.

C. Federal Management Regulations Part 102-81 (Security) and the regulations published in 41 CFR 101-20. As applicable, the ISC requirements supplement Title 41- Public Contracts and Property Management, Chapter 101-20 Federal Property Management Regulations, Management of Buildings and Grounds, which prescribes security standards for buildings and grounds under the assignment responsibility of the General Services Administration (GSA). Nothing in this chapter alters or minimizes the requirements for information resource security as prescribed by 375 DM 19, Information Technology Program, or any other requirement established by law or other authority.

1.4 **Definitions**.

A. Security Plan. A written document describing the practices, procedures, responsibilities, and equipment that provide for the security of assets/facilities. A security plan may be a stand-alone document, or it may be part of Standard Operating Procedures, Emergency Action Plans, or similar documents, as appropriate for the facility.

B. Consequence. Loss based on population at risk, economic impact, mission impact, symbolic value, national security impact, interdependencies, and public behavioral impact.

C. Critical Infrastructure. Systems and assets, whether physical or virtual, so vital to the bureau/office mission that the incapacity or destruction of such systems or assets would have a debilitating impact on daily operations, economic security, public health or safety, or any combination thereof.

D. Facility. Structures, buildings, dams, grounds, real property, and/or office space occupied by a DOI component whether owned, leased, or controlled by DOI.

E. Mitigation. Activities and/or systems designed to reduce or eliminate risks to persons or property or to lessen the actual or potential effects or consequences of an incident. Mitigation measures may be implemented prior to, during, or after an incident, and are often developed in accordance with lessons learned from prior incidents.

F. Physical Access Control System. A Physical Access Control System (PACS) is used to control both routine employee and visitor access to Federal campuses, facilities, and controlled interior facilities. Federal Identity, Credential, & Access Management (FICAM) compliant physical access control systems leverage identities, credentials, and privileges to determine an individual's access rights to facilities.

G. Physical Protection System. An integrated system of detection, delay, and response.

(1) Detection. Appropriate law enforcement/security force is notified as soon as possible after a security incident occurs.

(2) Delay. A combination of the security force and physical attributes designed to slow an incident in order to provide an effective response time.

(3) Response. Interdicting and neutralizing the incident; thus, eliminating the immediate threat.

H. Physical Security. Measures that prevent or deter the overall risk to DOI assets, systems, networks, or their interconnecting links resulting from exposure, injury, destruction, incapacitation, or exploitation. Physical security includes actions to deter the threat, mitigate vulnerabilities, or minimize consequences associated with a terrorist attack or other incident. These measures can include a wide range of activities, such as hardening facilities, building resiliency and redundancy, incorporating hazard resistance into initial facility design, initiating active or passive countermeasures, installing security systems, promoting workforce security, and implementing cyber security measures, among various others.

I. Security Assessments. An evaluation of assets or facilities that includes an analysis of the security and physical protection conditions at an asset/facility in order to identify gaps and overall resiliency to specific hazards.

J. Risk. The relationship or coexistence between consequences, vulnerabilities, and threats.

K. Threat. An indication of possible violence, harm, or danger.

L. Vulnerability. The weakness or susceptibility in the physical protection system that could be exploited by an adversary or disrupted by a natural hazard.

1.5 **Responsibilities**.

A. Senior DOI Officials with administrative jurisdiction over a facility are responsible for safeguarding personnel as well as real and personal property under the control of, or assigned to, the facility.

B. Heads of Bureaus/Offices are responsible for:

(1) Implementing, maintaining, and monitoring the security program and procedures; and ensuring that resources are available to protect the personnel, structure, operation, and contents of facilities under their administrative control in accordance with the security requirements contained in this chapter.

(2) Ensuring bureau/office specific physical security reviews and compliance

program policies are developed and implemented.

(3) Designating in writing a trained bureau/office physical security professional (hereafter referred to as the Security Manager/Officer) to perform the duties and responsibilities outlined in paragraph 1.5D. All security managers/officers must complete security training at the Federal Law Enforcement Training Center (FLETC) or complete another accredited Security Manager Course at another institution. The following bureaus/offices are required to designate a full time Security Manager/Officer:

(a) Bureau of Indian Affairs

(b) Bureau of Land Management

(c) Bureau of Ocean Energy Management

(d) Bureau of Safety and Environmental Enforcement

(e) Bureau of Reclamation

(f) National Park Service

(g) Office of Surface Mining

(h) U. S. Fish and Wildlife Service

(i) U. S Geological Survey

C. Office of Law Enforcement and Security (OLES), as referenced in 112 DM 17, is responsible for:

(1) Establishing and disseminating security policy.

