U.S. Department of Energy
Washington, DC

ORDER

DOE O 473.1A

Approved: 8-30-2021

SUBJECT: PHYSICAL PROTECTION PROGRAM

1. PURPOSE. This Order establishes requirements for the Department of Energy (DOE) Physical Protection (PP) Program for assets under the control of DOE.

2. CANCELLATION. The portions of DOE Order 473.3A Chg. 1 (MinChg), *Protection Program Operations,* dated January 2, 2018, that relate to PP Programs (Attachment 3 and Annex 1 Safeguards and Security Alarm Management and Control Systems [SAMACS]) are hereby cancelled. Policy clarification memoranda related to PP are hereby incorporated into this Order and cancelled.

   Cancellation of a directive does not, by itself, modify or otherwise affect any contractual or regulatory obligation to comply with the directive. Contractor Requirements Documents (CRDs) that have been incorporated into a contract remain in effect throughout the term of the contract unless and until the contract or regulatory commitment is modified to either eliminate requirements that are no longer applicable or substitute a new set of requirements.

3. APPLICABILITY.

   a. Departmental Applicability. The requirements in this Order apply to all DOE elements unless exempted under paragraph 3.c.

      (1) The Administrator of the National Nuclear Security Administration (NNSA) will ensure that NNSA employees and contractors comply with their respective responsibilities under this directive. Nothing in this Order/Notice will be construed to interfere with the NNSA Administrator's authority under section 3212(d) of Public Law (P.L.) 106-65 to establish Administration-specific policies, unless disapproved by the Secretary. Any reference to a Program Secretarial Officer (PSO) in this Order is also applicable to the Deputy Administrator/Associate Administrators for the NNSA.

      (2) The Bonneville Power Administration (BPA) Administrator must assure that BPA employees and contractors comply with their respective responsibilities under this directive consistent with BPA's self-financing, procurement and other statutory authorities.

      DOE Contractors. Except for the equivalencies/exemptions in paragraph 3.c., the CRD (Attachment 1) sets forth requirements of this Order that must apply to contracts that include this CRD or its requirements as specified by the contracting officer.

(1) The CRD must be included in the site/facility management contracts that involve classified information or nuclear materials. It must also be included in contracts that contain DOE Acquisition Regulation (DEAR) clause 952.204-2, titled Security Requirements. Departmental Elements must notify contracting officers of affected contracts to incorporate this directive into those contracts.

(2) Upon notification, contracting officers are responsible for incorporating this directive into the affected contracts via the DEAR clause 970.0470-2, Laws, Regulations, and DOE directives clause of the contracts.

b. Equivalencies/Exemptions. Equivalencies and exemptions from the requirements of this Order are processed in accordance with DOE O 251.1, *Departmental Directive Program*, current version.

(1) Existing equivalencies and exemptions must be reviewed to determine applicability under DOE O 473.1A. If applicable, the site must document the review was completed and the equivalency or exemption remains valid.

(2) Equivalencies or exemptions from the requirements in this Order, must be supported by a vulnerability assessment (VA) or security risk assessment (SRA). If a VA or SRA is not applicable in accordance with DOE O 470.3, *Design Basis Threat (DBT)*, current version, an analysis approved by the responsible Program Office which establishes the basis for an informed risk management decision is required. This analysis must identify compensatory measures to be implemented, if applicable.

(3) Equivalencies and exemptions from safeguards and security (S&S) requirements within DOE O 473.1A require formal consultation with the Office of Security, Office of Environment, Health, Safety and Security; and the appropriate Office of the General Counsel (GC) as described in DOE O 251.1, current version. The Office of Security will respond to consultation requests within 45 business days from the receipt of the request.

(4) All approved equivalencies and exemptions under this Order must be entered in the S&S Information Management System (SSIMS) database and incorporated into the affected security plan(s) (SP). Approved equivalencies and exemptions become a valid basis for operation when they have been entered in SSIMS and documented in the appropriate SP and incorporated into site procedures.

(5) DOE S&S program requirements may also be located in, or based on, regulations issued by Federal agencies, and codified in the Code of Federal Regulations (CFRs), or other authorities, such as Executive Orders or Presidential Directives. In such cases, the process for

deviating from those requirements found in the source document must be applied. If the source document does not include a deviation process, the DOE GC, or NNSA GC, must be consulted to determine whether the Departmental Elements deviation from the source can be legally pursued.

(6) Equivalency. In accordance with the responsibilities and authorities assigned by Executive Order 12344, codified at 50 USC sections 2406 and 2511 and to ensure consistency throughout the joint Navy/DOE Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors (Director) will implement and oversee requirements and practices pertaining to this Directive for activities under the Director's cognizance, as deemed appropriate.

4. REQUIREMENTS. Departmental Elements must establish and maintain standardized requirements for management direction, maintenance of qualifications, and execution of operations for the various physical protection activities within DOE.

a. General. Departmental Elements must ensure S&S programs implement the requirements found in the attachments to this Order and contracts that include this CRD or its requirements as specified by the contracting officer.

(1) The Department intends that the highest level of protection be given to security interests and activities whose loss, theft, compromise, and/or unauthorized use would seriously affect national security, the environment, Departmental programs, and/or the health and safety of the public or employees. Accordingly, this Order has been developed to align with the protection levels (PL) defined within DOE O 470.3C, current version.

(2) Whenever a legal, regulatory, or other external standard, or a DOE directive referenced within this Order is amended or superseded, the successor document is applicable under this Order.

b. Planning. PP planning must be based on the adversary capabilities outlined in the DBT and the results of SRAs and VAs, as applicable.

c. Quality Assurance Program (QAP). Each Departmental and associated field element(s) must develop and implement a QAP in accordance with DOE O 414.1, *Quality Assurance*, current version, and incorporate into applicable QAP's and Quality Implementation Plans.

d. Records. Security related records including records documenting access control must be retained in accordance with the National Archives and Records Administration (NARA) General Records Schedule (GRS) 5.6: Security Records.

e. Implementation.

(1) Compliance with the requirements within this Order, including the attachments, must be complete within one (1) year of the issuance date.

(2) If compliance cannot be accomplished within one (1) year, an implementation schedule must be submitted to the appropriate Program Secretarial Officer (or their designee), prior to the deadline stated in 4.e.(1) above. Documentation must include timelines and resources needed to fully implement this Order as well as a description of the vulnerabilities and impacts created by delayed implementation of the requirements.

f. Contracting Officer (CO) Requirements. The Head of the Departmental Element, or his or her designee, must notify the CO and other appropriate subject matter experts in the organization that the directive applies to an existing contract or to a solicitation for a future contract.

(1) For existing contracts, the Head of Departmental Element must designate appropriate representatives (Federal and/or contractor) to work with the CO to develop an appropriately tailored set of standards, practice, and controls.

(2) For existing management and operating (M&O) contracts, after being notified by the Head of the Departmental Element or his or her designee, the CO must provide the contractor the opportunity to:

(a) Assess the effect of incorporating the CRD on contract cost, funding, schedule, and technical performance, and

(b) Provide input on the appropriately tailored set of requirements for the contract. All associated activities will be accomplished in a timely manner and, if applicable, in accordance with the timelines established in DEAR 970.5204-2. The CO will incorporate the CRD without alteration unless the directive permits alteration and the appropriate process is followed.

5. RESPONSIBILITIES.

a. Office of Environment, Health, Safety and Security. Review, develop, and coordinate policy requirements and guidance for the management, operation, and performance testing of PP programs and systems based on authority and requirements derived from the Atomic Energy Act and DOE Organization Act.

b. Officially Designated Federal Security Authority (ODFSA). Fulfill requirements and responsibilities that are formally delegated to them from DOE or NNSA. ODFSAs are Federal employees that possess the appropriate

knowledge and responsibilities for each situation to which they are assigned through delegation.

(1) Delegation authority for these positions is originated according to direction from the accountable Program Secretarial Officer, (or the Secretary or Deputy Secretary for Departmental Elements not organized under a Program Secretarial Office), who also provides direction for which of the ODFSA positions may be further delegated.

(2) Each delegation must be documented in written form. It may be included in other security plans or documentation approved by or according to direction from the accountable principal.

(3) Each delegator remains responsible for the delegatee's acts or omissions in carrying out the purpose of the delegation.

c. Officially Designated Security Authority (ODSA). Fulfill requirements and responsibilities that are formally delegated to them from DOE or NNSA. Throughout this Order, in instances where there is no designated ODSA the requirements and responsibilities remain with the ODFSA. Officially Designated Security Authority (ODSA): ODSAs are Federal or contractor employees that possess the appropriate knowledge and responsibilities for each situation to which they are assigned through delegation.

(1) Delegation of authority for these positions is originated according to direction from the accountable Program Secretarial Officer, (or the Secretary or Deputy Secretary for Departmental Elements not organized under a Program Secretarial Office), who also provides direction for which of the ODFSA positions may be further delegated.

(2) Each delegation must be documented in written form. It may be included in other security plans or documentation approved by or according to direction from the accountable principal.

(3) Each delegator remains responsible for the delegate's acts or omissions in
carrying out the purpose of the delegation.

d. DOE Line Management. DOE line management refers to the chain of responsibility that extends from the Secretary of Energy to the Deputy Secretary, to the Secretarial Officers who set program policy and plans and develop assigned programs, and to the program and Field Element Managers or ODFSAs who are responsible for execution of these programs.

(1) Provide guidance and oversight to site and facility management and operations offices that oversee PP programs, for the purposes of protecting S&S interests.

(2) Ensure that PP programs under their cognizance are adequately managed and maintained for the protection of S&S interests, as required by this and other S&S related directives.

(3) Ensure that systems updates and or patches are installed in accordance with manufacturer's instructions.

(4) Implement the requirements in paragraphs 4.a. through 4.f above.

e. Heads of Field Elements.

(1) Administer PP programs for the purposes of protecting pertinent S&S interests.

(2) Ensure contracting officers of responsible contracts incorporate the CRD into the contract.

f. Headquarters Security Operations.

(1) Administer PP programs for the purposes of protecting Headquarters S&S interests.

(2) Ensure contracting officers of affected contracts incorporate the CRD into the contract.

g. Office of Enterprise Assessments/National Training Center. Develops, maintains, and delivers standardized PP training for Federal and contractor employees, in order to ensure personnel are appropriately trained to fulfill their mission within the Department’s S&S program.

h. Contracting Officers.

(1) Upon notification of its applicability, incorporate the CRD into affected contracts via the appropriate process.

(2) Assist originators of procurement requests who want to incorporate the requirements of this Order in new non-site/facility management contracts, as applicable.

6. INVOKED STANDARDS. The following industry standards are invoked as required methods in this Order in accordance with the applicability and conditions described within this Order. Any technical standard or industry standard that is mentioned in or referenced by this Order, but is not included in the list below, is not invoked by this Order. Note: DOE O 251.1D, Appendix J provides a definition for "invoked technical standard."

a. FED-STD-832, Federal Standard Construction Methods and Materials for Vaults

b. FIPS 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*

c. *Intelligence Community Standard (ICS) ICD/ICS 705, Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities*, Version 1.4

d. NIST Special Publication 800-116, Rev 1, *Guidelines for the Use of PIV Credentials in Facility Access*

e. UL 2050, *National Industrial Security Systems*

f. UL 634, *Standard for Safety Connectors and Switches for Use with Burglar-Alarm Systems*, sections 58, 60, 61, 62, 63

7. REFERENCES. References specific to this Order are listed in Attachment 8 - Physical Protection Program References.

NOTE: Whenever a legal, regulatory, or other external standard, or a DOE Policy, Order, Notice or Manual is referenced, and such standard is amended or superseded, the successor standard is applicable under this Order.

8. DEFINITIONS. Terms commonly used in the program are defined in Attachment 7 - Physical Protection Program Definitions.

9. CONTACT. Questions concerning this Order should be addressed to the Office of Security Policy, Office of Environment, Health, Safety and Security at security.directives@hq.doe.gov. Formal policy clarifications should be directed to the Director, Office of Security, Office of Environment, Health, Safety and Security.

BY ORDER OF THE SECRETARY OF ENERGY:

DAVID M. TURK
Deputy Secretary

CONTENTS

ATTACHMENT 1. CONTRACTOR REQUIREMENTS DOCUMENT

Regardless of the performer of the work, the contractor is responsible for complying with the requirements of this CRD. The contractor is responsible for flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary to ensure the contractor's compliance with the requirements.

In addition to this order contractors are responsible for complying with Attachments 2-8 to DOE O 473.1A referenced in and made a part of this CRD and which provide program requirements and/or information applicable to contracts in which this CRD is inserted.

ATTACHMENT 2. PHYSICAL PROTECTION BASELINE REQUIREMENTS

The intent of this Attachment is to establish baseline requirements for all Department of Energy (DOE) Departmental Elements to provide protection to DOE's assets. This and all subsequent attachments apply to DOE Employees and Contractors.

CHAPTER I. PHYSICAL PROTECTION PLANNING

The intent of this Chapter is to provide the requirements for physical protection planning.

1. GENERAL REQUIREMENTS. Special Nuclear Material (SNM) must be protected at the higher level when credible roll up to a higher category can occur.

   If the facility has conducted an analysis and determined that roll up is not credible, the security measures that prevent roll up from being credible must remain in place, or the material must be protected at the higher level until an analysis determines that roll up to a higher category is not credible.

   a. SNM that is classified must receive the physical protection required by the highest level of classification or category of SNM, whichever is the more stringent.

   b. Countermeasures must be designed to mitigate the adversary scenarios and capabilities described within the DBT.

   c. Security Plans (SPs) must be developed in accordance with DOE O 470.4, *Safeguards and Security Program*, current version. The SP must be approved by the ODFSA.

   d. For certain facilities that do not possess a facility clearance the Interagency Security Committee Risk Management Process must be used as the baseline for the SP (see DOE O 470.4, current version).

   e. Protection measures must be documented in the SP. Cyber security protection measures must be consistent with the Departmental Element Cybersecurity Program Plan, as required by DOE O 205.1, *Cybersecurity Program*, current version.

   f. For assets requiring an SRA the protection strategy objectives below must be addressed in the SP:

      (1) Protection;

      (2) Mitigation;

      (3) Incident Response; and

      (4) Mission Recovery.

   g. Physical Access Control Systems (PACS) equipment used for physical protection must be in accordance with Attachment 6, Chapter I of this Order.

   h. Intrusion Detection Systems (IDS) equipment used for physical protection must be in accordance with Attachment 6, Chapter II of this Order.

i. Video Assessment and Surveillance Systems (VASS) equipment used for physical protection must be in accordance with Attachment 6, Chapter III of this Order.

j. Physical protection systems, including components, must be performance tested to ensure overall system effectiveness in accordance with Attachment 6, Chapter IV of this Order.

k. Physical security system maintenance must be implemented in accordance with Attachment 6, Chapter V of this Order.

l. Communications Systems equipment used for physical protection must be in accordance with Attachment 6, Chapter VI of this Order.

m. Power and lighting equipment used for physical protection must be in accordance with Attachment 6, Chapter VII of this Order.

n. Data transmission and line supervision of security systems equipment used for physical protection must be in accordance with Attachment 6, Chapter VIII of this Order.

o. Security containers or areas where explosives, pyrotechnics, weapons and/or ammunition, not assigned to the protective force (PF), and not located in limited areas (LAs), must be stored in a location monitored by IDS or checked at intervals to protect against unauthorized access as documented in the SP.

p. Unmanned Aircraft Systems.

(1) The ODFSA must approve use of unmanned aircraft systems used for security purposes.

(2) If used, sites must comply with DOE O 440.2, *Aviation Management and Safety*, current version.

q. Counter Unmanned Aircraft Systems. The ODFSA must approve the use of counter unmanned aircraft systems in accordance with the provisions of the 2017 *National Defense Authorization Act* [P.L. 114-328] and applicable delegation orders.

CHAPTER II. SECURITY AREAS

The intent of this Chapter is to establish requirements for security areas, which are designed to provide protection to the Department's assets.

1. GENERAL ACCESS AREA (GAA). GAAs may be designated by the ODSA to allow access to certain areas with minimum-security requirements.

    a. The ODFSA must approve security requirements for those areas designated as GAAs based on a risk management process.

    b. Security requirements and the identification of GAA locations must be documented in SPs approved by the ODFSA.

    c. The security requirements must be posted to inform all personnel, including the public, that entry into these areas subjects them to requirements.

2. PROPERTY PROTECTION AREA (PPA). PPAs are security areas that are designated to protect employees and government owned or leased, buildings, facilities and assets.

    a. The ODSA must approve security measures for those areas designated as PPAs based on an analysis in accordance with DOE O 470.4, current version.

    b. PPAs must be configured to provide a means to control access.

    c. Security requirements and the identification of PPA locations must be documented in SPs approved by the ODFSA.

    d. Warning signs and/or notices must be posted (see Chapter IV of this Attachment).

3. LIMITED AREA (LA). LAs are the minimum level security area designated for the protection of classified matter, category III SNM, or Departmental assets requiring limited access.

    a. Unescorted access must be limited to authorized personnel with the appropriate access authorization.

    b. PACS must be installed in accordance with Attachment 6, Chapter 1.

    c. Escort ratios for LAs must be documented in the approved SP.

    d. Measures must be implemented at the LA perimeter to deter, delay and detect unauthorized access into an LA, as documented in the approved SP.

    e. Ingress and egress points must be equipped with access control designed to grant authorized access and detect unauthorized entry.

    f. LAs must have boundaries defined by physical barriers in accordance with Chapter VI of this Attachment.

g. Entry portals must provide the same level of detection as all other points along the boundary.

h. Personnel access to LAs must be controlled in accordance with Attachment 6, Chapter I of this Order.

i. Vehicle access must be for official purposes and meet the following requirements:

(1) Allow entry via an approved process documented in the SP.

(2) Allow entry via DOE security badge authentication of all personnel within the vehicle by visual inspection, or

If used, PACS must be implemented in accordance with Attachment 6, Chapter I. of this Order.

(3) Operated by authorized personnel.

(4) Vehicle is inspected by approved process documented in the SP.

j. Signs must be posted as documented in the approved SP to convey information on:

(1) Prohibited and controlled articles.

(2) The inspection of vehicles, packages, hand carried items, and persons entering or exiting the security area.

(3) The use of video surveillance equipment.

(4) Trespassing (see 42 U.S.C. § 2278a; 10 CFR Part 860).

4. VAULTS AND VAULT TYPE ROOM (VTR). Vaults and VTRs are established for the protection of classified matter and DOE assets requiring limited access and security in depth (see Chapter VII of this Attachment).

5. SENSITIVE COMPARTMENTED INFORMATION FACILITY (SCIF). DOE follows the requirements in Intelligence Community Standard (ICS) ICD/ICS 705, *Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities*.

6. SPECIAL ACCESS PROGRAMS (SAPs). The requirements for SAPs are identified in DOE O 471.5, *Special Access Programs*, current version.

7. PROTECTED AREA (PA). PAs are security areas that are established to protect Category II or greater quantities of SNM and may contain classified matter (see Attachment 6).

8. MATERIAL ACCESS AREA (MAA). MAAs are security areas that are established to protect Category I quantities of SNM (see Attachment 6).

CHAPTER III. PROHIBITED AND CONTROLLED ARTICLES

The intent of this Chapter is to prescribe requirements for prohibited and controlled articles.

1. GENERAL REQUIREMENTS.

   a. Authorization for prohibited and controlled articles to be used for official Government business must be documented in an SP.

      Office of Secure Transportation (OST) Federal Agents, DOE protective personnel, other Federal agents, local law enforcement officials with jurisdiction, and emergency response personnel whose duties routinely require the carrying and operation of prohibited and controlled articles, may be exempt from this requirement unless a safety reason exists to prohibit certain communication devices, e.g., cellular telephones, transceiver radios and other electronic radiating/emitting devices. If such a prohibition exists, it is to be documented in specific agreements between the site and the appropriate agency.

   b. Sites are to develop procedures to deter the introduction of prohibited and controlled articles. These procedures must be documented in an SP approved by the ODFSA.

   c. The articles listed below must not be permitted onto DOE property without appropriate authorization.

2. PROHIBITED ARTICLES. Prohibited articles include but are not limited to:

   a. explosives,

   b. dangerous weapons, as defined by 18 USC § 930,

   c. instruments or material likely to produce substantial injury to persons or damage to persons or property,

   d. controlled substances (e.g., illegal drugs and associated paraphernalia but not prescription medicine), and

   e. other items prohibited by law. Additional information covering prohibited items may be found under the provisions of 18 USC § 930, 21 USC 841 et. seq, 10 CFR Part 860 and 41 CFR Chapter 102-74 Subpart C.

