NIH Policy Manual

1381 - Physical Security Project Requirements for NIH Owned and Leased Facilities

Issuing Office: OD/OM/ORS/SER/DPSM **Phone:** (301) 443-7287

Issuing Office Email: dpsm-servicerequest@mail.nih.gov

Approving Official(s): CIO

Release Date: 10/01/2021 ?

Transmittal Notice

1. **Explanation of Material Transmitted:** This chapter is revised to update the policy, procedures and organizational responsibilities to ensure compliance with updates to applicable federal security standards and guidelines for construction, renovation, lease acquisition and major equipment installation projects affecting active and passive security systems at all National Institutes of Health (NIH) owned and leased facilities.
2. **Filing Instructions:**

   Remove: NIH Manual Issuance 1381; Dated: 07/24/2014.
   Insert:NIH Manual Issuance 1381; Dated: 10/01/2020.

PLEASE NOTE: For information on:

- Content of this chapter, contact the issuing office listed above.
- NIH Policy Manual, contact the Division of Compliance Management, OMA, or by telephone at (301) 496-4606.

A. Purpose

This Manual Chapter ensures all National Institutes of Health (NIH) owned or leased facilities are designed, constructed, improved, renovated, and/or maintained in compliance with all applicable federal physical security requirements. This chapter serves as the basis for the NIH Physical Security Project Requirements for NIH Owned and Leased Facilities. This policy also establishes the authority of the Division of Physical Security Management (DPSM) as the NIH organization responsible for ensuring physical security countermeasures are designed and implemented to protect personnel and property from damage or harm from terrorism, criminal activity, and threats by individuals or groups.

B. Scope

This Manual Chapter is applicable to all NIH owned or leased facilities.

C. Background

On October 19, 1995, six months after the Oklahoma City bombing of the Alfred P. Murrah Federal Building, President Clinton issued Executive Order (EO) 12977, creating the Interagency Security Committee (ISC) to address continuing government-wide security for federal facilities. Prior to 1995, minimum physical security standards did not exist for nonmilitary federally owned or leased facilities. Following the September 11, 2001 terrorist attacks, the Department of Health and Human Services (HHS), Office of the Inspector General (OIG), conducted a comprehensive assessment of the NIH security operations and functions, including physical security policies, procedures and protective systems.

In response to the OIG report, the NIH Associate Director of Security and Emergency Response (ADSER) expanded existing security design guidelines and procedures to comply with increased federal mandates and threat levels. The security design guidelines and procedures are based on proven federal methodologies and best practices which provide the basis for the NIH Physical Security Program. As new threats emerge, the standards and guidelines included in the Reference Section of this chapter are subject to periodic updates.

The DPSM was established to ensure physical and engineering security initiatives at all NIH owned or leased facilities work in concert with the Office of Security and Emergency Response (SER) Divisions to provide the most secure environment for the NIH community. The DPSM mission is to ensure all NIH owned or leased facilities are protected against current and emerging threats by balancing high-quality, cost-efficient security systems and operations with federal mandates. In collaboration with the NIH community, DPSM strives to achieve optimum results for a safe environment that does not restrict but promotes the mission and goals of the NIH.

To accomplish this goal, DPSM applies the Interagency Security Committee (ISC) Risk Management Process (RMP) per EO 12977, and other federal security policies and standards.

D. Policy

This policy defines how physical security countermeasures and requirements are developed and implemented for all NIH owned and leased facilities. Additionally, this policy establishes a process to identify and obtain DPSM’s approval of the physical security requirements for alteration, construction, improvement, renovation, repair by replacement and/or major equipment installation projects taking place in NIH owned and leased facilities. This policy will ensure federally mandated physical security requirements are met and risks are mitigated.

Any NIH organization planning an alteration, construction, improvement, renovation, repair

by replacement and/or major equipment installation at NIH owned or leased facilities must coordinate such project activities with the Office of Research Facilities Development and Operations (ORFDO). To avoid incurring unplanned project cost and schedule impacts, ORFDO Project Officers (POs) must consult with DPSM as early as possible during the initial project planning stages; otherwise, any cost-change impacts will be borne by the organization sponsoring and funding the overall project.

It is strictly prohibited to remove, modify, or tamper with any DPSM-approved security systems including, but not limited to, access control devices such as card readers, door intercoms with remote unlocking systems, biometric devices and secure locking systems, security lighting, electronic surveillance and video recording systems, intrusion detection and alarm systems, blast mitigation techniques, pedestrian and vehicle barriers, facility/perimeter protection measures and other specialized security systems. Otherwise, cost impacts to restore the security system to its intended function as defined by DPSM, will be borne by the organization sponsoring and funding the overall project.