(2) Supporting the development of bureau/office programs related to personnel security and suitability, national security, industrial security, and physical security.

(3) Coordinating the activities of bureaus/offices for implementation of the National Infrastructure Protection Plan.

(4) Conducting security assessments of DOI's facilities, including critical infrastructure and key resources.

(5) Acting as the DOI representative for all external agencies regarding security issues.

(6) Developing policies related to the use of physical access control systems.

D. Security Managers/Officers are responsible for ensuring oversight and/or coordination of the bureau/office Security Program which includes:

(1) Safeguarding bureau/office personnel, contractors, and visitors.

(2) Securing bureau/office facilities and personal property.

(3) Complying with the requirements set forth in the OLES document titled "Security Manager Training Requirements and Recommendations." Security Managers/Officers (regardless of prior experience) are required to complete 40 hours of annual security related training.

(4) Representing the bureau/office at all DOI Security Advisory Council (SAC) meetings.

(5) Maintaining at least a Top-Secret Security Clearance.

(6) Representing the bureau/office and ensuring compliance with the DHS, Homeland Security Presidential Directive (HSPD) 7 (Critical Infrastructure Identification, Prioritization, and Protection) sector requirements.

(7) Overseeing and/or maintaining a liaison with the bureau/office Personnel Security and Suitability Program (441 DM); Classified National Security Information Program (442 DM); and Industrial Security Program (443 DM).

(8) Overseeing and coordinating all areas of the bureau/office Physical Protection and Facility Security Program in accordance with 444 DM.

(9) Maintaining oversight, coordination and/or a liaison with bureau/office designated Regional and/or Site Security Managers.

(10) Maintaining a liaison with the bureau/office Emergency Management Program (900 DM).

(11) Maintaining a liaison with the bureau/office Information Resources Management Program (375 DM).

(12) Maintaining a liaison with the bureau/office facilities management program for a current list of all facilities occupied by bureau/office personnel, related security assessments, and security level (see paragraph 1.6).

(13) Ensuring that security assessments on DOI and non-GSA operated facilities are conducted and updated. Coordinating with the facilities management staff to ensure implementation of measures designed to mitigate vulnerabilities discovered.

(14) Obtaining, if available, through the Facility Security Committee (FSC) and maintaining within the bureau/office, current security assessments of GSA facilities occupied by bureau/office personnel.

(15) Reviewing the physical security requirements with the bureau/office facilities management staff to ensure that necessary safeguards are included in new design and construction.

(16) Ensuring compliance with physical access control system policies.

(17) Collaborating with OLES on security assessments and providing those assessments to OLES upon request.

(18) Collaborating with OLES on security related budgets.

(19) Providing support as needed to OLES personnel conducting security assessments at DOI facilities.

(20) Ensuring that the protective measures identified in this chapter are the minimum actions to be taken by bureaus/offices in space that is owned, leased, or controlled by DOI. Each bureau/office or other organizational component is responsible for complying with the minimum actions and for developing specific security measures based on the types of risks associated with the facilities occupied and the programs and activities carried out at the facility (mission criticality).

E. Managers of DOI Bureaus/Offices or Other Organizational Components will develop additional security measures, as deemed appropriate. In space that is owned or leased by the GSA, DOI bureau/offices or other organization components will rely on minimum DHS/ISC issued guidance and protective measures when developing additional security measures and will at a minimum:

(a) Designate one or more individuals to be active members of the FSC.

(b) Designate one or more individuals as the point of contact to receive threat and security information from GSA or other viable sources. The individuals designated should be available on a full-time basis.

(c) Ensure that a current Occupant Emergency Plan (OEP) is developed and maintained in accordance with 900 DM 1.6.J. In buildings with multiple tenants, DOI may be a partner in the overall OEP for the building. In smaller buildings or those without multiple Federal tenants, DOI bureaus/offices or other organization components must develop and maintain their own OEP.