3. CONTROLLED ARTICLES.

   a. Controlled articles such as portable electronic devices (PED), both government and personally owned, capable of recording information or transmitting data (e.g., audio, video, radio frequency, infrared, and/or data link electronic equipment) are not permitted in LAs, VTRs, PAs, and MAAs, without prior written approval.

(1) The approval process permitting controlled articles must be documented in the approved SP.

(2) Medical devices with the ability to transmit or record data must be approved by the ODFSA.

(3) Government owned PEDs, information technology systems may only be authorized for introduction and use within LA's VTR's, PA's and MAA's by the ODFSA. Any ODFSA approval must be based on a documented risk analysis incorporating technical security countermeasures and cybersecurity input.

b. For application to SCIFs the ICS 705-1, *Physical and Technical Security Standards for Sensitive Compartmented Information Facilities* program guidance must be implemented.

c. See DOE O 471.5, *Special Access Programs*, current version, for guidance on controlled articles in Special Access Program Facilities.

CHAPTER IV. POSTING REQUIREMENTS

The intent of this Chapter is to establish requirements for signs posted at facilities, installations, and real property as defined in DOE O 430.1, *Real Property Asset Management*, current version, based on the need to implement Federal statutes protecting against degradation of S&S interests.

1. GENERAL REQUIREMENTS.

   a. 10 CFR Part 860, *Trespassing on Department of Energy Property*, requires facilities, installations, or real property subject to the jurisdiction, administration or in the custody of DOE to be published in the Federal Register in order to inform the public of the penalties for trespassing or introducing unauthorized weapons or dangerous materials (also known as prohibited articles) to these areas.

   b. 10 CFR Part 860 requires DOE to post signs warning of the consequences and penalties for trespassing and introducing unauthorized weapons or dangerous materials on to DOE controlled property.

   c. The Program Secretarial Office must approve all postings to the Federal Register and coordinate the publishing of the notice with the National Archives Office of the Federal Register. Additional guidance can be located at https://www.archives.gov/federal-register/write.

   d. The Program Secretarial Office must notify the local office of the Federal Bureau of Investigation with jurisdiction over the subject property, of the date of posting, relocation, removal of posting, or other change, and the identity of the property involved.

2. FEDERAL REGISTER POSTING PROCESS.

   a. Proposals for the posting of facilities, installations, or real property, or amendment to or revocation of a previous proposal must be submitted when one of the following occurs:

      (1) New property acquisition or a change in existing property owned by or contracted to the United States for DOE use.

      (2) New property acquisition or a change in existing property which requires protection under the Atomic Energy Act of 1954 and/or of the DOE Organization Act.

      (3) A previous notice needs to be amended or revoked.

   b. Each posting proposal must include:

      (1) The name and specific location of the installation, facility, or real property to be covered and the boundary coordinates.

(2) If boundary coordinates are not available, the proposal must include a description that will furnish reasonable notice of the area to be covered, which may be an entire area or any portion thereof that can be physically delineated by the posting indicated in paragraph 2.(c) below.

c. Each proposal for amendment or revocation must identify the property involved, state clearly the action to be taken (i.e., change in property description, correction, or revocation), and contain a new or revised property description, if required.

3. SIGNAGE POSTING REQUIREMENTS.

a. DOE real property must have signs posted according to statutes, regulations, and the administrative requirements for posting specified in this Chapter.

(1) Section 229 of the Atomic Energy Act of 1954 as amended (42 U.S.C. § 2278a), as implemented by 10 CFR Part 860.

(2) Section 662 of the DOE Organization Act (42 U.S.C. § 7270b), as implemented by 10 CFR Part 1048.

(3) The Federal Property and Administrative Services Act of 1949 (P. L. 152, Ch. 288, 63 Stat. 377, as amended).

(4) 41 CFR Part102-74, Subpart C governs entry to public buildings and grounds under the charge and control of the General Services Administration (GSA).

b. Signs prohibiting trespassing and the introduction of prohibited articles must be posted in accordance with 10 CFR Part 860.

(1) Signs must be configured with a white or yellow background and black lettering.

(2) Signs must measure at least 26.67 centimeters (10.5 inches) by 34.29 centimeters (13.5 inches).

c. Signs that notify of the use of deadly force are required for facilities with PL-1 through PL-4 assets.

(1) These signs must use a white background with red lettering for the words "WARNING USE OF DEADLY FORCE AUTHORIZED" and be clearly legible and commensurate with the size of the sign. The remaining words should be in black.

(2) Placement of these signs must be based on the site's determination of hostile intent and established rules of engagement.

d. Placement of signs on fences must not interfere with the function of fence mounted IDS. If the signage interferes with the IDS or video assessment and surveillance system (VASS), it could be mounted on posts outside the fenced area.

e. The signage must be mounted to establish demarcation of boundaries. This demarcation must be easily discernable, determined by the ODSA based on analysis to provide reasonable assurance of notice to persons about to enter, and documented in the approved SP.

CHAPTER V. SECURITY LOCKS AND KEYS

The intent of this Chapter is to establish requirements for the Department's security lock and key programs based upon the Department of Defense's (DoD) Lock Program. The GSA is a sponsor of the DoD Lock Program. More information can be found at the Naval Facilities Engineering Systems Command (NAVFAC) website using the following link, https://www.navfac.navy.mil/navfac_worldwide/specialty_centers/exwc/products_and_services/capital_improvements/dod_lock.html

Note: The General Services Administration, Interagency Advisory Committee on Security Equipment (GSA/IACSE) provides the following clarification on the status of the Fedsafes GSA-approved class 5 security cabinets manufactured under Federal Specification AA-F-358. Fedsafes was removed from the GSA Qualified Products List (by QPL-AA-F-358-16) on 9 September 2017 due to reoccurring inconsistent test results and failure to adequately resolve the issues during periodic re-evaluations of their class 5 cabinet.

Although Fedsafes was removed from the Qualified Products List as an authorized manufacturer, the original GSA approval of the existing class 5 cabinets has not been revoked.

Additionally, the GSA/IACSE in coordination with the Information Security Oversight Office (ISOO) is developing a phase-out plan for all GSA-approved security containers and vault doors manufactured prior to 1989 (Black GSA Label). The plan will rescind the approval for all GSA-approved security cabinets and vault doors manufactured from 1954 through 1989 (Black GSA-Approval labels) to store classified information and materials over a period of 4 years starting on as of October 1, 2024.

The phase-out plan will start with the oldest cabinets (class 2) and proceed to the last of the Black Label security equipment (class 5 & 6) over a period of at least 4 years as outlined below.

All GSA-approved Class 1, 2, 3 & 4 cabinets manufactured under Federal Specifications AA-F-357 and AA-F-358 600 (Revision Indicators A - F) will be considered obsolete for the storage of classified information and materials as outlined in the below chart.

All GSA-approved Class 5 & 6 cabinets and vault doors manufactured under Federal Specification AA-F-358 (Revision Indicators A - F) and AA-D-600 (Revision Indicators A - C) before 1989 will be considered obsolete for the storage of classified information and materials as of 1 October 2028.

Black Label Phased-Out Plan Chart

GSA CLASS	FED SPEC	AMEND	YEARS PRODUCED	YEARS OF SERVICE	END OF SERVICE
1	AA-F-357	A - F	1968 - 1982	46 - 60	1 October 2028
2	AA-F-357	A - F	1954 - 1970	50 - 70	1 October 2024
3	AA-F-358	A - F	1956 - 1968	52 - 69	1 October 2025
4	AA-F-358	A - F	1956 - 1968	52 - 69	1 October 2025
5	AA-F-358	A - F	1968 - 1989	31 - 60	1 October 2028
5	AA-F-363	A - B	1963 - 1989	57 - 65	1 October 2028
5	AA-D-600	A - B	1963 - 1989	57 - 65	1 October 2028
6	AA-D-600	A - C	1963 - 1989	57 - 65	1 October 2028
6	AA-F-358	A - F	1968 - 1989	52 - 60	1 October 2028

The old GSA-approved cabinets and vault doors produced prior to 1989 can be easily identified by the silver and black GSA approval label on the outside of the cabinet or vault door and by the certification labels and manufacturing dates located on the control drawer body or on the inside of the vault door.

1. GENERAL REQUIREMENTS.

   a. Security locks and key categories are based on the types of assets being protected and the levels of controls associated with the locks and keys. Non-security locks and keys are administrative in nature and are not addressed in this Order.

   b. The ODSA must establish a security lock and key program that:

      (1) Prescribes the installation, replacement, and maintenance requirements for security locks.

      (2) Prescribes the requirements for issuance, control and storage of security keys.

      (3) Limits the number of keys to the minimum amount needed for operational purposes.

      (4) Establishes the inventory system to ensure the accountability of security locks, keys, key rings, keyways, and removable pinned cores (as applicable). At a minimum, there must be a 100 percent annual inventory of all security locks and keys.

      (5) Prescribes the notification requirements for unaccounted for or broken security locks and keys in accordance with DOE O 470.4B Chg 2, Attachment 5.

      (6) Prescribes the approved destruction methods of inoperative or damaged keys.

(7) Establishes procedures for key turn in when personnel or programs are terminating or when an individual no longer has a need for the key.

(8) Includes a strategy for the use and protection of grand master, master, sub-master, and control keys.

(9) Is documented in the SP.

c. Keyed cylinders must meet Grade 1 American National Standards Institute (ANSI) Standard A 156.30-2014, *American National Standard for High Security Cylinders* and either;

(1) Grade 1 ANSI/A156.2-2017, *Bored and Preassembled Locks and Latches*, or

(2) Grade 1 ANSI A156.13-2017, *Mortise Locks and Latches.*

d. At locations implementing a multifaceted Insider Threat Mitigation Program and a Human Reliability Program (HRP), locksmiths must be analyzed for inclusion in HRP in accordance with 10 CFR §712.10.

2. LEVEL I LOCKS AND KEYS.

a. Level I locks including those that provide access to classified matter, MAAs, vaults and VTRs must be:

(1) Locks that meet Federal Specification FF-L-2740B, Amendment 2, *Locks, Combination, Electromechanical* and Federal Specification FF-L-2890C, Amendment 3, *Lock Extensions (Pedestrian Door Lock Assembly Preassembled, Panic, and Auxiliary Deadbolt)* or

(2) High security, shrouded shackle, key operated padlocks with Grade 1 ANSI hasps, that meet standards in Military Specification MIL DTL 43607J, *Padlock, Key Operated, High Security, Shrouded Shackle* or

(3) A High Security Deadbolt Locking System, Internal Locking Device (ILD) (dual cylinder model only) that meet DODM S-5210.41-M-V2 *Nuclear Weapon Security Manual* Enclosure 2, Section 3.b.(6)(c)(U).

(4) Combination padlocks meeting Federal Specification FF-P-110J may be used to secure storage areas for SNM or, bulky material containing Secret or Confidential information.

Hasps and yokes on containers storing classified matter must be constructed of steel material, be at least 6.35 millimeters (¼ inch) in diameter or equivalent cross section, and be secured to the container by welding, or riveting, to preclude removal.

b. Six locks have been approved under FF-L-2740B for the protection of classified matter. The Mas-Hamilton Group model X-07 lock was approved in February 1992, the X-08 in March 1999, the Kaba Mas X-09 in June 2002, the Sargent & Greenleaf (S&G) model 2740 in June 2010, the Kaba Mas X-10 in April 2013, and the S&G model 2740B in November 2013.The X-07 and X-08 locks have reached the end of their expected service life and a plan to replace these locks must be developed by the ODSA and documented.

c. The following combination locks are approved for the protection of Category I and II SNM:

(1) Kaba Mas model X-09;

(2) S&G model 2740B; or,

(3) Kaba Mas model X-10.

3. LEVEL I LOCK AND KEY CONTROL.

a. Level I key blanks must be restricted/proprietary; specifically, the blank must be unique to the site (e.g., it does not use a commercially available master key blank). Level I key blanks must be stored and protected as outlined in 3.e. below.

b. Level I key codes (information required to replicate/cut a key) must be stored and protected as outlined in 3.e below.

c. Access to Level I keys and key codes must be controlled and limited to personnel with an access authorization commensurate to the classification of the assets to which the keys or codes provide access.

d. Once they are put in service inside a security area, Level I security locks and keys must not leave the security area without authorization as described in the SP. Any key that leaves the security area without authorization must be considered unaccounted for and reported as lost.

e. When not in use, Level I security locks and keys must be stored in a:

(1) GSA approved container; or

(2) LA or higher within a locked receptacle or room; or

(3) Vault or VTR.

f. Locks meeting FF-L-2740 not in use, and set to default, may be stored in a locked receptacle or room within a PPA.

g. Level I keys must be on a separate key ring from all other levels of keys

(1) Level I keys must be permanently marked with a unique identifying number, and

(2) A unique identifying number must be placed on each key ring.

h. All parts of broken Level I security keys must be recovered. If the functional part of the key (the blade) is lost or not retrievable it must be reported as a lost/missing key and measures must be taken to replace the corresponding lock(s).

i. When a Level I security key is unaccounted for, immediate notification must be made to the ODSA and compensatory measures must be immediately initiated.

If an unaccounted for Level I key cannot be located within 24 hours, the affected lock must be changed.

4. LEVEL II SECURITY LOCKS.

a. Locations protecting PL-6 assets; Category III SNM; firearms and explosives require Level II security locks and keys.

b. Level II locks must meet the requirements of one of the below:

(1) ANSI grade 1 keyed locksets with grade 1 cylinders,

(2) Commercial Item Descriptions (CID) A-A-59486C, *Padlock Set (individually keyed or keyed alike)*,

(3) CID A-A-59487C, *Padlock (key operated)*, or

(4) Meet the requirements of Federal Specification FF-L-2937, *Combination Locks, Mechanical*, and its Amendment 2 with an FF-L-2890C Pedestrian door lock assembly.

5. LEVEL II LOCK AND KEY CONTROL.

a. When not in use, Level II security locks and keys must be stored in a:

(1) GSA approved container; or,

(2) Locked cabinet or drawer or otherwise secured in a PPA or higher; or,

(3) Vault or VTR.

b. Level II locks and keys once put into service must not leave the site without authorization as described in the SP.

c. All parts of broken Level II security keys must be recovered. If the functional part of the key (the blade) is lost or not retrievable it must be reported as a lost/missing key and measures must be taken to replace the corresponding lock(s).

d. Level II keys must be permanently marked with a unique identifying number.

e. Level II-III keys may be combined on the same key ring with a unique identifying number; however, the key ring must be protected according to the highest level of key on the ring.

6. LEVEL III SECURITY LOCKS.

a. Locations where Category IV SNM are stored and other areas designated by the ODSA require level III security locks and keys.

b. Level III lock types must be authorized by the ODSA.

7. LEVEL III LOCK AND KEY CONTROL.

a. When not in use, Level III security locks and keys must be stored in a manner approved by the ODSA.

b. All parts of broken Level III security keys must be recovered unless the functional part of the key (the blade) is lost or not retrievable.

c. Level III keys must be permanently marked with a unique identifying number.

d. Level II-III keys may be combined on the same key ring with a unique identifying number; however, the key ring must be protected according to the highest level of key on the ring.

CHAPTER VI. BARRIERS

The intent of this chapter is to prescribe requirements for physical barriers, which serve as the physical demarcation of security areas.

1. GENERAL REQUIREMENTS.

   a. The ODFSA must determine, based on analysis in accordance with DOE O 470.4, current version, what barriers are required for GAAs and PPAs.

   b. The following requirements apply to LAs:

      (1) Passive barriers such as fences, walls, and doors or active barriers such as bollards, wedge barriers, or sliding gates must be employed to deter and delay unauthorized access and control authorized access.

      (2) At a minimum, an analysis is required of DOE assets to determine the protection measures against vehicle borne improvised explosive devices (VBIED) to mitigate the DBT adversary threat.

      (3) Barriers must be used:

         (a) To direct the flow of personnel and vehicular traffic through designated entry points/portals;

         (b) To permit efficient operation of access controls and entry point inspections; and

         (c) To support the ability to engage adversaries along all feasible pathways.

      (4) Entry points/portals must be designed to provide a barrier resistant to bypass.

      (5) Permanent barriers must be used to enclose LAs, except during construction or temporary activities, when temporary barriers may be erected in accordance with locally approved procedures.

2. PENETRATION OF SECURITY AREA BARRIERS. Penetration of security area barrier requirements include the following:

   a. Elevators that penetrate a security area barrier must be provided with an access control system that is equivalent to the access control requirements for the security area being penetrated.

   b. Utility corridors that penetrate security area barriers must provide the same degree of penetration resistance as the barriers they penetrate.

c. Objects that intruders could use to scale or bridge barriers and enter security areas must be removed or secured to prevent their unauthorized use.

d. If a security area configuration is altered, barriers must be erected, and at a minimum, an analysis must be conducted and documented in accordance with locally approved procedures to validate equivalent protection measures.

e. The barrier design must consider proximity to buildings or overhanging structures.

3. HARDWARE.

a. Screws, nuts, bolts, hasps, clamps, bars, wire mesh, hinges, and hinge pins must be fastened securely to preclude removal and to ensure visual evidence of tampering.

b. Hardware accessible from outside the security area must be peened, brazed, or spot welded to preclude removal, or

c. The area must be otherwise secured by use of tamper resistant hardware (e.g., non-removable hinge pins), or

d. By other means as described in the SP.

Note: These requirements do not apply to fencing.

4. FENCING. When used to protect security areas designated as LAs or higher, fencing installed or modified after the issuance of this order must meet the following requirements:

a. Permanent Security Fencing Materials and Specifications.

(1) Chain link fabric consisting of a minimum of No. 11 American Wire Gauge (AWG) galvanized steel wire with mesh openings not larger than 5.08 centimeters (2 inches) must be used.

(2) Fencing must be topped by three or more strands of barbed wire, coiled barbed wire, or barbed tape coil with single or double outriggers. The direction of the single outrigger is at the discretion of the ODSA. For PAs this only applies to the inner fence.

(3) Overall fence height, excluding barbed wire or barbed tape coil topping, must be a minimum of 2.13 meters (7 feet) above grade.

(4) Fence lines must be kept clear of vegetation, trash, equipment, and other objects that could impede observation or facilitate bridging.

(5) Gate hardware that if removed would facilitate unauthorized entry, must be installed in a manner to mitigate tampering and/or removal (e.g., by brazing, peening, or welding).

(6) Posts, bracing, and other structural members must be located on the inside of security fences.

(7) Wire ties used to fasten fence fabric to poles must be of the same or more robust gauge than that of the fence fabric.

Note: Other fencing types (architectural or decorative) may be used without an equivalency if they have been performance tested to establish that the resulting barrier provides delay and deterrence equivalent to or greater than the above requirements and are documented in the SP.

b. Permanent Security Fencing. When permanent fencing is used to enclose LAs or higher, fencing must meet the following construction requirements:

(1) Areas under security fencing subject to water flow, such as bridges, culverts, ditches, and swales, must be blocked with wire, steel bars, or other methods that provide for the passage of floodwater but also provide a penetration delay equal to that of the security fence.

(2) Fencing must extend to within 5.08 centimeters (2 inches) of firm ground or below the surface.

(a) Surfaces must be stabilized in areas where loose sand, shifting soils, or surface waters may cause erosion and thereby assist an intruder in penetrating the area.

(b) Where surface stabilization is impossible or impractical, concrete curbs, sills, or a similar type of anchoring device extending below ground level must be provided.

(3) Alternate barriers or terrain may be used instead of fencing if the penetration resistance of the barrier is equal to or greater than security fencing specified in this Chapter. An analysis must be conducted and documented in accordance with locally approved procedures.

c. Temporary Security Fencing. Temporary barriers must effectively impede access to the area. During construction or temporary activities, security fencing must be installed to:

(1) Exclude unauthorized vehicular and pedestrian traffic from the security area,

(2) Restrict authorized vehicular traffic to designated access roads, and

(3) Comply with locally approved procedures and operational requirements.

5. PERIMETER BARRIER GATES. Controls for motorized gates used at entry points/portals must be located within PF posts or other locations as described in the SP. Motorized gates must be designed to facilitate manual operation during power outages.

6. EXTERIOR WALLS. Walls that constitute exterior barriers of security areas must extend from the true floor to the true ceiling unless equivalent means are used to provide evidence of penetration of the security area or access to the security interest being protected.

7. CEILING AND FLOORS. Ceilings and floors must be constructed of building materials that offer penetration resistance to, and evidence of, unauthorized entry into the area.