All ORFDO maintenance personnel are required to inform DPSM of any intent to disconnect, relocate, disable, remove, or reinstall any physical security device. These devices have been strategically placed and optimized for their intended function and any manipulation of such equipment may compromise their integrity to protect the NIH community and/or programs. All physical security related questions, requests or communications must be submitted, via email, to **DPSM-ServiceRequest@mail.nih.gov**.

1. **Privacy Policy Regarding Systems**

Records identifying individuals entering and/or exiting NIH owned and leased facilities are subject to the Privacy Act, as these records contain personally identifiable information, stored in a paper or electronic record system, designed to be retrieved by the name of the subject individual, or a unique identifier, linked to or assigned to the individual by ORS, or another office (biometric information, photographic images). The records are covered by NIH System of Records Notice 09-25-0054, Administration: Property Accounting (Card Key System) HHS/NIH/ORS. All staff handling any records maintained in this record system must safeguard and protect the records in accordance with the Privacy Act SORN (https://www.hhs.gov/foia/privacy/sorns/index.html).

2. **General Services Administration (GSA) Leased Facilities**

The Federal Protective Service (FPS) oversees GSA leased facilities and is responsible for providing risk assessments and physical security requirements for such facilities. Upon request, DPSM may provide consultative support to a NIH customer on FPS physical security requirements and when NIH is renovating space under Contracting Officer Representative (COR) authority in a GSA lease. However, DPSM may review these recommendations and adjust or augment the physical security requirements for such facilities where appropriate, to ensure consistency with NIH mission and security standards; and may include facility design review process, systems assessment and commissioning. To ensure risk management strategies are EO 12977 compliant, and in accordance with the ISC RMP, DPSM will assist

the Institutes, Centers and Offices (ICOs) with establishing a Facility Security Committee at multi-tenant NIH leased facilities.

3. **Potentially Dangerous or Disruptive Tools**

Throughout the course of facility construction, renovation or maintenance activities, any tool which may be weaponized, or produce sounds which may be mistaken for a weapon, must receive written authorization through a permit application process prior to arrival and/or use of such tool(s) on any NIH owned or leased facilities. Such tools include, but are not limited to, explosive powder and power activated tools (i.e., cartridge-based tools, gas, air, electrical or other) that can propel a projectile. A copy of the approved permit must be presented for inspection prior to said tool(s) entering the facility and must accompany the tool(s) at all times while on the NIH premises. The permit template and instructions may be accessed on the NIH ORFDO intranet.

E. Responsibilities

1. **The Associate Director, Security and Emergency Response (ADSER)** is responsible for all day-to-day security functions at NIH, as well as the direct oversight and financial management of security planning and operations of NIH owned or leased facilities through consultation and coordination with NIH ICOs and NIH Leadership. The ADSER's security responsibilities are implemented through the SER subordinate organizations:

    - Division of the Fire Marshal (DFM)
    - Division of Police (DP)
    - Division of Fire and Rescue Services (DFRS)
    - Division of Emergency Management (DEM)
    - Division of Personnel Security and Access Control (DPSAC)
    - Division of Physical Security Management (DPSM)

    In collaboration with NIH Leadership and the Director of DPSM, the ADSER maintains authority for all physical security matters requiring final determination with regard to NIH owned or single tenant leased facilities.

2. **The Director, Division of Physical Security Management (DPSM)** ensures all NIH owned or leased facilities comply with federally mandated physical security requirements and approved security systems that mitigate current and emerging threats. Physical security systems include, but are not limited to, access control devices such as card readers, biometric devices and secure locking systems, security lighting and video surveillance systems, intrusion detection and alarm systems, blast mitigation countermeasures, pedestrian and vehicle barriers, facility/perimeter protection measures, and other specialized security systems. The Director, DPSM will:

    a. establish and maintain all NIH physical security related policies and guidelines;