(d) Establish a notification system to ensure that appropriate personnel are advised of changes in protective measures and threat information affecting the facility.

(e) Develop a viable process for informing employees, volunteers, cooperators/partners, concessioners, and contractors of their security responsibilities.

(f) Ensure that each bureau/office employee and volunteer is notified of his/her responsibility to comply with the provisions of the DOI Security Program. In addition, notify employees and volunteers that they are also responsible for compliance with any additional directives developed by their respective bureau/office Security Manager/Officer.

1.6 **Security Assessments**. Security assessments will be conducted to identify vulnerabilities, develop countermeasures and evaluate the appropriate security safeguards. Assessments will be conducted by the Security Manager/Officer, and/or designee, at sites occupied by bureau/office employees; and may include those sites administered by GSA or another Federal entity. The OLES may conduct an independent security assessment at any facility. Security assessments will conform to the following requirements:

A. Bureaus/offices, at a minimum, will utilize the Interagency Security Committee (ISC) document titled, *"Facility Security Level Determinations for Federal Facilities"and "Physical Security Criteria for Federal Facilities – An Interagency Security Committee Standard,"* as a minimum guideline for the physical security assessment required at each facility.

B. Security assessment reports and security plans (refer to paragraph 1.7) will be created and maintained by the bureau/office in accordance with the General Records Schedule 18. These reports will be made available to OLES upon request.

C. Each security assessment will be conducted at least every 5 years for Federal Security (FSL) Level I and II facilities, and at least every 3 years for FSL III and IV facilities. (Refer to the *Federal Security Level Determinations for Federal Facilities – An Interagency Security Committee Standard,* in determining the FSL for DOI occupied facilities).

D. The bureau/office Security Manager/Officer will track and document actions taken to implement recommendations.

E. Security assessments should begin during the initial planning stage of new design or construction. The bureau/office Security Manager/Officer or designee will review physical security requirements with the designated bureau/office project manager to ensure compliance with the security program standards.

F. Prior to occupying a new facility, the bureau/office Security Manager/Officer or designee will ensure that a security assessment is conducted in coordination with the designated bureau/office project manager.

G. When a security assessment of a DOI occupied facility is conducted by another agency, the bureau/office Security Manager/Officer will obtain copies of all related documentation.

H. Security assessments will be conducted prior to completing a security plan. (Refer to paragraph 1.7.)

1.7 **Security Plan.** Bureau/office Security Mangers/Officers or designees are responsible for developing, implementing, and maintaining security plans for facilities under their administrative control in coordination with the bureau/office facilities management staff. Security plans will be reviewed and revised as necessary to ensure that they accurately reflect current threat conditions. Security Plans will address the following:

A. The impact of a partial or complete loss of a facility on the bureau/office mission and functions.

B. How each security requirement contained in the document entitled, "*Physical Security Criteria for Federal Facilities,*" is implemented at a specific facility. If a requirement is not applicable or feasible, then a written explanation detailing the reason for the deviation shall be documented.

C. Protective measures to be implemented at the facility under elevated threat conditions.

D. If vulnerabilities identified in a security assessment exist, a statement on how they will be mitigated must be provided or the person accepting the risk posed by the vulnerabilities must be identified.

1.8 **OLES Security Assessments**. As provided in 112 DM 17, the OLES Security Division is authorized to conduct security assessments on all DOI facilities including critical infrastructure and key resources. These security assessments are conducted to assist bureaus/offices in determining effectiveness of physical security safeguards in place at DOI facilities. At the conclusion of the evaluation, the senior official will be provided a written report of findings with recommended remedial and/or mitigating measures.

1.9 **Security Requirements**. The minimum physical security requirements for DOI facilities are contained in the ISC document titled, "*Physical Security Criteria for Federal Facilities – An Interagency Security Committee Standard.*" Bureaus/offices may increase security measures based on local circumstances, changes in the threat condition, and/or other indicators that necessitate a need for increased security. Implementation of any security requirement contained in this chapter should be contingent upon the findings of a security assessment. If a requirement is not applicable or feasible at a facility, then a written explanation detailing the reasons for the deviation shall be documented by the bureau/office Security Manager/Officer, in consultation with Facilities Management staff.