8. DOORS. For LAs and above doors, door frames, door threshold, and door jambs associated with walls serving as barriers must provide the necessary barrier delay required by the SP. Requirements include the following:

   a. Penetration Resistance Doors. Doors with transparent glazing material must offer penetration resistance to, and evidence of, unauthorized entry into the area. Doors that serve exclusively as emergency and evacuation exits from security areas must:

      (1) Not permit access to the security area from outside the security area; and

      (2) Comply with National Fire Protection Association *Life Safety Code* 101.

   b. Astragals or Mullions. An astragal or mullion must be used where doors used in pairs meet.

      Door louvers, baffles, or astragals/mullions must be reinforced and immovable from outside the area being protected.

   c. Visual Access. Visual barriers must be used if visual access is a factor.

9. WINDOWS. The following design requirements must be applied to security windows when used as physical barriers.

   a. Windows must offer penetration resistance to, and evidence of, unauthorized entry into the area.

   b. Frames must be securely anchored in the walls and windows locked from the inside or installed in fixed (non-operable) frames so the panes are not removable from outside the area under protection.

   c. Visual barriers must be used if visual access is a factor.

10. MISCELLANEOUS OPENINGS. The following requirements apply to LAs, Vaults, VTRs, PAs, and MAAs.

a. Barriers or detection are required for all miscellaneous openings penetrating security area boundaries for which the opening is larger than 619.20 square centimeters (96 square inches) in area and larger than 15.24 centimeters (6 inches) in the smallest dimension.

b. Detection and/or barrier designs for miscellaneous openings must be addressed in the SP. At a minimum, barriers must be;

(1) 9 gauge wire mesh;

(2) 9 gauge expanded metal; or,

(3) Solid steel bars at least 1.3 centimeters (0.5 inches) in diameter secured in a way to prevent unauthorized removal e.g., welded vertically and horizontally 15.24 centimeters (6 inches) on center.

c. Alternate barriers providing equivalent or greater protection must be supported by a documented analysis.

d. The delay material must be securely fastened to preclude removal.

e. Where used, wire mesh, expanded metal, or solid steel bars must be mounted so that classified matter or SNM cannot be removed.

f. When pipe or conduit pass through a wall, the annular space between the sleeve and the pipe or conduit must be filled with permanent material that would leave evidence of surreptitious removal of the pipe or conduit.

CHAPTER VII. SECURE STORAGE

The intent of this Chapter is to prescribe requirements for secure storage of certain Departmental assets.

1. GENERAL REQUIREMENTS.

   a. Classified Storage. The storage requirements for classified matter, including non-conforming storage can be found in DOE O 471.6, *Information Security*, current version.

   b. Classified Conference Rooms. Conference rooms and other similar facilities approved for classified discussions/processing must be located in a LA or higher and implement the provisions of DOE O 470.6, *Technical Security Program*, current version.

   c. Vaults and VTRs.

      (1) IDS must be installed in accordance with Attachment 6, Chapter II of this Order.

      (2) When used as storage all perimeter doors must be secured using locks as required by Chapter V of this Attachment (does not apply to emergency egress only doors).

      (3) Access to vaults and VTRs must be strictly controlled and based on an appropriate access authorization and need to know.

      (4) Means of controlling access must be documented in an SP.

      (5) Access controls at vaults and VTRs must provide logging or recording of all entries.

         (a) In vaults and VTRs utilizing vestibules/foyers (where no access to SNM or classified is possible), logging entry is not required unless entry is made into the vault or VTR.

         (b) Where PACS is not used, the ODFSA may waive the requirement for repeated logging for personnel whose offices are located within the boundary of the vaults and VTRs.

      (6) Persons without need to know or the appropriate access authorization must be escorted at all times.

         (a) Entries must be logged or recorded and must include the name and date/time of entry and exit of the individual and the escort.

(b) Protective measures to mask classified matter must be used before visitors or cleared persons without need to know are granted access.

(7) Vault and VTR doors must remain closed and controlled at all times. When a door needs to be open, it must be continually monitored by an authorized and cleared individual.

2. VAULTS AND VAULT TYPE ROOMS. The following minimum standards are required for all new construction, renovations, alterations, modifications and repairs that impact the integrity of the structure of vaults and VTRs.

a. Approval. The ODFSA must approve all construction and the methods used before the storage of classified matter or other S&S interests is authorized.

b. Vaults.

(1) Vault construction must comply with Class A from Federal Standard (FED-STD-832), *Construction Methods and Materials for Vaults*.

(2) A modular vault meeting Class B of FED-STD-832 may be used in lieu of a vault.

c. VTR. VTR construction standards must comply with the following requirements.

(1) The perimeter walls, floors, and ceiling must be permanently constructed and attached to one another.

Walls that constitute exterior barriers must extend from the true floor to the true ceiling unless equivalent means are used to provide evidence of penetration of the security area or access to the security interest being protected (see (10) and (11) below).

(2) The walls, floor, ceiling and door and door frame must be constructed of materials which provide comparable penetration resistance.

(3) All construction must be done in a manner that provides visual evidence of unauthorized penetration. Evidence of unauthorized penetration may consist of damaged surfaces, missing paint, and suspicious patching inconsistent with surrounding finishes.

(4) Floor and wall construction materials must offer resistance to and evidence of unauthorized entry into the VTR.

(5) For floors and walls, if insert type panels are used, a method must be devised to prevent their removal without leaving visual evidence of tampering.

(6) Should any of the outer walls/floors or ceilings be adjacent to space where security is not controlled by DOE, the walls must be constructed of or reinforced with more substantial building materials such as brick, concrete, corrugated metal, wire mesh, etc.

(7) Windows that can be routinely opened and are installed at a height of less than 5.48 meters (18 feet) from any point adjacent to the window that would permit unrestricted access must be:

(a) Provided with protective measures to delay or deter entry or to notify the response force of an attempted entry.

(b) During non-working hours, the windows must be closed and securely fastened to preclude surreptitious entry.

(8) If visual access is a security concern,

(a) Barrier walls must be opaque or translucent;

(b) Windows must be closed and locked and must be translucent or opaque; and,

(c) Doors that have windows, door louvers, baffle plates or service panels, or similar openings must be covered with translucent or opaque coverings.

(9) Perimeter doors must be of wood or metal.

(a) Wooden doors must be of solid core construction, 4.445 centimeters (1.75 inches) thick, or at a minimum faced on the exterior side with at least 16-gauge sheet metal.

(b) Hardware must be fastened in such a way to reveal or preclude surreptitious removal and to ensure visual evidence of tampering.

(c) Hardware accessible from outside the area must be peened, pinned, brazed, or spot welded to preclude removal.

(d) Doors that have windows, door louvers, baffle plates or service panels, or similar openings must be secured with 18 gauge expanded metal or wire mesh fastened inside the VTR to preclude unauthorized entry.

(e) When doors are used in pairs, an astragal or mullion must be installed where the doors meet. Both doors must be locked/secured.

(f) Emergency egress doors (when not used for ingress) must be locked (level I lock not required) in accordance with NFPA 101 *Life Safety Code* and have no exterior hardware.

(10) Ceilings.

(a) When barrier walls do not extend to the true ceiling and a false ceiling is created, the false ceiling must be reinforced with 18 gauge expanded metal or wire mesh to serve as a true ceiling or ceiling tile clips must be secured.

1 Any wire mesh or expanded metal used must overlap the adjoining walls and be secured to show evidence of any tampering.

2 When ceiling tile clips are used, a minimum of four clips per tile must be installed.

3 If the ceiling tile cannot accommodate four clips, the maximum number of clips that can be accommodated on the tile must be used.

4 The clips must be installed from the interior of the area, and each clip must be mounted to preclude surreptitious entry.

5 If 1-4 above cannot be met, IDS must be used above the ceiling tile.

(b) In some instances, it may not be practical to erect a solid suspended ceiling as part of the VTR. In such cases, IDS must be used to ensure that the area cannot be entered surreptitiously.

(11) When barrier walls do not extend to the true floor and a raised/false floor greater than 15.24 centimeters (6 inches) is created, the IDS is required below the raised floor.

CHAPTER VIII. ENTRY/EXIT SCREENING

The intent of this Chapter is to prescribe the requirements for the Department's random entry and exit screening program.

1. GENERAL REQUIREMENTS. Inspections are mandatory at PAs and MAAs (see Attachment 5, Chapter II), random inspections may be conducted at other designated areas.

    a. The ODFSA must determine the need and approve the scope and locations of screening programs at PPAs and LAs.

    b. Screening programs must be documented in the SP.

2. IMPLEMENTATION. Where implemented the entry/exit inspection program must be documented in an SP or procedure. Screening programs must include the following:

    a. Entry Inspections. Searches of personnel, vehicles, and all hand carried items must be performed to deter and detect prohibited article introduction.

    b. Exit Inspections. Personnel, vehicles, and all hand carried items must be inspected to deter and detect unauthorized removal of classified matter or other S&S interests from designated security areas.

CHAPTER IX. DOE SECURITY AND LOCAL SITE SPECIFIC BADGE PROGRAM

The intent of this Chapter is to prescribe requirements for the Department's Security badges.

1. GENERAL REQUIREMENTS. Security badges are used to support physical access control operations at DOE facilities. The DOE security badge is the Homeland Security Presidential Directive 12 (HSPD-12) *Personal Identification Verification* (PIV) credential, which establishes a mandatory, Federal government-wide standard for identification and physical access to Federally controlled facilities.

   a. Site specific requirements and procedures for receiving and escorting visitors must be developed and approved by DOE line management or the ODFSA and documented in the site's SP.

   b. Visitors not possessing PIV credentials must present a state-issued driver's license or identification card that is compliant with the REAL ID Act of 2005.

   c. If the visitor does not possess a state-issued driver's license or identification that is compliant with the REAL ID Act then the individual must present an acceptable document to establish identity following instructions listed on the Department of Homeland Security (DHS) Form I-9, "Employment Eligibility Verification" (see http://www.uscis.gov/i-9 and http://www.tsa.gov/traveler-information/acceptable-ids).

      The following alternate access control procedures, as identified in the DHS REAL ID Implementation Guide, if implemented must be approved by the ODFSA when a REAL ID compliant form of identification is not presented for access:

      (1) Escort of a visitor listed in a visitor control log without having to present ID; or,

      (2) Escort of a visitor presenting a non-compliant driver's license or ID; or

      (3) Use of a knowledge-based authentication to establish identity.

   d. Use of the DOE badges with PACS is described in Attachment 6, Chapter 1 of this Order.

   e. DOE PIV and Local Site Specific Only (LSSO) badges must display the holder's access authorization level.

2. DOE BADGES.

   a. DOE PIV Credentials.

      (1) The DOE PIV credential must be issued to all Federal employees and contractor employees who require long term (greater than six months) physical access to DOE facilities or information systems. Logical access

falls under the purview of the Chief Information Officer. Physical access falls under the purview of DOE Office of Environment, Health, Safety, and Security.

(2) The DOE PIV credential must be recognized for physical access at all DOE sites and facilities.

(3) The identity verification and issue process is described in FIPS 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*.

(4) Specifications for the DOE PIV credential are described in National Institute of Standards and Technology (NIST) 800-73 and FIPS 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*.

b. Local Site Specific Only (LSSO) Badges.

(1) When necessary to facilitate temporary (less than six months), or non-routine access, DOE line management or Officially Designated Federal Security Authority (ODFSA) may authorize the issuance of Local Site-Specific Only (LSSO) badges for physical access as documented in the approved Security Plan (SP). LSSO Badges may be developed and issued to address a variety of issues and unique local badging requirements. Example scenarios where this might apply include facility access cards issued to short term and non-routine individuals (e.g., employees with forgotten/misplaced PIV, summer interns, vendors).

(a) If LSSOs are used, the design, issuance, accountability and return process must be documented.

(b) LSSO badges must not resemble the design or color of the DOE PIV credential.

(c) LSSOs must not be recognized outside the jurisdiction of the cognizant ODFSA.

(d) For ongoing construction projects longer than six months, contractors may be issued an LSSO badge providing access to the construction area.

1 Provided they are not permanently assigned to another DOE facility; and

2 Do not require unrestricted physical access to other Departmental assets, security areas, and buildings; and

3 Have received a favorably adjudicated HSPD-12 Federal background investigation.

(2) Military and other Federal department and agency personnel who possess PIV credentials and who are assigned/detailed to DOE must have their badge enrolled in the appropriate DOE PACS, where possible, or issued an LSSO badge.

(3) Military and other Federal department and agency personnel who possess HSPD 12 credentials/badges issued by their respective organizations may, at the discretion of the DOE cognizant office, be permitted entry to a PPA without further badging.

(a) Even though the person possesses an HSPD 12 credential/badge, issued by another Federal department or agency, the local visitation process must be followed.

(b) If there is a requirement for entry beyond a PPA or access to SNM, nuclear weapons, or classified matter, the provisions of paragraph (4) below must be followed.

(4) Visitors possessing a commensurate access authorization who require access to a LA, PA, MAA, SNM, nuclear weapons or classified matter must verify identity and appropriate access authorization in accordance with local procedures or submit a DOE F 5631.20, *Request for Visit or Access Approval*, prior to arriving at the site. Visitors may be issued a temporary LSSO badge for the visit.

c. Foreign National Badges.

(1) Foreign Nationals who have been in the United States for three or more continuous years and require access longer than six months must be issued a DOE PIV credential, in accordance with FIPS 201-2. Foreign National access must be processed in accordance with DOE O 142.3, *Unclassified Foreign Visits and Assignments Program* prior to issuance of the PIV.

(2) Foreign Nationals who have been in the United States for less than three years and require access longer than six months may be issued an LSSO at the discretion of the Secretarial Program Office based on a risk determination. The risk determination must be documented and based on the results of the following:

(a) FBI fingerprint based National Criminal History Check (NCHC),

(b) FBI Investigations files (Name Check),

(c) Name check against the Terrorist Screening database,

(d) USCIS Check against SAVE, and,

(e) Any additional requirements in DOE O 142.3, *Unclassified Foreign Visits and Assignments Program*

(3) Foreign Nationals may be issued an LSSO badge for access less than six months for unclassified site access after an identity verification process has been completed by the foreign visits and assignments staff of the organization sponsoring the visit in accordance with DOE O 142.3, *Unclassified Foreign Visits and Assignments* Program prior to issuance of the badge.

3. EMERGENCY RESPONSE OFFICIAL (ERO). Personnel designated by their organizations as EROs as described in FIPS 201-2, can be issued a DOE PIV credential with the words "Emergency Response Official" in accordance with FIPS 201-2.

4. ISSUANCE, USE, RECOVERY, AND DESTRUCTION OF DOE PIV AND LSSO BADGES.

a. Procedures. DOE line management or ODFSA must approve local procedures for issuance, use, accountability, and return of DOE PIV credentials and LSSO badges.

(1) DOE PIV credentials must be processed and issued in accordance with FIPS 201-2.

(2) Measures must be taken to ensure that a single individual cannot process and/or issue an LSSO badge allowing unauthorized access.

(3) Personnel with the ability to edit access to security areas, authentication mechanism data, security access authorization data in badging systems must be cleared at the same level as the highest access authorization in the system.

(4) Sites must implement procedures to control access to security systems that maintain badging and clearance information.

(5) The information on the badge must not be used for any purpose other than access control (physical or logical).

(6) The information on the badge must not be collected or stored outside of DOE access control systems without prior authorization in accordance with established procedures for the control and protection of the information.

b. Individual Changes of Appearance. A DOE badge must be confiscated and reissued, with a new photograph, if the individual's appearance no longer resembles the person in the photograph.

c. Badge Holder Name Change. A DOE badge must be replaced when the badge holder's name is legally changed.

d. Recovery of DOE Badges. Local procedures, approved by the ODFSA, must be established for the recovery of the badge whenever an individual has terminated employment, their access authorization status changes, or they no longer require the badge.

e. Badge Destruction. DOE badges that are deactivated or no longer needed must be destroyed so that the badge cannot be reconstructed.

(1) If destruction is not immediate, badges must be stored at a minimum, in a locked container until they can be destroyed.

(2) DOE PIV credential must be destroyed in a manner approved by Federal Information Processing Standard (FIPS) FIPS 201-2, *Personal Identity Verification of Federal Employees and Contractors*.

5. ACCOUNTABILITY OF DOE BADGES.

a. The issuing office must maintain badging records to include the badge number; date of issuance; badge holder's name and organization; and the date of destruction, when applicable.

b. A record of missing DOE badges must be maintained.

(1) Personnel and/or systems controlling access to DOE security areas must be provided current information regarding missing badges to prevent badge misuse.

(2) The theft or loss and recovery of DOE issued security badges must be reported immediately in accordance with locally approved procedures.

c. Records must be maintained in accordance with the requirements of the local records management program. Personal data must be protected from loss or compromise (see 5 U.S.C. 522a).

6. PROTECTION OF DOE BADGE MATERIALS AND EQUIPMENT. Stocks of badging materials, unissued DOE PIV credentials and LSSO badges, and processing equipment must be stored in a locked room, filing cabinet or GSA approved container.

7. DOE BADGE VALIDATION. Badge validation procedures at access control points must be documented in the SP.

a. Badge validation procedures must be performed by PACS or physical examination of the DOE badge. For PIV credential, physical examination must be performed in accordance with FIPS 201-2.

b. Other methods of validation for LSSO badges may be approved by the ODFSA.

8. DOE BADGE RECIPIENT REQUIREMENTS. A written or electronic record of acknowledgement must be provided by the badge recipient of the following responsibilities.

a. Protecting the DOE PIV Credential through the use of only FIPS-201-2 compliant badge holders.

b. Protecting the DOE PIV credential/LSSO security badge against loss, theft, or misuse.

c. Reporting a lost, stolen, or misused badge to the issuing office within 24 hours of discovery.

d. Protecting its integrity by ensuring that the badge is not altered, photocopied, counterfeited, reproduced, or photographed (other than for official government business).

e. Returning the DOE PIV credential/LSSO badge when it is no longer valid or required.

f. Surrendering or returning the DOE PIV credential/LSSO badge when requested according to local procedures.

g. Wearing the DOE PIV credential/LSSO badge conspicuously, photo side out, in a location above the waist and on the front of the body while having access to DOE facilities. (This requirement may be modified for operational or safety reasons.)

h. When not on Federally controlled, owned, or leased property the badge should be removed or obscured from visual access. This does not preclude the use for identification purposes as necessary.

ATTACHMENT 3. PHYSICAL PROTECTION FOR PL-7 AND PL-8 ASSETS

The intent of this Attachment is to prescribe protection requirements for PL-7 and PL-8 assets. These are departmental assets that do not meet the criteria for other PLs. These requirements are in addition to those physical protection requirements outlined in Attachment 2 of this Order.

CHAPTER I. PHYSICAL PROTECTION FOR PL-7 ASSETS

1. GENERAL REQUIREMENTS.

   a. A facility must not possess, receive, process, transport, or store safeguards and security assets until that facility has been cleared (see DOE O 470.4, current version).

   b. The protection strategy of PL-7 assets is order compliance. The following require an SRA: PL-7 high value assets (as defined by Program Secretarial Officers), non-conforming storage of classified matter, noncompliant storage of Category III or IV SNM, or SNM as part of a roll-up analysis. The objectives of the protection strategy used for PL-7 assets requiring an SRA are:

      (1) Protection;

      (2) Mitigation;

      (3) Incident Response; and

      (4) Mission Recovery.

2. BIOLOGICAL AGENTS. PL-7 assets identified as biological agents requiring biosafety level (BSL)-1 or -2 or animal biosafety level (ABSL)-1 or -2 must meet the following requirements as applicable:

   a. 42 CFR § 73, *Select Agents and Toxins*, contains two lists of agents and toxins regulated by HHS/CDC (Centers for Disease Control and Prevention of the Department of Health and Human Services): 1) HHS Select Agents and Toxins (42 CFR § 73.3); and 2) Overlap Select Agents and Toxins (42 CFR § 73.4).

   b. 7 CFR § 331, *Possession, Use, and Transfer of Select Agents and Toxins*, contains a list of Plant Protection and Quarantine (PPQ) Programs of the Animal and Plant Health Inspection Service (APHIS), Select Agents and Toxins (7 CFR § 331.3(b)).

   c. 9 CFR § 121, Use, and Transfer of Select Agents and Toxins, contains two lists: 1) Veterinary Services Programs (VS) of the APHIS, Select Agents and Toxins(9 CFR § 121.3(b)); and 2) Overlap Select Agents and Toxins (9 CFR § 121.4(b)) .For more information, see DOE G 151.1-5, *Biosafety Facilities Emergency Management Guide*, current version.

3. CATEGORY III SNM. PL-7 assets identified as Category III SNM must meet the following requirements:

   a. SNM must be used or processed within at least a LA in accordance with security procedures documented in a Security Plan (SP).

b. Protect with barriers designed to mitigate the DBT adversary's capabilities.

c. SNM must be stored within a locked security container or room, either of which must be located within at least a LA in accordance with security procedures documented in a SP.