b. ensure new construction and renovation projects are in compliance with NIH physical security related policies and guidelines and other applicable federal physical security policies and requirements;
c. provide recommendations and cost-saving strategies to enhance the overall security in the absence of clearly defined federal requirements;
d. coordinate and consult with applicable representatives of the ORFDO and ICOs to identify physical security program requirements;
e. ensure appropriate DPSM staff participation in ORFDO's Pre-Project Planning Board (PPPB) and Project Definition Rating Index (PDRI) meetings to identify and incorporate physical security requirements into the scope of a project (i.e., Basis of Design [BOD], Bridging Documents, Facility Project Approval Agreement [FPAA], Program of Requirements [POR], etc.);
f. develop and maintain Facility Security Assessments (FSA) in accordance with federal policies and standards, and present recommended ISC RMP-based risk mitigating countermeasures to the appropriate stakeholders;
g. approve physical security requirements for new construction and renovation projects from the planning/design phase through the commissioning;
h. ensure appropriate DPSM staff participation in reviewing master plans, site improvements, statements/scopes of work, and submittals for construction, renovation or major equipment installation projects;
i. conduct security assessments and systems troubleshooting as needed from the project's planning/design phase through commissioning;
j. assist with ORFDO's Permit Review Process to identify, coordinate and approve physical security requirements; and
k. assist ICOs with establishing a Facility Security Committee (FSC) at multi-tenant leased facilities to ensure risk management strategies are EO 12977 compliant.

3. **The Office of Research Facilities Development and Operations (ORFDO)** will engage DPSM during planning, POR, or requirements definition phases, and submit notice of all proposed facility alteration, new construction, repair by replacement, renovation, and major equipment installation, projects or change in use or classification of a space, including those in the NIH Master Plan, and all NIH leases to DPSM in order to ensure physical security requirements are included prior to the design phase. ORFDO will coordinate with DPSM, through **DPSM-ServiceRequest@mail.nih.gov**, in advance for any project or activity to install, remove, modify, disable or hinder the performance of any physical security system or associated device.

   Periodic FSAs performed by DPSM shall be provided to ORFDO and any security vulnerabilities found will have requisite countermeasure recommendations as documented in the FSA. ORFDO will coordinate with the appropriate stakeholders and/or funding authority to either implement the recommendations or to accept and document the risk.

   a. *Pre-Project Planning Phase*: For DPSM's participation, ORFDO will notify DPSM of all Pre-Project Planning Board (PPPB) and Project Definition Rating Index (PDRI) meeting schedules.

b. *Planning Phase*: ORFDO will ensure DPSM's participation in the development and approval of documents to include, but not limited to, the POR, FPAA and others, as deemed necessary, based on the specific project requirements.
c. *Pre-Design Phase*: Prior to initiating contract actions for design, such as contract solicitations, requests for proposals, etc., ORFDO will submit the SOW for all projects with physical security requirements to DPSM for approval.
d. *Design Phase*: ORFDO will submit design documents to DPSM for review and approval, as consistent with ORFDO's Permit Review Process.
e. *Construction Phase*: ORFDO will submit to DPSM all project change orders that involve existing or new physical security systems and features, for DPSM's review and guidance. Any time a project, either temporarily or permanently adds, removes or modifies any device connected to an NIH security system, ORFDO will coordinate with DPSM so the associated system owner may perform and maintain the configuration management of the system.
f. *Operations and Maintenance*: Prior to performing such activities, ORFDO will coordinate with DPSM any activity associated with operations or maintenance of NIH facilities that adds, removes, modifies, or may affect the performance of any security systems or associated devices by sending notification to **DPSM-ServiceRequest @mail.nih.gov**. In the event an immediate modification is necessary to bring the facility to a stable condition without prior coordination with DPSM, DPSM must be notified as soon as possible after any modification to evaluate the physical security impacts and identify what, if any, measures are necessary to rectify the condition(s).
g. NIH Direct and GSA Lease Concurrence:

    i. To ensure ISC compliance, ORFDO must notify DPSM of all leases (both direct and GSA) at the POR Phase to include site selection to identify necessary physical security countermeasures and any challenges each site may have with incorporating these countermeasures.
    ii. Where applicable in accordance with the EO 12977 and the ISC RMP, ORFDO and/or the ICO shall notify DPSM of new GSA leases to facilitate the application of a FSC, where applicable, in accordance with the EO 12977 and the ISC RMP. The FPS will oversee GSA leased facilities and will be responsible for providing risk assessments and recommended security countermeasures.
    iii. DPSM will review these recommendations and adjust or augment the physical security requirements for such facilities where appropriate, to ensure consistency with the NIH mission and security standards, including facility design review process, systems assessment and commissioning.

4. **NIH Institutes/Centers/Offices (ICO)** officials authorized to conduct construction, renovations, major equipment installations, lease acquisitions, change of use or classification of a space, etc., without ORFDO involvement shall perform the responsibilities of ORFDO as defined above in Section E.3. NIH ICO officials must consult with DPSM, and receive prior written approval, as early as possible during the

initial project planning stages. Any contract impacts and/or unplanned physical security costs resulting from not receiving prior DPSM approval will be borne by the ICO funding authority sponsoring the project(s).