1.10 **Occupant Emergency Program**. In accordance with Federal Management Regulations (41 CFR 102-74.230) and 900 DM 1.6J, the Designated Senior Official at each facility is responsible for developing, implementing, and maintaining an OEP. The official's responsibilities include, but are not limited to, providing OEP program policy guidance, reviewing the OEP annually, and training personnel.

1.11 **General Services Administration (GSA) Guidelines for Conduct on Federal Property (Part 102-74, Subchapter C-Real Property, Subpart C)**. The rules referenced in this subpart have been adopted by DOI and apply to all property under the authority of GSA (hereinafter referred to as "property") and to all persons entering in or on such property. The following is a summary of the guidelines applicable to this DM chapter.

A. Inspection. Packages, briefcases, and other containers in the immediate possession of visitors, employees, or other persons arriving on, working at, visiting, or departing from Federal buildings and grounds, are subject to reasonable inspection.

B. Admission to Property. Property will be closed to the public during non-normal business hours. The closing of property will not apply to any space where after-normal business hours use/access has been approved by a designated official. Admission to property after normal business hours will be restricted to authorized persons who will register upon entry to the property and display Government or other identifying credentials to security personnel when entering, leaving, or while on the property. In addition, after approval by a designated official, authorized persons may provide after-hours escort for non-employees.

C. Preservation of Property. The improper disposal of rubbish on property; willful destruction of or damage to property; theft of property; creation of any hazard on property to persons or things; throwing of articles of any kind from or at a building or climbing upon statues, fountains, or any part of the building, is prohibited. Applicable Federal, state, and local laws and regulations also apply.

D. Conformity with Official Signs and Directions. Persons in or on the property will comply with prohibitions, regulations, or directions posted on official signs; and with the lawful direction of security personnel.

E. Disturbances. Any loitering, disorderly conduct, or other conduct on property that creates loud or unusual noise or a nuisance; that unreasonably obstructs the usual use of entrances, foyers, lobbies, corridors, offices, elevators, stairways, or parking lots; that otherwise impedes or disrupts the performance of official duties by Federal Government employees; or that prevents the general public from obtaining the services provided on the property in a timely manner, is prohibited.

F. Alcoholic Beverages and Narcotics. Operation of a motor vehicle, while on the property, by a person under the influence of alcoholic beverages or drugs is prohibited.

(1) Entering upon or occupying the property while under the influence of or during the use or possession of any illegal/controlled drug is prohibited. The prohibition will not apply in cases where the drug is being used/possessed in accordance with a prescription issued by a licensed physician.

(2) Entering upon or occupying the property under the influence of or during the use of alcoholic beverages is prohibited. The use of alcoholic beverages on the property is

prohibited, except as provided in 41 CFR 101-20.307.

G. Dogs and Other Animals. Dogs and other animals, except service dogs, law enforcement dogs, and animals used to guide or assist disabled persons, will not be brought on the property for other than official purposes.

H. Vehicular and Pedestrian Traffic.

(1) Drivers of vehicles entering and/or while on the property will drive in a careful and safe manner and will comply with signals, posted traffic signs, and directions of law enforcement and security personnel.

(2) The blocking of entrances, driveways, walkways, loading platforms, and fire hydrants on the property is prohibited.

(3) Except in emergencies, parking on the property is not allowed without a permit. Parking without authority, parking in unauthorized locations or in locations reserved for other persons, or parking contrary to the direction of posted signs is prohibited. Vehicles parked in violation may be subject to removal at the owners' risk and expense.

I. Explosives. No person entering and/or while on the property will carry or possess explosives, or items intended to be used to fabricate an explosive or incendiary device, either openly or concealed, except for official purposes.

J. Firearms. Unauthorized possession or transportation of firearms or other dangerous weapons in a DOI facility is prohibited and is a violation of Federal law. The carrying of firearms by anyone other than authorized individuals is prohibited. (Reference Title 18, U.S.C. 930.)

K. Removal of Government Property. Procedures should be established at DOI facilities to control the removal of Government property.

L. Violence in the Workplace. Violence and threatening behavior in the Federal workplace is prohibited. This includes any behavior that is harassing, intimidating, provoking, or unsafe which could be interpreted as intent or threat to cause physical harm to another individual or damage to property.