(1) The container or room must be protected by IDS in accordance with Attachment 6, Chapter II of this Order or by protective force (PF) patrol physical check at least every eight hours.

(2) The container or room must be secured with Level II locks.

d. Control access with PACS in accordance with Attachment 6, Chapter 1 of this Order or equivalent means and documented in an approved SP.

e. Category III quantities of SNM may be transported by the following methods unless otherwise prohibited by statute (see DOE O 460.2, *Departmental Materials Transportation and Packaging Management*, current version).

(1) Classified nuclear explosive parts, components, special assemblies, sub critical test devices, trainers or shapes containing no fissile nuclear material or less than Category II quantities of fissile nuclear material must be shipped consistent with both DOE policy governing protection of classified matter and Department of Transportation regulations governing interstate transportation.

(2) Domestic offsite shipments of classified configurations of Category III quantities of SNM must be made by OST or by an OST approved commercial carrier that meets the requirements listed below in (3)(a)-(e).

(3) Offsite shipments of unclassified configurations of Category III quantities of SNM are not required to be made by OST. If OST is not used, the shipments may be made by the following means:

(a) Government owned or exclusive use truck, commercial carrier, or rail may be used.

1 Transport vehicles must be inspected by authorized personnel before loading and shipment.

2 Cargo compartments must be locked and sealed after the inspection and remain sealed while en route.

3 Shipment escorts must periodically communicate with a control station operator.

4 The control station operator must be capable of requesting appropriate local law enforcement agency (LLEA) response if needed.

(b) Air shipments must be under the direct observation of the authorized escorts during all land movements and loading and unloading operations.

(4) Requirements for movement between security areas at the same site must be developed and documented in the approved SP.

4. CATEGORY IV SNM. PL-7 assets identified as Category IV SNM must meet the following requirements:

a. SNM must be stored, used or processed within at least a PPA in accordance with security procedures documented in a SP.

b. Protect with barriers designed to mitigate the DBT adversary's capabilities.

c. Secure with Level III locks and keys, including while in transit.

d. Control access either utilizing PACS in accordance with Attachment 6, Chapter 1 of this Order, or Level III locks and keys.

e. Category IV quantities of SNM may be transported by the following methods unless otherwise prohibited by statute:

(1) Domestic offsite shipments of classified configurations of Category IV quantities of SNM may be made by the OST or by other means when approved by DOE line management or ODFSA.

(2) Shippers are required to give the consignee an estimated time of arrival before dispatch and to follow up with a written confirmation not later than 48 hours after dispatch.

(3) Consignees must promptly notify the shipper by telephone and written confirmation upon determination that a shipment has not arrived by the scheduled time.

(4) Shipments must be made by a mode of transportation that can be traced, and within 24 hours from request, the carrier be capable of reporting the last known location of the shipment should it fail to arrive on schedule.

5. OTHER ACCOUNTABLE NUCLEAR MATERIAL. PL-7 assets identified as Other Accountable Nuclear Material as referenced by the DBT and defined by DOE O 474.2, *Nuclear Material Control and Accountability*, current version, must be protected in accordance with local security procedures documented in a SP, based on analysis:

6. RADIOLOGICAL MATERIALS. Protection of PL-7 assets identified as radiological materials as defined by the DBT (Appendix A, 2.g.5) must be protected in accordance with local security procedures documented in a SP, based on analysis:

7. CHEMICALS. PL-7 assets identified as chemical assets as defined by the DBT (Appendix A 2.g.6) must be protected in accordance with local security procedures documented in a SP, based on analysis.

8. GOVERNMENT PROPERTY AND FACILITIES. PL-7 assets identified as Government property and facilities must be protected in accordance with the applicable requirements in this Order.

9. CLASSIFIED OR CONTROLLED UNCLASSIFIED INFORMATION (CUI).

   a. PL-7 assets identified as classified matter must be protected with Level I locks and meet the requirements of DOE O 471.6, *Information Security*, current version, and Attachment 3 of this Order.

   b. PL-7 assets identified as CUI within the Department consists of:

      (1) Unclassified Controlled Nuclear Information (UCNI) which, must be protected in accordance with 10 CFR 1017 Subpart E, *Physical Protection* Requirements, and DOE O 471.1, *Identification and Protection of Unclassified Controlled Nuclear Information (UCNI)*, current version.

      (2) Official Use Only (OUO), which encompasses Personally Identifiable Information (PII) and other unclassified sensitive information not governed by specific directives. OUO must be protected in accordance with DOE O 471.3, *Identification and Protecting of Official Use Only Information*, current version. It will be subject to the Freedom of Information Act (FOIA), 5 U.S.C. 552, and applicable exemptions may apply if requested.

CHAPTER II. PHYSICAL PROTECTION FOR PL-8 ASSETS

1. GENERAL REQUIREMENTS. PL-8 assets are defined in the DBT as Departmental Federal employees, contractors, and the general public on Departmental property. This also includes childcare centers physically located on Departmental property, visitor centers, and government leased properties.

   a. The protection strategy of PL-8 assets is order compliance.

   b. When planning protection measures for workplace violence and active shooter events, the adversary characteristics, capabilities and scenarios described in the DBT for PL-8 must be used.

   c. Protection measures may be implemented using Departmental or non-Departmental resources (e.g., local law enforcement, commercial alarm monitoring, local fire department, and hazard material response). Additional measures may be applied based on local analyses.

ATTACHMENT 4. PHYSICAL PROTECTION FOR PL-5 AND PL-6 ASSETS

The intent of this Attachment is to provide the baseline physical protection requirements for PL-5 and PL-6 assets. These requirements are in addition to those physical protection requirements outlined in Attachment 2 of this Order.

CHAPTER I. PHYSICAL PROTECTION FOR PL-5 ASSETS

1. GENERAL REQUIREMENTS. PL-5 assets are assets designated as part of the United States National Critical Infrastructure as defined in Presidential Policy Directive-21, *Critical Infrastructure Security and Resilience*. PL-5 assets also include facilities with significant radiological, chemical, or biological sabotage targets, and have off-site consequences.

   a. Protection measures must be designed to mitigate the adversary scenarios and capabilities for PL-5 described within the DBT.

   b. An SRA is required for PL-5 assets. Additional requirements may be established by the Program Secretarial Office or Power Marketing Administration (PMA) as determined by the results of the SRA.

   c. The protection strategy objective for PL-5 assets is order compliance. The four elements below must be addressed in the SP or in the analyses that support the SP:

      (1) Protection;

      (2) Mitigation;

      (3) Incident Response; and

      (4) Mission Recovery.

   d. Boundaries must be defined by physical barriers (fences, buildings, rooms, containment structures, etc.) encompassing the designated space containing the asset with access controls to ensure that only authorized personnel are allowed to enter the area containing the asset.

   e. Intra-site transportation procedures must be covered in the SP.

2. NATIONAL CRITICAL INFRASTRUCTURE. PL-5 assets designated as national critical infrastructure as defined in the DBT must meet the following requirements:

   a. Deter cyber sabotage by preventing unauthorized on-site or remote access to critical process controls.

   b. Deter insider sabotage which would result in a release of chemicals offsite by employing measures established by the ODSA and documented in a SP approved by the ODFSA.

   c. Control access to the asset by either utilizing PACS in accordance with Attachment 6, Chapter 1 of this Order, or through the use of Level I locks and keys**.**

d. Protect vehicle avenues of approach with barriers designed to mitigate the DBT adversary's capabilities based on the results of the SRA.

e. Monitor with IDS in accordance with Attachment 6, Chapter II of this Order, or monitor using authorized personnel**.**

f. Ensure that site security participates in coordinating an emergency response that supports a documented Emergency Management program that provides a foundation for planning, preparedness, response, recovery, and readiness assurance to respond to/recover from incidents involving these assets.

3. RADIOLOGICAL MATERIALS. PL-5 assets identified as radiological or nuclear materials defined in the DBT must meet the following requirements:

a. Control access to the asset either utilizing PACS in accordance with Attachment 6, Chapter 1 of this Order, or through the use of Level I locks and keys.

b. Deter insider sabotage which would result in a release of chemicals offsite by employing measures established by the ODSA and documented in a SP approved by the ODFSA

c. Protect with barriers designed to mitigate the DBT adversary's capabilities, as required, based on the results of the SRA.

d. Monitor via IDS in accordance with Attachment 6, Chapter II of this Order, or monitor using authorized personnel.

e. Ensure that site security participates in coordinating an emergency response that supports a documented Emergency Management program that provides a foundation for planning, preparedness, response, recovery, and readiness assurance to respond to/recover from incidents involving these assets.

4. BIOLOGICAL AGENTS AND SELECT AGENTS AND TOXINS. PL-5 assets identified as biological agents and select agents and toxins as defined by the DBT must meet the requirements contained in the following national and departmental policies:

a. 42 CFR § 73, *Select Agents and Toxins*, contains two lists of agents and toxins regulated by HHS/CDC: 1) HHS Select Agents and Toxins (42 CFR § 73.3); and 2) Overlap Select Agents and Toxins (42 CFR § 73.4).

b. 7 CFR § 331, *Possession, Use, and Transfer of Select Agents and Toxins*, contains a list of Plant Protection and Quarantine Programs (PPQ) of the Animal and Plant Health Inspection Service (APHIS), Select Agents and Toxins (7 CFR § 331.3(b)).

c. 9 CFR § 121, , Use, and Transfer of Select Agents and Toxins, contains two lists: 1) Veterinary Services Programs (VS) of the APHIS, Select Agents and Toxins (9 CFR § 121.3(b)); and 2) Overlap Select Agents and Toxins (9 CFR § 121.4(b)).

d. DOE Policy 434.1, *Conduct and Approval of Select Agent and Toxin Work at DOE Sites*, current version.

e. For more information, see CDC guidance from *Biosafety in Microbiological and Biomedical Laboratories* and DOE Guide 151.1-5, *Biosafety Facilities*, current version.

f. Ensure that site security participates in coordinating an emergency response that supports a documented Emergency Management program that provides a foundation for planning, preparedness, response, recovery, and readiness assurance to respond to/recover from incidents involving these assets.

5. CHEMICALS. Chemicals with PL-5 consequences must be protected in accordance with the requirements below and as required based on the results of an SRA. Chemicals typically found on DOE facilities are identified here: https://edms.energy.gov/pac/TeelDocs.

PL-5 assets identified as chemical assets as defined by the DBT must be protected by/contained within areas meeting the following requirements:

a. A boundary must be established to protect the asset.

b. The boundary must be defined by physical barriers that may include fences, buildings, rooms, or other barriers that surround the asset.

c. A means of intrusion detection and surveillance must be provided for protection of the asset. The level of intrusion detection and surveillance must be based on the results of the SRA for the asset.

d. Deter vehicles from penetrating the perimeter of the area where the asset is stored, gaining unauthorized access or otherwise presenting a hazard to potentially critical targets.

e. Be stored in a location that is secured with Level I locks.

f. Approved procedures must be in place to monitor the shipping, receipt, and storage of hazardous materials within the facility.

g. Deter insider sabotage that would result in a release of chemicals offsite by employing measures established by the ODSA and documented in a SP approved by the ODFSA including:

(1) Limit access to authorized individuals,

(2) Provide access control by using PACS in accordance with Attachment 6, Chapter I, or authorized personnel,

(3) Control visitor access as documented in the approved SP,

(4) Provide tamper-resistant storage of the chemical.

h. Deter cyber sabotage by preventing unauthorized on-site or remote access to critical process controls.

i. Maintain effective monitoring, communications, and warning systems.

j. Ensure proper security training of facility personnel is specific to the assets being protected.

CHAPTER II. PHYSICAL PROTECTION FOR PL-6 ASSETS

1. GENERAL REQUIREMENTS. PL-6 assets are assets designated as critical program assets or facilities; radiological, chemical, or biological materials; or assets determined to be sabotage targets with on-site consequences as defined in the DBT.

   a. Protection measures must be designed to mitigate the adversary scenarios and capabilities for PL-6 described within the DBT.

   b. An SRA is required for PL-6 assets. Additional requirements may be established by the Program Secretarial Office or PMA as determined by the results of the SRA.

   c. The protection strategy objective for PL-6 assets is order compliance. The four elements below must be addressed in the SP or in the analyses that support the SP:

      (1) Protection;

      (2) Mitigation;

      (3) Incident Response; and

      (4) Mission Recovery.

   d. Boundaries must be defined by physical barriers (fences, buildings, rooms, containment structures, etc.) encompassing the designated space containing the asset with access controls to ensure that only authorized personnel are allowed to enter the area containing the asset.

   e. Intra-site transportation procedures must be covered in the SP.

2. CRITICAL PROGRAM ASSETS. PL-6 assets designated as critical program assets as defined in the DBT must meet the following requirements:

   a. Control access either utilizing PACS in accordance with Attachment 6, Chapter 1 of this Order, or Level II locks and keys.

   b. Monitor with IDS in accordance with Attachment 6, Chapter II of this Order, or monitor using authorized personnel based on the results of an SRA.

   c. Deter cyber sabotage by preventing unauthorized on-site or remote access to critical process controls.

   d. Ensure that site security participates in coordinating an emergency response that supports a documented Emergency Management program that provides a foundation for planning, preparedness, response, recovery, and readiness assurance to respond to/recover from incidents involving these assets.

e. Deter insider sabotage would result in sabotage of critical program assets by employing measures established by the ODFSA and documented in a SP.

3. RADIOLOGICAL MATERIALS. PL-6 assets identified as radiological or nuclear materials defined in the DBT must meet the following requirements:

a. Protect with barriers designed to mitigate the DBT adversary's capabilities based on the results of an SRA.

b. Control access either utilizing PACS in accordance with Attachment 6, Chapter 1 of this Order, or Level II locks and keys.

c. Monitor via IDS in accordance with Attachment 6, Chapter II of this Order, or monitor using authorized personnel.

d. Ensure that site security participates in coordinating an emergency response that supports a documented Emergency Management program that provides a foundation for planning, preparedness, response, recovery, and readiness assurance to respond to/recover from incidents involving these assets.

e. Intra-site transportation procedures must be covered in the SP.

4. BIOLOGICAL AGENTS. PL-6 assets identified as Biological agents as defined by the DBT must meet the requirements contained in the following national policies:

a. 42 CFR § 73, *Select Agents and Toxins*, contains two lists of agents and toxins regulated by HHS/CDC: 1) HHS Select Agents and Toxins (42 CFR § 73.3); and 2) Overlap Select Agents and Toxins (42 CFR § 73.4).

b. 7 CFR § 331, *Possession, Use, and Transfer of Select Agents and Toxins*, contains a list of Plant Protection and Quarantine Programs (PPQ) of the Animal and Plant Health Inspection Service (APHIS), Select Agents and Toxins (7 CFR § 331.3(b)).

c. 9 CFR § 121, Use, and Transfer of Select Agents and Toxins, contains two lists: 1) Veterinary Services Programs (VS) of the APHIS, Select Agents and Toxins(9 CFR § 121.3(b)); and 2) Overlap Select Agents and Toxins (9 CFR § 121.4(b))

d. DOE Policy 434.1, *Conduct and Approval of Select Agent and Toxin Work at DOE Sites*, current version.

e. For more information see CDC guidance from Biosafety in Microbiological and Biomedical Laboratories and DOE Guide 151.1-5, *Biosafety Facilities*, current version.

Ensure that the site has established a documented Emergency Management program that provides a foundation for planning, preparedness, response, recovery, and readiness assurance to respond to/recover from incidents involving these assets.

5. CHEMICALS. Chemicals with PL-6 consequences must be protected in accordance with the requirements below and as required based on the results of an SRA. Chemicals typically found on DOE facilities are identified here: https://edms.energy.gov/pac/TeelDocs.

   a. Monitor with IDS or authorized personnel.

   b. Control access either utilizing PACS in accordance with Attachment 6, Chapter 1 of this Order, or Level II locks and keys.

   c. Deter vehicles from gaining unauthorized access to the asset.

   d. Secure and monitor the shipping, receipt, and storage of hazardous materials for the facility.

   e. Deter insider sabotage which would result in a release of chemicals onsite by employing measures established by the ODSA and documented in an approved SP.

   f. Deter cyber sabotage by preventing unauthorized on-site or remote access to critical process controls.

   g. Maintain effective monitoring, communications, and warning systems.

   h. Ensure proper security training of facility personnel specific to the assets being protected.

ATTACHMENT 5. PHYSICAL PROTECTION OF PL 1-4 ASSETS

The intent of this Attachment is to prescribe the physical protection requirements for PL-1 through PL-4 assets. These requirements are in addition to those physical protection requirements outlined in Attachments 2 and 6.

CHAPTER I. PROTECTION OF PL-1 THROUGH PL-4 ASSETS

The intent of this Chapter is to establish requirements for physical protection of PL-1 through PL-4 assets consistent with the DBT.

1. GENERAL REQUIREMENTS. The requirements cited in this Chapter apply to fixed facilities and not the conduct of onsite movement of SNM or operations managed by OST.

   a. Protection of PL-1 through PL-4 assets must be based on the results of a vulnerability analysis (VA) as required by DOE O 470.3, *Design Basis Threat*, current version.

   b. Roll-up is the accumulation of lower categories of SNM to attain a higher Category of SNM. SNM must be protected at the higher level when roll up to Category I or II quantities can occur on site unless the facility has conducted an analysis that determined roll up is not credible.

   c. Protection measures must be designed to prevent malevolent acts and to respond to adverse conditions such as emergencies caused by acts of nature.

      (1) An integrated system of protection measures must be developed, documented, and implemented to protect PL-1 through PL-4 assets.

      (2) Protection measures must address physical protection strategy (i.e., denial or containment) as well as recapture, recovery, and/or pursuit by an armed PF.

   d. A facility must not possess, receive, process, transport, or store nuclear weapons or SNM until that facility has been issued a facility clearance. (see DOE O 470.4B, Appendix B, Section 1).

2. FACILITIES WITH PL-1 THROUGH PL-3 ASSETS. PL-1 through PL-3 assets must be located within a Material Access Area (MAA).

   a. Any MAA containing unattended (not in use/processing) PL-1 through PL-3 assets must be equipped with an IDS, or detection must be provided by the PF.

   b. PL-1 assets must be stored in a vault within an MAA. Storage facilities constructed after July 15, 1994, must be built below grade i.e., underground.

   c. PL-2 assets must be stored in a vault within an MAA; however, certain operational activities may dictate other storage configurations. These storage configurations must be supported by a VA and approved by the appropriate Federal risk acceptance official.

   d. PL-3 assets must be stored in a vault or VTR within an MAA.

3. FACILITIES WITH PL-4 ASSETS.

a. PL-4 assets must be located, at a minimum, within a Protected Area (PA).

b. PL-4 assets must be stored in a vault or VTR within a PA; however, certain operational activities may dictate other storage configurations. These storage configurations must be supported by a VA and approved by the appropriate Federal risk acceptance official.

4. PROTECTED AREAS (PAs).PAs are security areas designed to protect PL-1 through PL-4 assets by providing concentric layers of security.

a. PAs must be surrounded by a perimeter intrusion detection and assessment system (PIDAS) (see Attachment 6, Chapter II).

b. PAs must be designed to facilitate assessment.

c. PA entrances (e.g., gates in fences, doors in buildings) must be secured using Level I locks when not under observation by PF.

d. PAs must be designed to mitigate the VBIED threat, as identified in the DBT.

e. PA access control systems must ensure only authorized personnel are allowed to enter and exit (see Attachment 6, Chapter I).

(1) Unescorted access must be limited to individuals with an appropriate access authorization and for the conduct of official duties.

(2) Individuals without an appropriate access authorization must be escorted.

(a) The ODSA must establish escort to visitor ratios for the PA and document in an approved Security Plan (SP).

(b) Escort responsibilities must be documented in the approved SP.

(c) Escorts must acknowledge understanding of escort responsibilities.

(d) The escort must ensure measures are taken to prevent compromise of classified matter or access to SNM.

(e) Visitors to PAs must be documented in a log or PACS.

(f) Information from visitor logs must be retained in accordance with local records management procedures.

(3) Automated access control at PAs must have anti-passback protection.

f. An inspection program must be developed by the ODSA in accordance with the requirements cited in Chapter II of this Attachment and documented in the approved SP.

g. Vehicles authorized by the ODSA in accordance with local procedures may be admitted as operationally required.