F. Procedures

1. **Initial Project Planning Phase:**

    a. All alterations, new construction, repair by replacement, renovation and major equipment installation projects in NIH owned or leased facilities must be coordinated with ORFDO and DPSM. Examples include but are not limited to projects that:

        - Impact existing security systems
        - Require new security systems
        - Integrate with multiple security systems
        - create security vulnerability
        - change the use or function of a space that may require additional security measures

    b. DPSM will participate in ORFDO Pre-Project Planning Board (PPPB) and Project Definition Rating Index (PDRI) meetings to ensure mandatory physical security features are understood and included for each project.
    c. DPSM will review all new construction requests initiated and captured in ORFDO's Unstructured Project Database (UPD) and identify the DPSM contact with whom the ORFDO PO must coordinate and define the physical security needs and requirements of the project.

2. **Planning Phase:**

    a. Based on the type of procurement action anticipated, the Planning Phase may include, but is not limited to, the development of a POR, FPAA, Bridging or other documents. DPSM will review and provide input to the POR, FPAA, with any other planning documents necessary to ensure the physical security requirements are properly included in the scope of the project.
    b. DPSM will consult available FSAs, and/or perform a preliminary FSA, as appropriate, to identify the physical security requirements provided to ORFDO PO for incorporation in the project's POR documents.
    c. Planning documents must be approved by customers and stakeholders prior to the start of the Design Phase. Any contract impacts and/or unplanned physical security costs resulting from not receiving prior DPSM approval will be borne by the ICO funding authority that is sponsoring the project.

3. **Design Phase:**

a. DPSM will adhere to the ORFDO Permit Review Process and coordinate project physical security requirements with the design teams.
b. DPSM will perform security assessments, develop recommendations, review SOWs and coordinate proposed actions with customers and other stakeholders on an as-needed basis. The SOW may include, but is not limited to, approved equipment and functionality, evaluation and other applicable project security requirements.
c. In accordance with the ORFDO Permit Review Process, DPSM will review design documents and verify the security countermeasure requirements will satisfy the designated threat level or recommended level of protection identified by the ISC RMP.
d. For designs and projects that impact existing, or include new security systems or features, final design submissions must be approved by DPSM prior to being released for bid. If a design is amended during the advertisement/award period impacting the physical security systems or requirements, DPSM must review the scope of the amendment to ensure compliance with federal security requirements.

4. **Construction/Renovation/Project Completion Phases:**

a. During project construction activities, ORFDO PO will notify DPSM when the project is preparing to, either temporarily or permanently, add, remove, or modify any security device connected to any NIH security system so DPSM may coordinate with the appropriate system owner to ensure necessary system configuration management activities are performed.
b. *Change Orders*: The ORFDO PO will notify DPSM of any change orders affecting the physical security features or requirements. DPSM shall review each physical security change and provide comments within the established project schedule.
c. *Ongoing/Periodic Security Assessments*: DPSM will conduct periodic inspections and systems troubleshooting assessments, as deemed appropriate, during ongoing construction, renovation or major equipment installation projects.
d. *Commissioning*: Prior to closeout/completion of the project, all construction, renovation or major equipment installation projects that may impact existing or new security features/systems, must be inspected and approved by DPSM.

G. References

New and emerging threats to the United States necessitate periodic updates to federal security requirements. Therefore, physical security requirements and guidelines unique to the mission of the NIH may include, but are not limited to:

1. ABA Standards for (Federal Facilities)
2. Americans with Disabilities Act (ADA)
3. Architectural Barriers Act Accessibility Guidelines;

4. DHS Interagency Security Committee (ISC) Standards: The Risk Management Process for Federal Facilities
5. DHS National Infrastructure Protection Plan (NIPP)
6. DPSM Physical Security Policies and Design Requirements (not a public document)
7. HHS Internal Critical Infrastructure Protection (CIP) Policy (not a public document)
8. HHS Program Support Center, Physical Security and Emergency Management (PSEM) Policies
9. International Building Code (IBC)
10. National Fire Protection Association (NFPA) Life Safety Code (NFPA 101))
11. NIH Design Requirements Manual
12. NIH Information Security (InfoSec) Policy Handbook
13. NIH Manual Chapter 1405 - Access Control
14. NIH Manual Chapter 1415 - Key and Lock Services
15. NIH Policy Manual, Chapter 1743 Keeping and Destroying Records; GRS 5.1 and GRS 6.5
16. NIST Federal Information Processing Standards Publications (FIPS PUBS)
17. 5 U.S.C. Section 552a (The Privacy Act of 1974, as amended);

For more information on current editions or additional sources not listed, contact the DPSM, via telephone at (301) 443-7287 or by email to DPSM-ServiceRequest@mail.nih.gov.