5. MATERIAL ACCESS AREAS. In addition to requirements for a PA the following apply to an MAA:

a. Multiple MAAs may exist within a single PA. MAAs must be located wholly within a PA with no common boundary.

b. MAAs must have barriers that provide sufficient delay to facilitate a timely response, as informed by the results of a vulnerability analysis.

c. While an MAA is required for the protection of Category I quantities of SNM, classified matter may exist within an MAA. In such instances, the classified matter must be stored according to the requirements in DOE O 471.6, *Information Security*, current version.

d. An inspection program must be developed in accordance with the requirements cited in Chapter II of this Attachment.

e. Access control must be administered by armed PF personnel and/or automated physical access control systems.

(1) Automated access control at MAAs must have anti-passback protection.

(2) MAA entrances must be secured using Level I locks when not under observation by PF.

(3) Access must be controlled to limit entry to individuals with an appropriate access authorization and who have been authorized for entry in accordance with local procedures.

(4) Individuals without appropriate access authorization must be escorted.

(a) The ODSA must establish escort to visitor ratios for the MAA and document in an approved SP.

(b) Escort responsibilities must be documented in the approved SP.

(c) Escorts must acknowledge understanding of escort responsibilities.

(d) The escort must ensure measures are taken to prevent compromise of classified matter or access to SNM.

(e) Visitors to MAAs must be documented in a log or PACS.

CHAPTER II. INSPECTION PROGRAMS

The intent of this Chapter is to establish requirements for inspection programs utilized at PA and MAA boundaries.

1. GENERAL. These programs are also intended to protect Department assets and interests from unauthorized removal. An entry/exit inspection program must be documented in an SP.

    a. An inspection program must be established and documented in an approved SP to detect prohibited and controlled articles before being brought into DOE facilities and prevent the unauthorized removal of Departmental assets.

    b. Passage of individuals, vehicles, and/or packages or mail through entry control point inspection equipment must be observed and controlled by trained designated personnel.

    c. Inspection equipment must be used for PAs and MAAs such as x-ray machines, metal detectors, and SNM detectors.

        (1) Uninterruptable power supplies must be provided to all inspection equipment. In those instances where uninterrupted power is not practical, there must be locally developed procedures to provide alternative measures for conducting entry/exit screening when loss of electrical power occurs.

        (2) The testing and configuration of inspection equipment must be documented in the SP approved by the ODFSA.

    d. Entry/exit control points.

        (1) Entry control points must allow the entry and exit of authorized personnel while detecting prohibited and controlled articles.

        (2) Entry control point configuration must allow for the inspection of personnel, packages, and hand carried items.

        (3) Entry/exit point inspection operations and equipment must be collocated with designated permanent PF posts to facilitate the initiation of a timely response to a security event.

        (4) Permanent PF posts must be designed with an unobstructed view to facilitate observation of any attempt to bypass systems.

        (5) Entry/exit points must be alarmed with intrusion detection sensors when not in use or controlled at all times.

(6) Entry/exit points must be designed to preclude commingling of searched and unsearched personnel.

2. ENTRY/EXIT SCREENING EQUIPMENT.

a. Explosives Detection.

(1) Sites must analyze PA and MAA access points to determine whether vulnerability exists for an adversary to use explosives to affect consequences of DOE assets.

(2) Sites must implement protective measures to mitigate the risk of the DBT adversary threat.

(3) These protective measures must be supported by a VA and be included in the overall protection planning process.

(4) If the analysis determines that explosive detection is required, explosive detection measures must ensure that explosives are not introduced without appropriate authorization as described in Attachment 2, Chapter III.

(5) The SP or procedure must document the analysis that establishes a facility's capability to detect explosives and provide protection against the malicious use of explosives.

(6) Documentation must include the rationale for explosive detection measures selection, deployment, and use.

(7) Security procedures for explosive detection measures must be documented in the SP approved by the ODFSA.

b. Metal Detection.

(1) Metal detectors must ensure weapons are not introduced without authorization. (For details on testing and maintenance see Attachment 6, Chapter IV paragraph 3.c.).

(2) Security procedures for metal detection equipment must be documented in site specific procedure(s) or the approved SP.

c. X-ray Machines.

(1) X-ray machines may be used to supplement metal detectors and protective personnel hand searches for prohibited and controlled articles. (For details on testing and maintenance see Attachment 6, Chapter IV paragraph 3.d.).

(2) X-ray machines must provide a discernible image of the prohibited and controlled article.

(3) Security procedures for X-ray machines must be documented in site specific procedure(s) or the approved SP.

d. SNM Detectors.

(1) SNM detectors must be configured to ensure SNM is not removed without authorization. Detection thresholds must be consistent with the SNM type, form, quantity, attractiveness level, size, configuration, portability, and credible diversion amounts of the articles or property contained within the area.

(2) SNM detectors used in the inspection process must be tested using materials with radioactive signatures and strengths consistent with required detection thresholds that depict the type of SNM located within the security area.

(3) Security procedures for SNM detection equipment must be documented in site specific procedure(s) or the approved SP.

3. ENTRY SCREENING. Entrance inspections of personnel, vehicles, packages, and hand carried items must be performed to deter and detect prohibited and controlled articles.

a. Bypass routes around inspection equipment must be closed or monitored to deter unauthorized passage of personnel, prohibited and controlled articles.

b. Measures must be taken to preclude the unauthorized alteration of control settings on all entry/exit control point inspection equipment.

c. Equipment, excluding x-ray machines, must have audible and visual alarms monitored by trained personnel.

d. Measures must be taken to prohibit the commingling of screened individuals from unscreened individuals during the entry screening process.

4. EXIT SCREENING.

a. Personnel, vehicles, and hand carried items including packages, briefcases, purses, and lunch containers are to be inspected to deter and detect unauthorized removal of SNM, classified matter, or other S&S interests from designated security areas.

b. Items to be detected during vehicle screening must be determined by site analysis.

c. Exit inspection procedures must be written to ensure:

(1) SNM and Metal Detectors must be co-located with PF to assist in detection of attempted shielding and/or diversions of SNM.

(2) SNM detectors and metal detectors must be used in a combination that precludes the opportunity to defeat the detectors (e.g., the placement of the metal detector ahead of the SNM detector to prevent use of metal shielding to remove SNM).

(3) Metal detectors, SNM detectors, and x-ray machines used in the exit inspection process must ensure shielded SNM is not removed without authorization.

(4) Specific inspection procedures and response to alarms with limitations and thresholds for the various detectors must be established and documented in the SP or procedure.

(5) The identification of detection thresholds for the various specified threats and shielding must be consistent with the type, form, quantity, attractiveness level, size, configuration, portability, and credible diversion amounts of material contained within the area.

5. EMERGENCY PERSONNEL AND VEHICLES. Emergency personnel and vehicles, whether onsite or offsite responders, may be authorized for immediate entry to security areas in response to a verified emergency if:

a. The PF or other designated site personnel maintain continuous surveillance of all emergency vehicles that enter the site.

b. Arrangements are made to inspect emergency personnel and vehicles when exiting after the emergency is over or when leaving the site.

(1) If the emergency condition prevents an exit inspection before departing the site, an escort must be provided as required in site specific procedures or the approved SP.

(2) Both personnel and emergency vehicles must be inspected as soon as the emergency is over.

CHAPTER III. SECURE STORAGE

The intent of this Chapter is to establish requirements for SNM vaults.

1. GENERAL.

   a. A Special Nuclear Material (SNM) Vault must:

      (1) Be a penetration resistant enclosure that has doors, walls, floor, and roof/ceiling;

      (2) Designed and constructed to delay penetration from forced entry; and

      (3) Equipped with IDS devices on openings that may allow access.

   b. The material thickness must be determined by the requirement for forcible entry delay times for the Safeguards and Security (S&S) interests stored within but must not be less than the delay time provided by a minimum 20.32 centimeters (8 inch) thick reinforced concrete poured in place with a 28-day compressive strength of 17,237 kilopascal (2,500 pounds per square inch).

   c. Activated technologies such as active barriers or passive/active denial systems may be used when analysis indicates that longer delay times are required.

   d. The site's analysis of the protection measures in use must be documented in the SP.

   e. The vault door and frame must meet the GSA's highest level of penetration resistance. The lock on the door must be a Level I lock that meets the requirements of Attachment 2, Chapter V.

   f. Certain operational activities may dictate other storage configurations. These storage configurations must be supported by a VA and approved by the appropriate Federal risk acceptance official.

CHAPTER IV. PROTECTIVE FORCE POSTS

The intent of this Chapter is to establish requirements for PF posts used in the protection of PL-1 through PL-4 assets.

1. PERMANENT PF POSTS. Permanent PF posts providing overwatch to PA and MAA access operations at the entry control point must be constructed to meet the requirements for a hardened post as stated in a. below.

   These posts must be constructed of, or reinforced with, materials that have a bullet penetration resistance equivalent to the Level 8 high power rifle rating given in UL 752, *Standard for Bullet Resisting Equipment*.

2. TACTICAL FIGHTING POSITIONS. Interior posts intended to be used as tactical fighting positions (including exterior walls, windows, roofs, doors, and floors (if elevated)) must have, as a minimum, a bullet penetration resistance equivalent to the Level 8 high power rifle rating given in UL 752.

3. NEW CONSTRUCTION AND RENOVATION. Exterior posts intended to be used as tactical fighting positions constructed or renovated after issuance of this Order must have, as a minimum, a bullet penetration resistance equivalent to the Level 10 high power rifle rating given in UL 752.

CHAPTER V. BARRIERS

The intent of this Chapter is to establish requirements for barriers used in the protection of PL-1 through PL-4 assets.

1. GENERAL REQUIREMENTS.

   a. Barriers must be designed to channel adversaries into attrition areas to facilitate effective economical use of protective personnel while maximizing their tactical posture.

   b. Barriers must be used to direct the flow of personnel and vehicular traffic through designated entry control points to permit efficient operation of access controls and entry point inspections.

   c. Barriers must provide PFs the ability to identify and engage adversaries along all feasible pathways.

   d. Two permanent, continuous fences must identify the boundary of the PA.

   e. A clear zone must be provided along each side of security fences to facilitate intrusion detection and assessment.

   f. Objects that intruders could use to scale or bridge barriers and enter the PA must be removed or secured to prevent their unauthorized use.

   g. A clear zone of at least 6 meters (20 feet) must be provided between the inner and outer PIDAS fences to facilitate intrusion detection and assessment and be kept clear of fabricated or natural objects that would interfere with operation of detection systems or the effectiveness of the assessment.

   h. Where minimum distances cannot be provided, supplementary protective measures must be considered (i.e., greater fence height or other protective measures as required by the ODFSA) and equivalencies be requested.

   i. The PA perimeter barrier design must deter an insider from diverting S&S interests past the barrier for later retrieval.

2. SECURITY AREA BARRIERS. In addition to the requirements in Attachment 2 Chapter VI, penetration of security area barrier requirements for PAs and MAAs includes the following:

   a. Overhead utilities must not allow for access into a PA or higher security area without physical protection features to prevent or detect unauthorized access into the security area.

b. Barrier requirements:

(1) Barriers must delay or deter the unauthorized movement of SNM while allowing access by authorized personnel and material movement through entry control points and emergency evacuation as necessary.

(2) Doors at entry control points such as transfer locations must be alarmed, and the alarms must communicate with the central alarm station and secondary alarm station when an unauthorized entry/exit occurs.

(3) PF must provide a timely response to intrusion alarms.

(4) Penetrations in the floors, walls, or ceilings for piping, heating, venting, air conditioning, or other support systems must not create accessible paths that could facilitate the removal or diversion of S&S interests.

(5) Exit doors designed for emergency evacuation must be alarmed with an IDS or controlled at all times.

3. BARRIERS DELAY MECHANISMS. Mechanisms must be used to deter and delay access, removal, or unauthorized use of PL-1 through PL-4 assets.

a. Delay mechanisms may include both passive physical barriers (e.g., walls, ceilings, floors, windows, doors, or security bars) and activated barriers (e.g., sticky foam, pop up barriers, cold smoke or high intensity sound).

The appropriate delay mechanisms must be used at site specified target locations to reduce reliance on PF recapture/recovery operations.

b. Active and passive denial systems must be utilized, as appropriate, to reduce reliance on recapture operations.

4. ACTIVATED BARRIERS, DETERRENTS, AND OBSCURANTS. If used, activated barriers, deterrents, and obscurants must meet the following requirements.

a. Obscurants must consider spatial density versus time to deploy as determined by a VA.

b. Dispensable materials must be individually evaluated for effectiveness of delay.

c. Controls and dispensers must be protected from tampering and must not be collocated.

5. VEHICLE BARRIERS. Vehicle barriers must be used to deter, and where necessary, prevent penetration into security areas when such access cannot otherwise be controlled to mitigate the DBT adversary threat. These requirements must be consistent with the operation of the facility and protection goals as documented in the VA.

a. All potential vehicle approach routes to identified target areas must have barriers in place that will preclude an adversary from reaching the target.

b. If required by vehicle barrier design limits, speed reducers must be used to slow adversary vehicles to achieve site specific threat/target system response requirements.

CHAPTER VI. PROTECTION DURING TRANSPORTATION

The intent of this Chapter is to establish requirements for the transportation of PL-1 through PL-4 assets.

1. GENERAL REQUIREMENTS.

   a. The OST is responsible for the dissemination of specific internal guidance governing the protection afforded to all DOE matter entrusted to OST for transport by surface and air.

   b. Protection measures, whether onsite or by OST, must be consistent with DBT threat scenario analysis and in accordance with established standards.

   c. Packages or containers containing SNM must be sealed with tamper indicating devices.

   d. Offsite shipment of fissile nuclear materials of national security interest Category I and II quantities of SNM must be transported within the Transportation Safeguards System as addressed in DOE O 461.1, *Packaging and Transportation for Offsite Shipment of Materials of National Security Interest*, current version.

      Specific items included in this policy are nuclear explosives, nuclear explosive components, special assemblies, sub critical test devices, trainers, bulk fissile nuclear materials, and truck transported naval fuel elements.

   e. Movements of SNM between PAs at the same site or between PAs and staging areas on the same site must be escorted by armed PF officers.

   f. Nuclear explosive like assemblies, classified nuclear explosive parts, components, special assemblies, sub-critical test devices, trainers, or shapes containing no fissile nuclear material or less than Category II quantities of fissile nuclear material must be shipped consistent with both DOE policy and ODFSA approved protection requirements that have been analyzed, developed, and documented in the approved SP.

ATTACHMENT 6. PHYSICAL PROTECTION SYSTEMS

The intent of this Attachment is to provide the requirements for physical protection (PP) systems, including Physical Access Control Systems (PACS), Intrusion Detection Systems (IDS), Video Assessment and Surveillance Systems, PP Systems Testing, PP Systems Maintenance, Security Communications, Security Electrical Power and Lighting, and Security Data Transmission and Line Supervision consistent with applicable National drivers and standards.

CHAPTER I. PHYSICAL ACCESS CONTROL SYSTEMS

The intent of this Chapter is to establish requirements for DOE Physical Access Control Systems (PACS) consistent with the Design Basis Threat (DBT).

1. GENERAL REQUIREMENTS. PACS may be used in place of, or in conjunction with, protective or other authorized personnel to meet access requirements as appropriate and commensurate with prescribed Protection Levels (PLs). The minimum requirements for PACS are specified in paragraph 2 below. PL-1 – PL-6 must meet all PL-7 – PL-8 requirements in addition to those identified in the PL 1-6 paragraphs in this Chapter. The DOE security badge is the Homeland Security Presidential Directive (HSPD)-12 compliant Personal Identity Verification (PIV) credential and must be used with all PACS in use at DOE and NNSA sites. When necessary to facilitate temporary (Less than six months) access, DOE line management or Officially Designated Federal Security Authority (ODFSA) may authorize the issuance of Local Site-Specific Only (LSSO) badges for physical access as documented in the approved Security Plan (SP).

   a. PACS must be installed in accordance with manufacturer's specifications.

   b. PACS equipment (badge readers, panels etc.) must conform to NIST Special Publication 800-116, *Guidelines for the Use of PIV Credentials in Facility Access*. PACS must be capable of utilizing appropriate PIV authentication mechanisms as expressed within FIPS 201 including multi-factor authentication.

   c. As per Office of Management and Budget (OMB) policy, installed PACS readers are required to be from the approved products list of the GSA FIPS 201 Evaluation Program https://www.idmanagement.gov/approved-products-list-pacs-products/. PACS readers installed after the issuance of this order are required to be from the approved products list of the GSA FIPS 201 Evaluation Program https://www.idmanagement.gov/approved-products-list-pacs-products/

   d. Digital networks supporting PACS must be protected in accordance with NIST Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*.

   e. Lock requirements (see Attachment 2, Chapter V) apply to primary locking devices (e.g., Level I) not to key override switches which do not disable the locking device but simply override the card reader. The intent is to apply security lock requirements to the primary locking device, not to all access control devices.

2. PL-7 – PL-8. When used, PACS must meet the following requirements:

   a. When used as part of an integrated IDS boundary (e.g., a boundary protected by an IDS consisting of exterior and/or interior sensors and automated access control systems), PACS alarms (e.g., door forced open alarm, duress alarm, or tamper alarm) must be treated as an intrusion alarm and must comply with the requirements in Chapter II, for the area being protected.

(1) Supervisory alarms must be assessed by authorized personnel.

(2) Technical/maintenance support personnel must determine the cause of supervisory alarms in accordance with local procedures.

(3) When used without an integrated IDS, PACS alarms do not have to be treated as intrusion alarms and the requirements in Chapter II, do not apply.

b. To the extent practicable personnel or other protective measures are required to protect PINs, card reader access transactions, displays (e.g., badge-encoded data), and keypad devices. The process of inputting, storing, displaying, or recording verification data must ensure the data are protected in accordance with an approved SP.

c. The system must record all access attempts to include valid and invalid card reads.

The system must create a record in the log file that includes but is not limited to:

(1) Name of entrant;

(2) Event time and date;

(3) Portal identification;

(4) Credential numbers; and

(5) Type of transaction (access granted, or access denied).

d. Access authorization and personal identification or verification data between devices/equipment must be protected in accordance with an approved SP.

e. Access to limited areas must be controlled by PACS or authorized personnel.

(1) PACS must be configured for at least two factor authentication,

(2) Authorized personnel must visually authenticate the individual requiring access and verify the individual is on an approved access list and has the appropriate access authorization, or

(3) Other means documented in procedures and approved by the ODFSA that demonstrate two-factor authentication may be used.

f. PACS must be installed in vaults, and Vault-Type Rooms (VTRs) and be configured for at least two factor authentication. This requirement is for PACS installed after the date of this Order.

g. For vault and VTR doors that are not unlocked by PACS, the system must be used to record all entries and exits. This requirement is for PACS installed after the date of this Order.

h. Door locks unlocked by PACS must be configured to relock after the door has closed to mitigate the risk of unauthorized entry.

i. Doors unlocked by PACS, but not physically opened, must be configured to relock to mitigate the risk of unauthorized entry.

j. PACS door status switches must be supervised. See Chapter VIII, Data Transmission and Line Supervision of this Attachment.

3. PL-5 – PL-6. PACS for PL-5 – PL-6 assets must meet all PL-7 – PL-8 requirements in addition to the following requirements.

a. Field processors, reader housing, and junction boxes must be tamper alarmed and be monitored by authorized personnel. Tamper indicating devices may be used if checked at a periodicity documented in the approved SP.

b. Uninterruptable power supply or compensatory measures must be provided at portals where continuous operation is required.

4. PL-1 – PL-4. PACS must be used for access to PAs, Material Access Areas (MAAs), vaults containing PL-1 – PL-3 assets and VTRs containing PL-4 assets must meet all PL-5 – PL-8 requirements in addition to the following requirements.

a. Both the Central Alarm Station (CAS) and Secondary Alarm Station (SAS) must monitor PACS alarms unless monitored by a Protective Force (PF) post (e.g., door forced open alarm, duress alarm, or tamper alarms and be treated as intrusion alarms).

b. PACS for access to PAs must employ a minimum of two factor authentication.

c. PACS for access to MAAs must employ three factor authentication even if three factor is employed for PA access.

d. PACS field processors and junction boxes must be:

(1) Located within an area where they can be protected.

(2) Housed in locked and tamper-alarmed enclosures. (Level I lock not required.)

(3) Physical access to PACS components must be under two-person rule (PF escort could meet the requirement for a second person) with at least one person trained on the equipment, possessing an access authorization commensurate with the assets being protected or;

(4) If a trained and qualified technician without the appropriate clearance is used, an appropriately cleared individual who has knowledge of the activity being performed to the level necessary to detect malicious tampering must escort them with over-watch provided by PF personnel.

e. PACS must:

(1) Provide positive feedback to the user in the form of a light, an audible tone, or alphanumeric message at the portal to indicate that passage is granted or denied.

(a) Verbal or visual prompts may be used to instruct/interact with personnel on portal usage during emergency response actions.

(b) If multiple actions are required for passage, PACS equipment must provide instructions or positive feedback at the end of each action.

(2) Be capable of generating a notification when a site-specified number of consecutive invalid passage attempts with a particular badge have been exceeded at a single portal.

(3) Be configured to shunt door forced open alarms for a maximum of 45 seconds upon valid authorized entry through a control portal.

(4) Provide the capability to generate a muster report.

(5) Accommodate a multi-person rule in which two or more authorized users must successfully complete the required automated access procedures (such as badge read, PIN entry, and/or biometric verification) at the portal within a site-specified time-out period before allowing the persons to enter or exit a security area.

(6) Provide anti-passback capability.

(7) Provide anti-tailgating capability, which precludes the passage of more than one person upon a single authorized access attempt.

(8) Allow passage of properly escorted visitors.

(9) Permit the passage of one or more escorts and visitors who are authorized passage as escortees. Visitors must interface with the portal user entry device (badge and/or PIN and/or biometric) as required for the security area.

(10) Automatically update field processor local databases with portal access list data from the host database when data is added or deleted or modified.

(11) Update within 15 minutes all field processor databases when an individual's privileges are modified or suspended.

(12) Be capable of denying access to the PA if the badge has not been processed and accepted at a lower security area.

(13) Deny access to an MAA if the badge has not been processed and accepted at the PA boundary.

(14) Provide the capability to synchronize system clocks to ensure PACS, intrusion detection, and video assessment and surveillance systems all have the same time.

f. Field processors must maintain local access lists of authorized users and the following requirements apply:

(1) If the user requesting passage is not found in the local database, the system must automatically search the host computer database.

(2) When communications are lost between the field processor and the host, the field processor must continue to operate the portal with its local database. The duration of communications loss must be recorded.

(3) When communications are reestablished between the field processor and the host system, the field processor must provide an upload to the host of all logged transactions that occurred while communications were lost.

(4) If the number of transactions exceeds local memory size in the field processor during the loss of communications, the system must provide the capability to disable the portal so that no passage is allowed until communications are restored. Compensatory measures must be implemented until communications are restored.

CHAPTER II. INTRUSION DETECTION SYSTEMS

The intent of this Chapter is to establish requirements for DOE Intrusion Detection Systems (IDS) consistent with the DBT.

1. GENERAL REQUIREMENTS. IDS are required to protect certain DOE assets commensurate with prescribed DBT PLs.

   Digital networks supporting IDS must be compliant with NIST SP 800-53.

2. PL-7 AND PL-8 IDS. IDS used for PL-7 and PL-8 assets must meet the following requirements:

   a. IDS must be continuously monitored at an alarm monitoring station using:

      (1) On-site alarm stations with access control to the station in accordance with local procedures as documented in an approved SP, or

      (2) Off-site commercial monitoring stations that meet Underwriters Laboratory (UL) 827, *Standard for Central Station Alarm Services*.

   b. Alarms must annunciate both audibly and visibly to an alarm station.

   c. Alarm stations must provide a capability for initiating responses to Safeguards and Security (S&S) events.

   d. Alarm station personnel must be knowledgeable of the area being protected and the emergency notification procedures.

   e. Tamper and supervisory alarms must be assessed by authorized personnel and technical/maintenance support personnel in accordance with local procedures.

   f. Records must be kept of each alarm received in the alarm station and of any maintenance activities conducted on the alarm system or any of the related components.

   g. Personnel staffing the alarm station must possess an appropriate access authorization commensurate with the most sensitive interest under the protection of the alarm station. If alarm station operators do not have the ability to make programming or alarm status changes in the system and can only monitor and acknowledge alarms commensurate access authorization is not required.

   h. The system must be capable of prioritizing alarm conditions. Prioritization must be based on the importance of the S&S interests.

   i. IDS alarms must be assessed to facilitate a timely response to determine the cause via Video Assessment and Surveillance Systems (VASS) or by other authorized personnel as identified in an approved SP.

j. The Officially Designated Security Authority (ODSA) must:

(1) Establish False Alarm Rates (FAR)/Nuisance Alarm Rates (NAR) standards based on site specific systems,

(2) Develop a program to analyze FAR/NAR data ensuring acceptable system effectiveness and,

(3) Document the FAR/NAR standard and analysis program in an approved SP.

k. IDS must be maintained in accordance with Chapter V of this Attachment.

l. IDS must be designed to:

(1) Utilize appropriate sensor technology to address applicable environmental conditions.

(2) Ensure that annunciation of an alarm indicates the type and location of the alarm.

(3) Ensure that only authorized personnel can make changes to the system configuration and functionality.

(4) Generate a log of system configuration changes including:

(a) What changed

(b) The time and date the change was made

(c) Who made the change

(5) Provide an indication upon failure of any critical component that the alarm system requires to perform its intended function.

(6) Provide an indication upon loss of primary power.

(7) Automatically switch to back up power.

(8) Provide an indication upon loss of communications.

(9) Support the initiation of a timely response.

m. IDS must be installed in accordance with manufacturer's specifications.

n. IDS equipment e.g., terminations, field processors, must be housed in a locked enclosure in accordance with local procedures.

o. IDS equipment must only be serviced by trained and authorized personnel.

p. IDS installed at Sensitive Compartmented Information Facilities (SCIFs) must comply with Intelligence Community Directive (ICD) 705 and UL 2050. As specified by ICD 705 Technical Specifications, Chapter 7.A.2.c. "*Systems developed and used exclusively by the U.S. government do not require UL certification, but must comply with an Extent 3 installation as referenced in UL 2050*".

q. IDS alarm zones must be supervised. See Chapter VIII of this Attachment.

r. At a minimum Limited Areas (LAs) must have detection capability such as IDS or equivalent as documented in the approved SP.

At a minimum, LAs must be provided detection at all entry and exit points.

s. Vaults and VTRs utilizing IDS must meet the following requirements:

(1) IDS field processors and termination boxes, must be:

(a) Located within the area being protected or within an associated LA for Vaults and VTRs storing classified.

(b) Wired using armored cable, electric metallic tubing or threaded conduit if not located within the area being protected.

(c) Housed in tamper-alarmed enclosures in accordance with local procedures as documented in the approved SP.

(d) Be provided an uninterruptable power supply that:

1 Ensures a smooth transition to a back-up source such as a generator or

2 Ensures power remains available for a minimum of four hours.

(e) Serviced only by trained personnel possessing an access authorization commensurate with the assets being protected or;

(a) If a trained and qualified technician without the appropriate clearance is used an appropriately cleared individual who has knowledge of the activity being performed to the level necessary to detect malicious tampering must escort them.

(2) A balanced magnetic switch (BMS) must be used on each door or movable barrier to allow detection of attempted or actual unauthorized access. BMSs must:

(a) Meet UL 634 requirements for a level 2 high security switch (BMS).

(b) Initiate an alarm upon attempted substitution of an external magnetic field when the switch is in the normal secured position.

(c) Initiate an alarm when the door moves more than 2.5 centimeters (1 inch) from the fully closed position.

(3) IDS sensors must detect movement along accessible paths within the vault/VTR or surround the security interest being protected.

(4) The IDS must be placed in secure mode when the vault or VTR is unoccupied.

(5) Where visual access to classified information is a concern, detection must occur prior to the point where visual access becomes possible.

3. PL-5 AND PL-6 IDS. IDS for PL-5 and PL-6 assets must meet all PL-7 and PL- 8 requirements in addition to the following requirements.

a. IDS must be continuously monitored at an alarm monitoring station on-site or utilize an off-site commercial monitoring station that is UL 827, *Standard for Central Station Alarm Services* compliant.

b. Field processors and junction boxes must be tamper alarmed.

c. IDS transmission lines must be supervised or encrypted (see Chapter VIII, Data Transmission and Line Supervision of this Attachment).

d. IDS sensors providing detection for PL-5 – PL-6 assets must be provided with compensatory measures when the system is not functioning.

e. IDS must support the initiation of a timely response.

4. PL-1 THROUGH PL-4 IDS. IDS must be implemented for the protection of PL-1 through PL-4 assets and must meet all PL-5 through PL-8 requirements in addition to the requirements in this section. FAR/NAR requirement from above does not apply to PL-1 through PL-4 protection. The requirements for FAR/NAR are below in f (1).

a. Field processors for sensors and devices must be:

(1) Located within a PA or MAA.

(2) Housed in locked and tamper-alarmed enclosures (Level I lock not required).

(3) Physical access to IDS components must be under two-person rule (PF escort could meet the requirement for a second person) with at least one

person trained on the equipment, possessing an access authorization commensurate with the assets being protected, or;

(4) If a trained and qualified technician without the appropriate clearance is used an appropriately cleared individual who has knowledge of the activity being performed to the level necessary to detect malicious tampering must escort them with over-watch provided by PF personnel.

b. IDSs must be designed with independent communication paths to the CAS and SAS after the issuance of this Order, for new installations or system upgrades.

c. All signal lines must be supervised or encrypted to detect tampering in accordance with Chapter VIII of this Attachment.

d. The system must:

(1) Be provided a stand-alone network for communications between system components that operates independently of, and separate from, the site's IT/ business LAN or

(2) Be provided a network that allows secure and private data transfers such as a segregated VLAN (Virtual LAN) with a dedicated network switch or other similar logical isolation technology.

e. At a minimum, IDS must be performance tested at a documented frequency and in accordance with Chapter IV of this Attachment.

f. The IDS must be designed, installed, operated, and maintained to ensure that FAR/NAR do not reduce system effectiveness.

(1) At a minimum:

(a) Each interior intrusion detection sensor must not have a FAR of more than one alarm per 2400 hours of operation while maintaining proper detection sensitivity.

(b) Each exterior intrusion detection sensor must not have a FAR of more than one alarm per 24 hours of operation while maintaining proper detection sensitivity.

(c) NAR must not reduce overall system effectiveness which negatively impacts the ability of CAS/SAS operators to initiate a response, and must be analyzed in accordance with the approved SP.

(d) Alarm occurrences must be categorized as intrusion, false, nuisance, authorized, or maintenance and documented for analysis and trending purposes.

(2) Sites may use early warning intrusion detection to supplement their Perimeter Intrusion Detection and Assessment System (PIDAS) as a means of achieving increased adversary detection and improved overall system performance. The FAR/NAR, degradation, and detection area maintenance requirements of a PIDAS do not apply to early warning systems. Each individual early warning or extended range exterior intrusion detection sensor must have FAR/NARs that do not degrade the overall effectiveness of the system, including monitoring personnel's ability to assess and manage alarms, and be documented in the SP. A vulnerability analysis process will determine the effectiveness of these systems and performance testing requirements.

g. The security system must be capable of being expanded to at least an additional 50 percent capacity of inputs and outputs, at the time of installation.

h. PA IDS equipment utilized with the PIDAS must:

(1) Cover the entire perimeter without a gap in detection, including exterior walls and roofs of any structure that is part of the PA boundary and must use complementary intrusion detection sensors across the same zone (see Attachment 7 – Definitions).

(2) Be assessed in a timely manner to facilitate the required response to the DBT adversary.

(3) Be continuously monitored at the CAS and SAS.

(a) CASs constructed after publication of this Order must be located within a PA. CASs may be responsible for more than one PA.

(b) The CAS and SAS must monitor all alarms to support initiation of a timely response. The SAS does not have to be capable of performing all functions of the CAS but must be capable of providing full command and control in support of response functions.

(c) Both alarm stations must be continuously staffed with at least one trained and qualified alarm station operator and;

Ensure that an alarm station operator cannot change the status of a detection point or deactivate a locking or access control device at a PA portal without authorization and notification to the other alarm station operator.

(d) Both alarm stations must be designed and equipped to ensure that a single event cannot disable both alarm stations and ensure the survivability of at least one alarm station to perform the following functions:

1 Detect and assess alarms;

2 Initiate and coordinate a timely response to an alarm;

3 Summon offsite assistance; and

4 Provide command and control.

(4) Be capable of detecting an individual crossing the detection zone by any of the applicable following activities—walking, crawling, jumping, running, rolling, or climbing the fence at any point in the detection zone—with a detection probability of 90 percent and confidence level of 95 percent.

Note: if no fence sensor is present, then fence climbing is not an applicable activity.

The detection probability and confidence level must be validated annually in accordance with the performance testing requirements in Chapter IV of this Attachment.

(5) Be designed, installed, and maintained to deter adversaries from circumventing the detection system.

(6) Have compensatory measures, based on analysis, identified that ensure the effectiveness of detection when there is a failure or degradation of the IDS.

Compensatory measures must be documented in an approved SP and:

(a) Be implemented upon discovery of the degraded or inoperable equipment to facilitate the required response to the DBT adversary.

(b) Provide a level of protection to compensate for the degraded or inoperable equipment, system, or components until fully functional.

(c) Facilitate the same response as the failed IDS component when functioning properly.

(7) For IDS equipment at a MAA perimeter: A BMS must be used on each door or movable barrier to allow detection of attempted or actual unauthorized access. BMSs must:

(a) Meet UL 634 requirements for a level 2 high security switch (BMS).

(b) Initiate an alarm upon attempted substitution of an external magnetic field when the switch is in the normal secured position.

(c) Initiate an alarm when the door moves more than 2.5 centimeters (1 inch) from the fully closed position.

CHAPTER III. VIDEO ASSESSMENT AND SURVEILLANCE SYSTEMS (VASS)

The intent of this Chapter is to establish requirements for DOE VASS consistent with the DBT.

1. GENERAL REQUIREMENTS. VASS may be used to meet assessment requirements as appropriate and commensurate with prescribed DBT PLs. Visual observations by protective personnel may be used in place of or to complement VASS depending on the requirements for the area being protected.

   VASS may not be used in areas where visual access to classified information is a concern. Classified VASS used in areas where access to classified information is a concern may only be used to view classified information when approved for that purpose.

2. PL-7 THROUGH PL-8 VASS. When used VASS must meet the following requirements.

   a. VASS must be maintained in accordance with Chapter V of this Attachment.

   b. VASS must be designed to:

      (1) Function effectively in all environmental conditions and under all types of lighting conditions applicable to the asset being protected.

      (2) Provide visual display capabilities.

      (3) Ensure that only authorized personnel can make changes to the system programming, configuration and functionality.

      (4) Provide an indication upon loss of primary power.

      (5) Provide an indication when the video signal from the camera is disrupted or lost.

   c. VASS must be installed in accordance with manufacturer's specifications.

   d. VASS equipment must only be serviced by trained personnel.

3. PL-5 THROUGH PL-6 VASS. When used, VASS for PL-5 through PL-6 assets must meet all PL-7 through PL-8 requirements in addition to the following requirements;

   a. The system must provide pre-alarm and post alarm video.

   b. When VASS is used as the primary means of assessment, video field junction boxes must be tampered alarmed.

   c. When VASS is used as the primary means of assessment, an uninterruptable power supply must be provided that:

      (1) Ensures a smooth transition to a back-up source such as a generator or;

(2) Ensures power remains available for a minimum of 4 hours.

d. When VASS is used as the primary means of assessment, be provided with compensatory measures when the system is not functioning.

4. PL-1 THROUGH PL-4 VASS. VASS must be installed/implemented as the primary means of assessment for the PIDAS and must meet all PL-5 through PL-8 requirements in addition to the requirements in this Section.

a. VASS must support the initiation of a timely response.

b. Physical access to VASS components must be under two-person rule (PF escort could meet the requirement for a second person) with at least one person trained on the equipment, possessing an access authorization commensurate with the assets being protected or;

(1) If a trained and qualified technician without the appropriate clearance is used an appropriately cleared individual who has knowledge of the activity being performed to the level necessary to detect malicious tampering must escort them with over-watch provided by PF personnel.

c. VASS junction boxes must be:

(1) Located within an area where they can be protected.

(2) Housed in locked and tamper-alarmed enclosures. (Level I lock not required.)

d. Digital networks supporting VASS must be compliant with NIST SP 800-53.

e. VASS signal lines must be supervised or encrypted to detect tampering in accordance with Chapter VIII of this Attachment. The system must:

(1) Be provided a stand-alone network for communications between system components that operates independently of, and separate from, the site's IT/ business LAN or;

(2) Be provided a segregated VLAN (Virtual LAN) with a dedicated network switch.

f. VASS must be performance tested with the IDS at a documented frequency in accordance with Chapter IV of this Attachment.

g. The VASS must be maintained to ensure system effectiveness is not reduced.

h. The system must be capable of being expanded to at least an additional 50 percent capacity, at the time of installation.

i. Video recorders must be actuated by the intrusion alarm and record automatically.

j. Video recorders must have capacity to store at least 30 days of video/event logs.

k. PA VASS equipment utilized with the PIDAS must:

(1) Be utilized for assessment of IDS alarms.

(2) Be designed with independent redundant signal paths to CAS and SAS respectively from the PIDAS for video transmission, after the issuance of this order, for new installations or system upgrades.

(3) Be monitored at the CAS and SAS.

(4) Be designed with video call up for each detection zone using fixed cameras, with fixed focal lengths.

(5) Be capable of assessing an individual crossing the detection zone by walking, crawling, jumping, running, rolling, and climbing, at any point in the detection zone.

(6) Be designed, installed, and maintained to deter adversaries from circumventing the system.

(7) Have compensatory measures, based on analysis, identified that ensure the effectiveness of assessment when there is a failure or degradation of the IDS.

Compensatory measures must be documented in an approved SP and:

(a) Be implemented upon discovery of the degraded or inoperable equipment to facilitate response timelines based on adversary task times.

(b) Provide a level of protection to compensate for the degraded or inoperable equipment, system, or components until fully functional.

(c) Facilitate the same response as the failed VASS component when functioning properly.

CHAPTER IV. IDS AND SCREENING EQUIPMENT TESTING

The intent of this Chapter is to establish requirements for Department of Energy (DOE) physical protection systems testing.

1. GENERAL REQUIREMENTS.

   a. Acceptance Testing. Acceptance testing for all physical protection systems, in conformance with the manufacturer's specification, must be performed prior to acceptance of the installed system and include the following:

      (1) Acceptance testing for a new system must include all sensors, equipment, and devices.

      (2) Verify the system was installed as designed.

      (3) Verify the alarm station(s) or CAS/SAS receive alarms as designed.

      (4) Verify assessment is accomplished as designed.

      (5) Verify response is initiated as designed.

   b. Operability Testing. Operability testing indicates a piece of equipment is powered on and functioning without any indication of effectiveness. Procedures must be developed and implemented as documented in the approved SP.

   c. Performance Testing. Performance tests are tests that ensure a system or component is performing as intended and is effective. These testing methods are used in a combination to analyze system effectiveness. Systems, system components, and essential elements must be performance tested at a frequency documented in the Performance Assurance Plan, and, at a minimum annually.

      (1) The testing program for systems and system components must be developed and implemented in local procedures and documented in the approved SP.

      (2) The testing program must address the capabilities of sensors detailed in the manufacturer's specifications and include the testing methods recommended in the manufacturer's specifications.

      (3) Additionally, the testing program must include the testing methods in this Chapter as specified for certain equipment.

   d. System Effectiveness Testing. System effectiveness of physical protection systems must be determined by performance testing of detection, assessment, delay and response capabilities in concert. System effectiveness does not apply to any individual detection sensor but to all parts of the protection systems that work together in facilitating a response that mitigates the DBT adversary threat. System

effectiveness is determined through performance testing, and analyzing the results, at a frequency as documented in the Performance Assurance Plan.

e. Testing Personnel Access Authorizations. See Chapter V, paragraph 4 of this Attachment for access authorization requirements.

f. Zone supervision alarms (see Chapter VIII) must be tested to verify effectiveness at least annually.

2. IDS SENSOR PERFORMANCE TESTING PROCEDURES. For PL-5 through PL-8 the following procedures must be followed when performance testing the specified devices.

a. Performance testing must be conducted to determine the proper settings for high detection rates with the lowest possible nuisance or false alarm rates.

b. Tests must be performed along credible pathways with a low-profile target (crawling) and a higher velocity and profile targets (walking, running, fast crawl, rolling) or as appropriate given space considerations for interior applications as documented in the SP.

c. If assessment is by fixed camera, the tests must be conducted under the lowest lighting conditions that are routinely available.

d. The testing must be conducted against the worst case "light to dark ratio" to determine if shadows or dark spots in the field of view degrade assessment viability.

e. Testing must ensure that the alarm communication line or data link is capable of transmitting an alarm signal and that it has not been compromised.

f. Testing must confirm the equipment performs its intended function.

g. If testing indicates degradation of the IDS, it must be repaired and retested.

h. All tamper alarms must be tested annually at a minimum.

i. Loss of communications and loss of power supervisory alarms must be tested annually at a minimum.

j. Balanced Magnetic Switches must be tested by:

(1) Attempted substitution of an external magnetic field when the switch is in the normal secured position

(2) Initiating an alarm when attempting to move the door more than 2.5 centimeters (1 inch) from the fully closed position or alternative methods approved by the manufacturer.