APPENDIX 1: Definitions

1. **Alterations** - Improvements or changes to an existing property to modify or update its use for a different purpose or function. *See also*, **Improvements**.
2. **Biometric** – A measurement of physical characteristics, such as fingerprints, DNA, or retinal patterns, used to verify an individual's or individuals' identity.
3. **Construction** - The erection of a building, structure or facility, including, but not limited to, the installation of equipment, site preparation, landscaping, associated roads, parking, environmental mitigation, and/or utilities, which provides additional space not previously available. Construction may also include freestanding structures, additional wings or floors, enclosed courtyards or entryways and/or any other means to provide additional usable program space, which did not previously exist, excluding temporary facilities.
4. **DPSM-ServiceRequest@mail.nih.gov** – Dedicated email address for submission of physical security requests, questions or other physical security related communications, including installation, relocation or decommissioning requests, to DPSM.
5. **Facility Project Approval Agreement (FPAA)** - A written agreement between designated HHS Operating Division (OPDIV) officials (i.e., Project Manager, Project Director and OPDIV Board Member) and the Department authorizing the OPDIV's commitment to execute a particular project. A FPAA is required for all facility construction and improvement projects exceeding $1M, and all repair projects exceeding $5M. The FPAA details the project's scope, description, basis of need, funding source(s) and total cost from all sources. The FPAA also identifies project schedule milestones, including completion of design, construction, activation and operational phases.

6. **Facility Security Assessment (FSA)** - A security inspection and report documenting ISC RMP based federal security requirements for a facility, identifying possible vulnerabilities and providing recommendations to bring the facility into compliance.
7. **Facility Security Committee (FSC)** - Facility tenant leadership group which convenes to address security issues at applicable facilities such as multi-tenant leased facilities in accordance with ISC RMP. The FSC is typically chaired by the tenant occupying the most space within said facility or their designee.
8. **Facility Security Level (FSL)** – ISC developed security standards corresponding with the necessary to the security level for differences among federal buildings and their security needs and federal facilities categorized into five classes based on building size, agency mission and/or function, tenant population, threats to tenant agency, and degree of public access to the facility.
9. **Federal Protective Service (FPS)** - A federal law enforcement agency providing integrated security and law enforcement services to federally owned and leased buildings, facilities, properties and/or any other federal assets.
10. **General Services Administration (GSA)** - Central management agency responsible for setting federal policy for federal procurement and real property management and information resources.
11. **Improvements (Renovations/Alterations)** - Any enhancement or change to an existing property, allowing continued, or more efficient use, within its designated purpose (Renovation) or use for a different purpose or function (Alteration). Building improvements may also include upgrading primary mechanical, electrical or other building systems and site improvements not associated with construction projects.
12. **Interagency Security Committee (ISC) Risk Management Process (RMP)** - The ISC's mandate is to enhance the quality and effectiveness of physical security in, and the protection of, buildings and nonmilitary federal facilities in the United States (government-owned, leased or managed; to be constructed, renovated, or modernized or to be purchased).
13. **Major Equipment Installation** - The installation of new equipment that may adversely impact existing security features, such as reinforced walls, ceilings, floors, windows, gates, doorways, security workstations and closets, as well as security systems (identified in No. 18, below) and their related connectivity infrastructure, such as security conduit, cabling, wiring, etc.
14. **Office of the Inspector General (OIG)** - Office charged with identifying, auditing and investigating fraud, waste, abuse and mismanagement within an agency.
15. **ORFDO Project Officer (PO)** - The ORFDO representative who manages the execution of projects that involve construction, alteration, renovation or maintenance of NIH facilities and ensures compliance with all NIH policies and procedures.
16. **Program of Requirements (POR)** - One of the planning and programming documents used to describe a proposed facility and includes estimates of design and construction costs, space and environmental requirements and any other pertinent program information.
17. **Renovation** - Improvements or changes to an existing property to allow continued, or more efficient, use within its designated purpose. *See also,* **Improvements**.

18. **Security Systems** - Active or passive systems including, but are not limited to, access control devices such as card readers, biometric devices and secure locking systems, security lighting, electronic surveillance and video recording systems, intrusion detection and alarm systems, blast mitigation techniques, pedestrian and vehicle barriers, facility/perimeter protection measures and other specialized security systems.