(3) BMS tamper alarms must be tested in accordance with UL 634 sections 58, 60, 61, 62, 63 which describes tamper testing based on device type.

k. Volumetric sensor tests must employ a range of walk tests to verify the detection pattern is effective as designed.

3. TESTING OF SCREENING EQUIPMENT. Screening equipment for PL-5 through PL-8 can include explosive detectors, metal detectors, and x-ray systems and must be capable of detecting prohibited and controlled articles before being permitted into DOE facilities.

a. All screening equipment must be tested for operability daily at a minimum as documented in local procedures.

b. When used, explosive detectors must be performance tested in accordance with manufacturer's specifications and local procedures as documented in the approved SP.

c. At a minimum, the following for performance testing of metal detectors are required as appropriate depending on the specific equipment used:

Standard test objects:

(1) Steel and aluminum alloy .25 caliber automatic pistol manufactured in Italy by Armi Tanfoglio Giuseppe, sold in the United States by Excam as Model GR 27B and by F.I.E. as the Titan (weight about 343 grams); or

(2) Aluminum, model 7, .380 caliber Derringer manufactured by American Derringer Corporation (weight about 200 grams); or

(3) Stainless steel .22 caliber long rifle mini revolver, manufactured by North American Arms (weight about 129 grams); or

(4) NIJ Standard 0601.02 Law Enforcement and Corrections Standards and Testing Program, Section 5.1/5.2, and 5.3.2.

d. When used, X-ray machines must be performance tested to ensure the equipment is performing its intended function in accordance with the following requirements:

(1) Provide a discernible image of prohibited and controlled articles.

(2) Comply with the practices described in ASTM standard for test objects (see ASTM Standard F792-17, *Standard Practice for Evaluating the Imaging Performance of Security X-ray Systems*).

e. Screening equipment that has been powered off must be performance tested to ensure capability of detecting prohibited and controlled articles before being placed back into service.

4. PL-1 THROUGH PL-4 ADDITIONAL REQUIREMENTS. For sites protecting PL-1 through PL-4 assets security equipment testing must meet the above requirements as well as the requirements of this section.

a. IDS Testing Definitions. The following definitions apply to sensor performance testing procedures required below.

(1) The definition of crawling is crossing the detection zone lying prone on the ground with a low profile at an approximate velocity of .15 meters (one foot) per second.

Sites may use an aluminum sphere that is 30 centimeters (approximately 11.8 inches) in diameter to simulate crawl tests.

(2) The definition of walking is entering and leaving the zone of detection with a normal stride 2 76.2 centimeters (2 30-inch) steps per second.

(3) The definition of running is entering and leaving the zone of detection at an approximate velocity of 5 meters (16 feet) per second.

(4) The definition of jumping is leaping over the zone of detection, including standing on a fence and attempting to leap across the zone of detection.

(a) An aluminum sphere with a 30 centimeter (approximately 11.8-inch) diameter, or one that meets manufacturer's specifications, can be used to simulate jump tests.

(b) Although an aluminum sphere tests the microwave sensors from the ground level during crawl tests, using the same sphere for jump tests would test the microwave sensors from a third dimension as it is dropped down vertically.

(5) The definition of rolling is crossing the detection zone on the ground with a low profile, body parallel to the zone of detection, and moving at an approximate velocity of .15 meters (one foot) per second.

b. PIDAS Detection Capability. A PIDAS must be capable of detecting an individual crossing the detection zone by walking, crawling, jumping, running, rolling, and/or climbing the fence at any point in the detection zone, with a detection probability of 90 percent and confidence level of 95 percent.

(1) The IDS must be performance tested when installed and annually (at least every 12 months) thereafter to validate that it meets detection probability and confidence level requirements.

(2) Any time the IDS falls below the required probability of detection, the IDS must be repaired and retested.

(3) When calculating detection probability for multiple sensor systems, detection is assumed if any of the sensors report an intrusion.

(4) Performance testing must be conducted to determine the proper settings for high detection rates with the lowest possible NARs.

(5) Tests must be performed with a low-profile target (crawling) and a higher velocity and profile targets (walking, running, fast crawl, rolling).

(6) The tests must be conducted under the sort of weather and lighting conditions that are common to the local environment.

c. IDS Sensor Performance Testing Procedures. The following procedures must be followed when performance testing the specified devices.

(1) Interior Volumetric Sensor. Interior volumetric sensor tests must employ a range of crawl, walk, and run tests to verify the detection pattern is effective as designed.

(2) Microwave Systems. A microwave perimeter detection system should be capable of detecting an individual passing through the zone of detection between the transmitter and receiver, including the area in front of both the transmitter and receiver, whether the individual is walking, running, jumping, crawling, or rolling.

The receiver must be limited to respond to selected frequencies to decrease susceptibility to bypass.

(3) Electric Field Systems. An electric field perimeter detection system should be able to detect an individual whether the individual is crawling or rolling under the lowest wire or stepping between the wires.

(4) Ported Coaxial Cable Systems. A ported coaxial cable perimeter detection system should be capable of detecting an individual passing over the transmitter and receiver wires, whether the individual is walking, running, jumping, crawling, or rolling.

The electromagnetic field must be modulated, and the receiver must be frequency selective to decrease susceptibility to "receiver capture."

(5) Active Infrared Multi-Beam System. The system must be capable of detecting an individual passing between the transmitters and receivers whether the individual is walking, running, jumping, crawling, or rolling.

(6) Taut Wire Systems. The system must be installed so that an alarm is received when the wire is deflected 15.24 centimeters (6 inches).

(7) Fiber Optic Systems. A fiber optic detection system must be capable of detecting an individual passing over the cable, whether the individual is walking, running, jumping, crawling or rolling.

(8) Vibration or Strain-Detection Systems. Vibration or strain-detection systems used for fence protection must detect an individual attempting to climb the fence.

(a) The system should also detect any attempt to cut the fence or lift the fence fabric 15.24 centimeters (6 inches) or more above grade. The system must not generate excessive nuisance alarms.

(b) In addition, the vibration or strain detection systems must be tested for their ability to detect fence cutting attacks or other means of defeating detection unique to these systems.

d. Testing of Screening Equipment. Explosive detectors, metal detectors, x-ray systems, and SNM detectors must be tested to ensure that prohibited and controlled articles are detected before being permitted into DOE facilities as described above.

(1) Explosive Detectors. Explosive detectors used in the entry inspection process must be tested in accordance with manufacturer's specifications.

(2) SNM Detectors. For areas containing PL-1 through PL-4 assets in order to meet the requirements of DOE 474.2 SNM detectors must be used in the exit inspection process, and must be tested in accordance with manufacturer's specifications and using materials with radioactive signatures and strengths consistent with required detection thresholds that depict the type of SNM located within the security area.

(a) The testing procedure must provide the detection thresholds.

(b) The thresholds must be consistent with the SNM type, form, quantity, attractiveness level, configuration, portability, and credible diversion amounts contained within the area.

(c) Detection thresholds must meet detection requirements as defined by the MC&A plan (see DOE O 474.2, current version).

5. RECORD KEEPING.

a. Record of the failure and repair of all equipment must be maintained so that type of failure, unit serial number or other identifier, and equipment type can be compiled.

b. Testing and maintenance records must be retained in accordance with the requirements of approved records management procedures.

CHAPTER V. PHYSICAL SECURITY SYSTEMS MAINTENANCE

The intent of this chapter is to establish requirements for physical security systems maintenance.

1. GENERAL REQUIREMENTS.

   a. Security related systems and components must be maintained in operable condition.

   b. A corrective maintenance program must be established by the ODSA and documented in the approved SP.

   c. A regularly scheduled preventive maintenance program must be established by the ODSA and documented in the approved SP.

2. CORRECTIVE MAINTENANCE.

   a. Corrective Maintenance within 24 Hours. Corrective maintenance must be initiated within 24 hours of receiving a report that there has been a malfunction of equipment protecting PL-1 through PL-4 assets, classified matter, and SCI or SAP interests, or have compensatory measures in place until the system is restored to functionality.

   b. Corrective Maintenance within 72 Hours. Corrective maintenance must be initiated within 72 hours of receiving a report that there has been a malfunction for all other equipment protecting PL-5 through PL-8 non classified assets.

   c. Return to Service Testing. Physical protection system equipment must be performance tested after corrective maintenance and prior to being put back into service in accordance with locally developed procedures and documented in the approved SP.

3. PREVENTIVE MAINTENANCE. Preventive maintenance must be performed on S&S related subsystems and components in accordance with manufacturers' specifications as documented in local procedures.

4. MAINTENANCE PERSONNEL ACCESS AUTHORIZATIONS. Personnel who test, maintain, or service physical protection system equipment must have access authorizations consistent with the S&S interest being protected unless an un-cleared qualified technician is escorted by an appropriately cleared individual possessing knowledge about the work being performed sufficient to detect malicious tampering. When an un-cleared qualified technician is escorted as described and performs maintenance, performance testing must be conducted immediately upon return to service.

   a. Maintenance must not be performed by personnel remotely (accessed remotely via secure connections over the internet, telephone connection, or other data communication medium), who do not possess appropriate access authorization

commensurate with the asset being protected, on systems protecting classified matter, SNM, and PL-1 through PL-4 assets.

b. Access authorizations are not required when testing and maintenance are performed as bench services away from the security area.

c. Systems or essential elements bench tested or maintained away from the security area by personnel without the appropriate access authorizations must be inspected and performance tested by qualified and cleared personnel before being returned to service.

5. COMPENSATORY MEASURES. Compensatory measures approved by the ODFSA must be implemented immediately when any part of an essential element protecting, classified matter, SNM, SCI or Special Access Program (SAP) interests is out of service.

a. Compensatory measures must be continued until maintenance is complete and the system is back in service.

b. Compensatory measures must provide a level of protection to compensate for the degraded or inoperable equipment, system, or components until fully functional and not introduce any additional risk as documented in the approved SP.

c. For non-essential elements, the ODFSA must approve compensatory measure implementation procedures.

CHAPTER VI. SECURITY COMMUNICATIONS

The intent of this Chapter is to establish requirements for security communications equipment.

1. GENERAL REQUIREMENTS.

   a. For protection of PL-5 through PL-8 assets IDS may use radio frequency communications to transmit alarm and other data for alarms, video, early warning devices, and other data utilized by the IDS provided:

      (1) The data being transmitted are not classified.

      (2) The data being transmitted are protected consistent with the Departmental Element Cybersecurity Program Plan (DE-CSPP). DOE O 205.1, *Department of Energy Cybersecurity Program*, current version, states Heads of Departmental Elements have overall responsibility for the DE-CSPP.

      (3) Self-checking alarm communication paths that annunciate system failure in the alarm stations exist.

      (4) Unique status change messages for alarm, tamper, and power conditions exist.

      (5) Tamper resistant or tamper switch alarm transmitters exist.

      (6) The system has auxiliary power for critical components until power can be restored or compensatory measures can be implemented.

      (7) The system does not produce spurious signals that interfere with other security system components.

      (8) The system has a unique electronic address code for each transmitter/receiver pair.

      (9) The system has a means of interfacing with the alarm annunciation system (e.g., the alarm station or central alarm station).

      (10) Reliable communications in all weather conditions exist.

      (11) System integrity is maintained (i.e., not diminished) during multiple alarms.

      (12) The system operates on authorized frequency bands.

      (13) Notification is made to the alarm station operator if a network failure is detected.

(14) Performance testing is conducted in accordance with established performance assurance procedures at a documented frequency.

(15) A risk assessment is conducted and documented identifying that no risk exists or that the risk is acceptable.

b. Protective personnel communications include the procedures and hardware that enable officers to communicate with each other. Communications equipment must be provided to support reliable information exchanges between protective personnel.

(1) Communications equipment must remain operable during the loss and recovery of primary electrical power.

(2) Voice communications systems used for security purposes must provide intelligible voice communications in all security areas for all modes of operation and operating conditions.

(3) All protective personnel fixed posts must have duress devices. The duress alarms built into mobile radios meet this requirement.

(4) Tests of communications systems must be conducted daily.

c. Protection system communications must support alarm communication/display.

(1) Communications equipment must remain operable during the loss and recovery of primary electrical power.

(2) Duress systems, fixed post and portable, must be tested weekly.

2. RECORDS. Records of the failure and repair of all protective personnel radio communications equipment must be maintained so that type of failure, unit serial number, and equipment type can be compiled.

3. RECORDING OF COMMUNICATION. A continuous electronic recording system must be provided for all security radio traffic and hardwired telecommunications that provide support to the protective personnel in accordance with local procedures documented in the approved SP.

a. The recordings must be stored for a period of time in accordance with locally developed procedures.

b. The recorder must be equipped with a time/date stamp and must cover all security channels.

c. Sites must ensure that systems comply with all local and national level requirements for consensual listening. The heads of Departmental Elements or their Federal designees, in consultation with Counsel, may determine whether

consensual listening-in and recording is appropriate for certain security operations if it is found to be necessary, must approve local procedures for such activities.

d. Approved procedures must be in accordance with all applicable Federal, state, and local statutes and must contain carefully articulated procedures, including periodic review, meeting Federal statutory guidance [e.g., U.S.C., Title 18, Part I, Chapter 119, section 2511(2)(d)], applicable State and local laws, and current DOE directives.

4. PL-1 THROUGH PL-4 COMMUNICATIONS EQUIPMENT. Communications equipment used in the protection of PL-1 through PL-4 assets must meet the following requirements:

a. Redundant Voice Communications. Facilities must have a minimum of two different voice communications technologies to link the CAS/SAS to each fixed post and PF duty location in accordance with local procedures documented in the approved SP.

Alternative communications capabilities must be available immediately if the primary communications system fails.

b. Communication Systems. Protection system communications must support two essential functions: alarm communication/display and PF communications. PF communications include the procedures and hardware that enable officers to communicate with each other.

c. Design Considerations. The design of a PF communication system must address resistance to eavesdropping, vulnerability to transmission of deceptive messages, and susceptibility to jamming.

d. Alternative Means of Communication. Alternative means of communication must be in place such as telephones, intercoms, public address systems, hand signals, sirens, lights, pagers, couriers, computer terminals, flares, duress alarms, smoke, or whistles.

e. Local Law Enforcement Agency (LLEA) Communication. When LLEA support is used a method must be established to ensure communication with LLEAs.

(1) An alternative communications capability from a SAS must be provided if the primary station is compromised.

(2) All response vehicles designated for fresh pursuit/response/recovery must be capable of communicating with supporting LLEAs. This capability must be performance tested at least annually.

f. Duress Systems. Facilities with PAs and MAAs must have duress notification capabilities for mobile and fixed posts and for the CAS/SAS.

The duress system must meet the following requirements:

(1) Activation of the duress alarm must be as unobtrusive as practicable. The duress alarm must annunciate at the CAS and SAS but not at the initiating PF post.

(2) The duress alarm for a CAS must annunciate at the SAS while the duress alarm for the SAS must annunciate at the CAS.

(3) Mobile duress alarms must annunciate at the CAS, SAS, or another fixed post.

Where the duress annunciates at another fixed post, the post must be staffed 24/7 and initiate a response in accordance with documented local procedures.

g. PF Radio System Requirements. Fixed post radios, mobile radios, and portable radios must be provided to support operational security requirements and meet the following:

(1) The application of digital encryption must be implemented.

(2) Radio system components must be protected against destruction and unauthorized access.

(3) Radio programming consoles must be protected from unauthorized programming changes.

(4) Portable radios must be capable of two- way communication from within buildings and structures.

(a) An alternative means of communications must be provided if transmission is prohibited or not possible within a building or structure.

(b) Radios must be equipped with duress capabilities.

(5) Base stations located within the CAS must have the capability to communicate with LLEA and other emergency response organizations as applicable.

(6) Portable radios must operate for an 8 hour period at maximum expected duty cycles. Procedures for radio exchange, battery exchange, or battery recharges can be used to meet this requirement.

h. Radio Frequency Alarm Communications. The radio frequency (RF) alarm communications systems must be limited to emergency, temporary situations, or early warning detection applications. When used, RF alarm communications

systems must be evaluated for vulnerabilities to spoofing and jamming and documented in an analysis approved by the ODFSA prior to implementation.

CHAPTER VII. SECURITY ELECTRICAL POWER AND LIGHTING

The intent of this Chapter is to establish requirements for security power and lighting systems.

1. PL-5 THROUGH PL-8 ELECTRICAL POWER. Sites protecting PL-5 through PL-8 assets must meet the following requirements:

    a. Power supply elements located or operating within the confines of the site must be protected from malicious physical attacks based on a documented analysis.

    b. The site must determine the need for auxiliary power based on S&S interests being protected and document it in the SP.

    c. IDS, VASS, and PACS, protecting Top Secret matter must have auxiliary power capability.

2. PL-1 THROUGH PL-4 ELECTRICAL POWER. Sites protecting PL-1 through PL-4 assets must meet the following requirements in addition to above:

    a. Primary Power Supply. All IDSs protecting S&S interests must have a primary power source from normal onsite power.

        (1) Early warning systems that have self- contained electrical power are exempt from this requirement.

        (2) Power sources must contain a switching capability for operational testing to determine required auxiliary power sources.

        (3) The following power supply requirements apply:

            (a) Alarm and Communication Systems. Normal primary power must come directly from the onsite power distribution system or for isolated facilities, directly from the public utility.

            (b) Communications and Automated Information Systems, Alarm Stations, and Radio Repeater Stations. Essential elements must be connected to an uninterruptible power supply or to auxiliary power.

            (c) Radio System Centers. Power supply requirements must be determined assuming that all transmitters are keyed simultaneously while associated receivers and other equipment and building services are in operation.

    b. Auxiliary Power Sources. IDS, automated access control, and VASS must have an auxiliary power capability.

(1) Transfer to auxiliary power must be automatic upon failure of the primary source and must not affect operation of the protection system, subcomponents, or devices or compensatory measures must be immediately implemented.

(2) The CAS and SAS must receive an alarm indicating failure of the protection system's primary power.

(3) When used, rechargeable batteries must be kept fully charged or subject to automatic recharging whenever the voltage drops to a level specified by the battery manufacturer.

(4) When used, non-rechargeable batteries must be replaced based on manufacturer's recommendations.

(5) Both rechargeable and non-rechargeable battery systems must be capable of generating a low battery alarm which must be transmitted to the CAS and SAS.

(6) Power sources must have the necessary built in features to facilitate periodic testing to verify their readiness.

c. Uninterruptible Power Supply. UPS must be provided for systems requiring continuous power and considered for systems that, if interrupted, would degrade the protection of the associated security area.

3. PL-5 THROUGH PL-8 LIGHTING. Sites protecting PL-5 through PL-8 assets must meet the following requirements. When used, lighting systems must facilitate the detection and assessment of unauthorized persons. Protective system lighting must:

a. Enable assessment of unauthorized activities and/or persons at pedestrian and vehicular entrances and allow examination of DOE security badges and inspections of personnel, hand carried items, packages, and vehicles;

b. Be positioned so that PF personnel are not spotlighted, blinded, or silhouetted by the lights, and the lighting placement and design should enhance, not minimize, PF night vision capabilities;

c. Ensure that compensatory measures identified in the SP are implemented when lighting systems used for assessment of IDS alarms fail, based on a documented analysis;

d. Be maintained and tested in accordance with locally approved procedures;

e. Not illuminate patrol paths or PF personnel manning fixed posts other than at entry points/portals;

f. Illuminate the area outside the fence line or barrier so that it will expose anyone approaching the coverage area and limit the vision of anyone outside of the fence or barrier;

g. Complement the VASS;

h. Illuminate the area within the fence/barrier boundary or the exterior of a building;

i. Be configured so that an intruder cannot defeat the system by easily gaining access to the lighting controls and turning off the system; and

j. Allow for the rapid and reliable assessment of alarms from either the VASS or PF personnel.

4. PL-1 THROUGH PL-4 LIGHTING. Sites protecting PL-1 through PL-4 assets must meet the following requirements in addition to above:

a. Sufficient lighting for assessment must be maintained on the PIDAS sensor zones and the clear zones for video assessment and surveillance 24 hours a day based on a documented analysis. Analysis must consider shadows and dark spots in the field of view that degrade VASS and personnel alarm assessment.

b. Where protective lighting at remote locations is not feasible, PF patrols and/or fixed posts must be equipped with night vision and/or thermal imaging devices.

Night vision and/or thermal imaging devices should not be used routinely in lieu of protective lighting at entrances and exits but may be used if lighting is lost.

c. Light glare must be minimized.

d. Light sources on protected perimeters must be located so that illumination is directed outward so that the PF is not blinded or silhouetted.

e. When back up emergency lighting is used, it must be periodically tested to ensure that it will function as configured for a specified sustained period.

CHAPTER VIII. SECURITY DATA TRANSMISSION AND LINE SUPERVISION

The intent of this Chapter is to establish line supervision, zone supervision, and data transmission requirements for DOE IDS, PACS, VASS, and other Physical Protection Systems as appropriate.

1. GENERAL REQUIREMENTS. For the purposes of this Order:

   a. Line supervision is the signal confirmation of a communication path accomplished by regularly sending and receiving messages over the path in a specified timeframe. The 2-way exchange between the protected property and the monitoring station is often referred to as a "check-in" or "heartbeat" e.g. when a field processor sends a daily test signal through a phone line or network connection.

   b. Line security is considered to exist where a communication channel between the alarmed area and the alarm station is supervised against being compromised via surreptitious attack. Encrypted line security is where the signal transmission line is supervised by a means employing a data encryption standard. Standard line security is where a signal transmission line is supervised by a means other than encryption.

   c. Zone supervision is used for detection circuits, i.e. IDS alarm detection zones and PACS inputs such as door position switches and request to exit devices e.g. end-of-line (EOL) resistors.

   d. Data transmission is digital data transmitted between field processors and host systems e.g. badge information digitally transmitted from a card reader to a field processor and ultimately the host computer.

2. IDS DETECTION CIRCUITS. IDS detection circuit zone supervision must meet the following requirements:

   a. All signal lines connecting detection sensors to field processors etc. must be supervised using EOL resistors or some other device that accomplishes the same objective.

   b. EOL devices must be physically located at the supervised device e.g. at the end of the wire run from the field processor to the detection sensor.

   c. Supervision on these circuits must protect against simple electrical bridging of the system or compromise of the system by any of the following means.

      (1) Substitution of resistance, voltage, or current,

      (2) Substitution of equipment of the same design and manufacturer,

      (3) Introduction of signals onto the path that were synthesized externally.

d. The tamper switch and transmission medium must be supervised to the same extent regardless of the armed or disarmed state of the system.

e. For PL-1 through PL-4 in addition to the above requirements;

Alarm zones employing EOL devices must be provided with four-state supervision (see Attachment 7 Definitions).

3. IDS COMMUNICATIONS CIRCUITS. Communications line supervision requirements:

a. All IDS must be provided with line supervision and must be programmed at a minimum for daily check-in signals to be sent to the alarm monitoring station.

b. IDS used to protect PL-1 through PL-4 assets must be provided with line security as follows:

(1) Provide central station line security in accordance with UL 1076 the *Standard for Proprietary Burglar-Alarm Units and Systems*, or UL 1610 *Central-Station Burglar-Alarm Units*, or UL 1635 *Digital Alarm Communication System Units,* or

(2) Provide encrypted line security by a means employing a data encryption standard. The encryption must be at least 128-bit that meets Federal Information Processing Standards (FIPS) 197 *Advanced Encryption Standard (AES)* or equivalent.

4. PACS. PACS zone supervision must meet the following requirements.

a. Inputs such as door position switches and request to exit devices must be supervised at a minimum with EOL devices.

b. PL-1 through PL-4 PACS inputs must be provided with four-state supervision (see Attachment 7 Definitions).

5. VASS. Must be protected against malicious tampering which could degrade the ability to assess alarms based on a documented analysis.

6. DATA TRANSMISSION.

a. IDS and PACS data that is carried on transmission lines to a lower security area than the area being protected must be encrypted with 128 bit or greater encryption algorithm that meets FIPS-197, or equivalent.

b. If the communication technology described above is not feasible, the transmission line must be installed within a protective covering to preclude surreptitious manipulation or be supervised to protect against modification and/or substitution of the transmitted signal.

ATTACHMENT 7. PHYSICAL PROTECTION PROGRAM DEFINITIONS

1. GENERAL DEFINITIONS. Terms commonly used in the program are defined in the AU Policy Information Resource (PIR) website, https://pir.doe.gov/. Use of these definitions is not mandatory. They are provided as a resource to information security planners, managers and practitioners.

2. TECHNICAL DEFINITIONS. The following list of definitions is meant to provide clarity for additional terms used within this Order. If there should be a conflict between the PIR definitions and this Order, this Order takes precedence.

   a. **ACCEPTANCE TESTING**. The process of exercising or evaluating a system or system component by manual or automated means to ensure that it satisfies the specified requirements and the system or component performs as intended in the operating environment.

   b. **ACCESSIBLE PATH**. A continuous path, humanly achievable, connecting a location outside an area being protected by IDS to an asset.

   c. **ALARM ASSESSMENT**. The process of determining an alarm condition stimulus.

   d. **ALARM SHUNT**. A pre-defined programmable period of time when alarms are NOT sent to the monitoring station due to a valid, authorized entry into or exit from an area.

   e. **ALARM ZONE**. A specified area that is protected by one or more intrusion detection devices.

   f. **ANNUNCIATOR**. A visual or audible signaling device (monitor) that indicates the condition of associated circuits.

   g. **ANTI-PASSBACK**. An access control feature which prevents authorized users from accessing an area and subsequently passing their credential to a second person to gain access.

   h. **ANTI-TAILGATING.** An access control feature which precludes the passage of more than one person upon a single authorized access attempt.

   i. **BALANCED MAGNETIC SWITCH**. A magnetically operated switch using a balanced magnetic field, designed to detect the opening of a secured door, window, or other point of entry. In addition, it detects attempts to defeat the switch by substituting a magnetic field and may have provisions for internal adjustments and detection of switch tampering attempts.

   j. **CENTRAL ALARM STATION (CAS)**. A continuously staffed centralized location from which a facility's IDS(s) and other security activities are monitored.

k. **COMPENSATORY MEASURES.** Safeguards or security activity designed to provide a level of protection to compensate for the degraded or inoperable equipment, system, or components until fully functional.

l. **COMPLEMENTARY INTRUSION DETECTION SENSORS.** Sensor combinations that enhance the system performance by mutually providing what the other lacks in terms of three sensor characteristics 1. Probability of detection, 2. Nuisance Alarm Rate, 3. Vulnerability to Defeat.

m. **DOOR FORCED OPEN ALARM**. An alarm which occurs at a monitored door if it is opened without presentation of a valid authorized card, such as through the use of a key or an actual forced entry.

n. **DOOR HELD OPEN ALARM**. An alarm which occurs following an authorized entry if the door is left open for a period which exceeds the programmed alarm shunt time.

o. **END OF LINE RESISTOR**. Resistors, of a known value, that are used to terminate protective circuits or alarm zones, the purpose of which is to provide zone supervision e.g. allow the field processor to supervise the field wiring for open or short circuit conditions.

p. **ENTRY CONTROL POINT**. A portal/facility which controls entry to and exit from PAs and MAAs.

q. **ESSENTIAL ELEMENTS**. For the purpose of this "Physical Protection Program" order essential element is used in the context of physical protection equipment e.g. physical protection system elements necessary for the initiation of a timely response, the failure of any one of which would result in protection effectiveness being significantly reduced.

r. **FALSE ALARM**. An alarm for which the specific cause is unknown but is not an attempt to defeat the detection system nor is it caused by an individual not following procedures (e.g., an individual forces open a door without using the card reader). False alarms can be an indication of electronic malfunction such as component failure, communications failure, loose connections, power faults, or many other issues.

s. **FALSE ALARM RATE (FAR)**. The frequency at which false alarms occur.

t. **FOUR STATE SUPERVISION**. This is the most secure wiring type. With double End-of-Line resistor wiring (series/parallel), the control panel is able to differentiate between four conditions:

(1) Zone normal

(2) Zone violated

(3) Open circuit: ∞Ω

(4) Short circuit: 0Ω

u. **GENERAL ACCESS AREA**. GAAs are areas that may be designated by the ODSA to allow access with minimum-security requirements.

v. **INTRUSION DETECTION SYSTEM (IDS)**. A physical security system consisting of sensors capable of detecting one or more types of phenomena, signal media, annunciators, energy sources, alarm assessment systems, and alarm reporting elements including alarm communications and information display equipment. The term IDS has no association with a cyber IDS which is a cyber/network security technology designed for detecting vulnerabilities such as unauthorized intrusion into network or computer systems.

w. **INVALID CARD READ**. An attempt to use an access card at the wrong door (user is not authorized access to the area) or at the wrong time (users access is limited to specific days/times) usually resulting in an "access denied" message.

x. **JUNCTION BOX**. A box where wiring is spliced either by terminal block or mechanical means. A pull box (box used to pull wire but not spliced) is not a junction box.

y. **KNOWLEDGE-BASED AUTHENTICATION**. A method of authentication based on knowledge of personal information associated with the asserted identity. This may involve the use of information sent to the individual in advance as part of the access control process or use answers to questions generated from a wider base of personal information (e.g., previous addresses) to which the agency has access.

z. **LIMITED AREA (LA)**. The minimum level security area designated for the protection of classified matter and Departmental assets requiring limited access.

aa. **MATERIAL ACCESS AREA (MAA)**. A type of security area that is approved for use, processing, and/or storage of a Category I quantity or other quantities of special nuclear material that can credibly roll-up to a Category I quantity and which has specifically defined physical barriers, is located within a protected area, and is subject to specific access controls.

bb. **MUSTER REPORT**. A system generated report which accounts for personnel in a certain area.

cc. **NUISANCE ALARM**. The alarm produced by an intrusion detection sensor in response to a known stimulus (e.g., wind, lightning, thunder, accident) unrelated to an intrusion attempt.

dd. **NUISANCE ALARM RATE (NAR)**. The frequency at which nuisance alarms occur.

ee. **OVERWATCH**. The process of watching from a position which allows observation of those involved in an activity (i.e., inspection activities at an entry control facility) and providing support if necessary.

ff. **PERIMETER INTRUSION DETECTION AND ASSESSMENT SYSTEM (PIDAS)**. A mutually supporting combination of barriers, clear zones, lighting, and electronic intrusion detection, assessment, and access control systems constituting the perimeter of the protected area and designed to detect, impede, control, or deny access to the protected area.

gg. **PERSONAL IDENTITY VERIFICATION (PIV) CREDENTIAL**. The HSPD-12 compliant credential is a physical identity card/smart card issued to Federal employees and contractors that contains authentication mechanisms that are used to verify the claimed identity of the cardholder.

hh. **PHYSICAL ACCESS CONTROL SYSTEM (PACS)**. An electronic system that controls the ability of people to enter an area by means of authentication and authorization at access control points. (NIST Special Publication (SP) 800-116, Rev.1, Appendix G).

ii. **PORTAL.** An entry point, door, mantrap booth or other access control points to a designated area.

jj. **PROPERTY PROTECTION AREA (PPA)**. A type of security area having defined boundaries and access controls for the protection of Departmental property.

kk. **PROTECTED AREA (PA)**. A type of security area defined by physical barriers (i.e., walls or fences) and surrounded by intrusion detection and assessment systems, to which access is controlled, used to protect Category II special nuclear material and classified matter and/or to provide a concentric security zone surrounding a material access area.

ll. **PROTECTION LEVEL (PL)**. A graded protection approach which categorizes Department assets into levels or categories based on consequence of loss. Protection levels are defined for specific assets. Since Departmental facilities have multiple asset categories, sites will have multiple protection levels.

mm. **RESPONSE TIMELINE.** The time it takes for a responder to get from their ready position to their response location.

SECONDARY ALARM STATION (SAS). A continuously staffed location, physically separated from the Central Alarm Station, with the capability to provide alarm annunciation and response as a back-up to the Central Alarm Station, so that a single act cannot remove the capability of calling for assistance or otherwise responding to an alarm.

nn. **SECURITY PLAN**. An official document that describes the methodologies, implementation, and the use of resources by a facility to protect the facility, its sites, and its assets.

oo. **SECURITY RISK ASSESSMENT (SRA)**. An evaluation of potential threats against a safeguards and security interest and the development of potential countermeasures to address vulnerabilities. It also provides the decision-maker with a firm foundation on which to make informed decisions regarding the effectiveness of a safeguards and security system.

pp. **STAND-ALONE NETWORK**. A network comprised of information systems only and exclusively capable of communicating with other information systems on the stand-alone network.

qq. **SUPERVISORY ALARM**. An alarm that notifies operators of system problems such as loss of communications, loss of primary power, etc. depending upon the specific system used.

rr. **THREE-FACTOR AUTHENTICATION**. Authenticating something you have, and something you know, and something you are. In the context of this Order the PIV is something you have; something you know is a PIN and something you are is Biometric authentication.

ss. **TIMELY RESPONSE**. A response based on adversary task times and responder timelines that would mitigate the DBT adversary threat.

tt. **TWO-FACTOR AUTHENTICATION**. Authenticating something you have, and something you know or something you are. In the context of this Order the PIV is something you have; something you know is a PIN and something you are is Biometric authentication.

uu. **VALID CARD READ**. An authorized access control card has been presented by a user who is authorized access at that door at that time usually resulting in an "access granted" message.

vv. **VIDEO ASSESSMENT AND SURVEILLANCE SYSTEM (VASS)**. Video systems used in the assessment of intrusion detection alarms and for the remote surveillance of DOE assets.

ATTACHMENT 8. PHYSICAL PROTECTION PROGRAM REFERENCES

1. The following URL's are provided for convenience:

   - DOE Orders referenced in this Order can be located on the DOE Directives webpage, https://www.directives.doe.gov/.
   - DOE Technical Standards referenced in this Order can be located on the DOE Technical Standards webpage, https://www.standards.doe.gov/.
   - Other referenced material may be located at the AU Policy Information Resource website, https://pir.doe.gov/.

   NOTE: Whenever a legal, regulatory, or other external standard, or a DOE Policy, Order, Notice or Manual is referenced, and such standard is amended or superseded, the successor standard or Order is applicable under this Order.

2. The following references are applicable to the Physical Protection Program.

   a. Public Law (P.L.) 106-65, National Defense Authorization Act for Fiscal Year 2000

   b. P.L. 114-328, National Defense Authorization Act for Fiscal Year 2017

   c. P.L. 81-152, Federal Property and Administrative Services Act of 1949 (as amended) (Ch. 288, 63 Stat. 377, as amended)

   d. REAL ID Act of 2005

   e. 5 U.S. Code § 552a, *Records Maintained on Individuals*

   f. 50 U.S.C. § 2406, *Deputy Administrator for Naval Reactors*

   g. 50 U.S.C. § 2511, *Naval Nuclear Propulsion Program*

   h. 18 U.S.C. § 930, *Possession of Firearms and Dangerous Weapons in Federal Facilities*

   i. 18 U.S.C., Part I, Chapter 119, § 2511(2)(d), *Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited*.

   j. 21 U.S.C. § 841, Prohibited Acts A

   k. 42 U.S.C. § 2278a, *Trespass on Commission Installations*

   l. 42 U.S.C. § 7270b, *Trespass on Strategic Petroleum Reserve Facilities*

   m. 7 CFR § 3 31.11, *Possession, Use, and Transfer of Select Agents and Toxins*, Security

n. 9 CFR § 121.11, Possession, Use and Transfer of Select Agents and Toxins, Security

o. 9 CFR § 122, Organisms and Vectors

p. 10 CFR Part 860, Trespassing on Department of Energy Property

q. 10 CFR 1017 Subpart E, Physical Protection Requirements

r. 10 CFR Part 1048, Trespassing on Strategic Petroleum Reserve Facilities and Other Property

s. 10 CFR § 712.10, *Human Reliability Program*, Designation of HRP Positions

t. 41 CFR Part 102, *Federal Management Regulation*

u. 42 CFR § 73.11, *Select Agents and Toxins*, Security

v. 48 CFR § 952.204-2, *Security*

w. 48 CFR § 970.0470-2, *Contract Clause*

x. 48 CFR § 970.5204-2, *Laws, Regulations, and DOE Directives*

y. Executive Order 12344, Naval Nuclear Propulsion Program

z. ANSI/BHMA A156.2-2017, Bored and Preassembled Locks and Latches

aa. ASTM F2656 / F2656M-20, Standard Test Method for Crash Testing of Vehicle Security Barriers

bb. ASTM F792-17e1, *Standard Practice for Evaluating the Imaging Performance of Security X-Ray Systems*

cc. CID A-A-59486D, *Padlock Set (Individually Keyed or Keyed Alike)*

dd. CID A-A-59487D, *Padlock (Key Operated)*

ee. Federal Information Processing Standard (FIPS) 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors

ff. FIPS 197, Advanced Encryption Standard

gg. FIPS 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors

hh. Federal Specification FF-L-2740B, Amendment 1, Locks, Combination, Electromechanical

ii. Federal Specification FF-L-2890C, Amendment 3, Lock Extensions (Pedestrian Door Lock Assembly Preassembled, Panic, and Auxiliary Deadbolt)

jj. Federal Specification FF-P-110J Amendment 1, Padlock, Changeable Combination (Resistant to Opening by Manipulation and Surreptitious Attack)

kk. FED-STD-832, Federal Standard Construction Methods and Materials for Vaults

ll. Federal Specification FF-L-2937 Amendment 2, Combination Lock, Mechanical

mm. Homeland Security Presidential Directive 12 (HSPD-12): Policy for a Common Identification Standard for Federal Employees and Contractors

nn. Intelligence Community Standard (ICS) ICD/ICS 705, Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities, Version 1.4

oo. Military Specification MIL DTL 43607J1, Padlock, Key Operated, High Security, Shrouded Shackle

pp. National Fire Protection Association (NFPA) 101, Life Safety Code, 2018

qq. National Institute of Justice (NIJ) Standard 0601.02, Walk-Through Metal Detectors for Use in Concealed Weapon and Contraband Detection

rr. NIST Special Publication (SP) 800-116, Rev 1, Guidelines for the Use of PIV Credentials in Facility Access

ss. NIST SP 800-73-4, Interfaces for Personal Identity Verification – Part I: PIV Card Application Namespace, Data Model and Representation

tt. NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations

uu. Underwriters Laboratories (UL) 1076, Standard for Proprietary Burglar-Alarm Units and Systems

vv. UL 1610, Central-Station Burglar-Alarm Units

ww. UL 1635, Digital Alarm Communication System Units

xx. UL 2050, National Industrial Security Systems

yy. UL 634, Standard for Safety Connectors and Switches for Use with Burglar-Alarm Systems

zz. UL 752, Standard for Bullet Resisting Equipment

aaa. UL 827, Standard for Central Station Alarm ANSI/BHMA A156.13-2017, Mortise Locks & Latches, Series 1000

bbb. DODM S-5210.41-M-V2, *Nuclear Weapon Security Manual*, Enclosure 2, Section 3.b.(6)(c)(U)

ccc. National Archives and Records Administration (NARA) General Records Schedule (GRS) 5.6: Security Records

ddd. DOE Policy 434.1, *Conduct and Approval of Select Agent and Toxin Work at DOE Sites*, current version

eee. DOE Order 142.3, *Unclassified Foreign National Access Program*, current version

fff. DOE O 205.1, *DOE Cybersecurity Program*, current version

ggg. DOE O 251.1, *Departmental Directives Program*, current version

hhh. DOE O 414.1, *Quality Assurance*, current version

iii. DOE O 430.1, *Real Property Asset Management*, current version

jjj. DOE O 440.2, *Aviation Management and Safety*, current version

kkk. DOE O 460.2, *Departmental Materials Transportation and Packaging Management*, current version

lll. DOE O 461.1, *Packaging and Transportation for Offsite Shipment of Materials of National Security Interest*, current version

mmm. DOE O 470.3, *Design Basis Threat*, current version

nnn. DOE O 470.4, *Safeguards and Security Program*, current version

ooo. DOE O 470.6, *Technical Security Program*, current version

ppp. DOE O 471.1, *Identification and Protection of Unclassified Controlled Nuclear Information*, current version

qqq. DOE O 471.3, *Identifying and Protecting Official Use Only Information*, current version

rrr. DOE O 471.5, *Special Access Programs*, current version

sss. DOE O 471.6, *Information Security*, current version

ttt. DOE O 474.2, *Nuclear Material Control and Accountability*, current version

uuu. DOE O 475.2B, *Identifying Classified Information*, current version

vvv. DOE Guide 151.1-5, *Biosafety Facilities Emergency Management Guide*, current version