DoD Manual S-5210.41, Volume 2

(U) Nuclear Weapon Security Manual: General Nuclear Weapon Security Procedures

Originating Component:	Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics
Effective:	August 11, 2016
Releasability:	Not cleared for public release. Available to authorized users from the DoD Issuances Website on the SECRET Internet Protocol Router Network at https://www.dtic.smil.mil/whs/directives.
Reissues:	DoD Manual S-5210.41, "Nuclear Weapon Security Manual: The DoD Nuclear Weapon Security Program," July 13, 2009
Approved by:	Arthur T. Hopkins, Principal Deputy Performing the Duties of Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs

(U) Purpose: (U) This manual is composed of several volumes, each containing its own purpose. The purpose of the overall manual, in accordance with the authority in DoD Directives (DoDD) 5134.08 and O-5210.41, is to:

- (U) Implement policy, assign responsibilities, and prescribe mandatory procedures for the security of nuclear weapons.
- (U) Describe DoD security policy, objectives, and concepts, and prescribe minimum security criteria for protecting nuclear weapons on alert, in storage, in maintenance facilities, in-transit, and in regeneration situations.
- (U) Implement the Nuclear Security Threat Capabilities Assessment (NSTCA), including subsequent updates or replacement threat capabilities assessments (TCAs) as endorsed by the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs (ASD(NCB)); provide security planning guidance; and describe security requirements for selected weapon configurations.
- (U) This volume prescribes the general security procedures applicable to all DoD nuclear weapon security environments.

TABLE OF CONTENTS

(U) TABLE OF FIGURES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. (U) APPLICABILITY. This volume:

a. (U) Applies to the OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the "DoD Components").

b. (U) Does **not** abolish or abridge the authority or responsibility of a commander to apply different but equal (or more stringent) criteria and standards during emergencies. Such a change in standards does not abolish the requirement for maintaining U.S. control of nuclear weapons and components. Improvements to storage facilities requiring construction effort or procurement should be accomplished in accordance with Section 5 of Volume 1 and Section 3 of Volume 2 of this manual.

c. (U) Does **not** provide protection standards for nuclear command and control (NC2) facilities or special nuclear materials (SNM). Protection standards for NC2 facilities and SNM are provided by DoD Manual (DoDM) S-5210.92 and DoD Instruction (DoDI) O-5210.63, respectively.

d. (U) Pertains to all nuclear weapons, nuclear weapon systems, and nuclear components for which DoD Components have operational, maintenance, or custodial responsibility. The standards and criteria contained in this volume are the absolute minimums required to be implemented. Additional security measures may be required as dictated by threat, site configuration, topography, or operational considerations.

1.2. (U) POLICY. In accordance with DoDD 5210.41, it is DoD policy that

a. (U) Nuclear weapons are assets vital to the security of the United States. Nuclear weapons require special protection because of their political and military importance, their destructive power, and the consequences of an unauthorized deliberate or inadvertent pre-arming, arming, launching, releasing, or detonation.

b. (DCNI) The central and overriding objective for nuclear weapon security will be **denying** an adversary unauthorized access to nuclear weapons. In instances where an adversary gains unauthorized access to nuclear weapons, commanders will take any and all actions necessary to regain control of the nuclear weapons immediately.

1.3. (U) CLARIFYING INFORMATION.

a. (U) Warning Statements.

(1) (U) *Information removed.*

(2) (U) *Information removed.*

(3) (U) The remaining paragraphs of this volume contain UNCLASSIFIED information, some of which is protected as DoD Unclassified Controlled Nuclear Information (DCNI) in accordance with DoDI 5210.83. The decision to protect this information as DoD Unclassified Controlled Nuclear Information is based on the determination that the unauthorized dissemination of such information could reasonably be expected to have an adverse effect on the health and safety of the public and the security of DoD nuclear weapons, components, and facilities. Accordingly, users of this volume are prohibited from the unauthorized dissemination of DCNI contained herein regarding U.S. nuclear weapons security policy.

b. (U) Descriptive Words. The language used in this volume includes:

(1) (U) Mandatory guidance includes the words "will" or "must," and provides standards, measures, or actions that are required and subject to inspection. An inability to meet the requirement in this manual necessitates a request for a deviation as described in Section 6.

(2) (U) Recommendations in this volume that, although not mandatory, provide a framework to support implementation of the mandatory guidance more fully but are not within the purview of this volume to mandate (e.g., use of the word "should").

(3) (U) Enabling procedures that permit actions or measures within described parameters (e.g., use of the words "may" or "can"). These are not requirements, but are offered as possible actions or measures to take at the discretion of the responsible party.

SECTION 2: RESPONSIBILITIES

2.1. (U) ASD(NCB). Under the authority, direction, and control of the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), the ASD(NCB):

a. (U) Provides management oversight of the nuclear weapon security program.

b. (U) Maintains and monitors prescribed nuclear security management processes.

c. (U) Reviews the DoD Component implementation guidance for consistency and compliance with policy stated within in this manual..

d. (U) Conducts programmatic reviews and management audits of nuclear weapons security processes.

2.2. (U) DIRECTOR, DEFENSE THREAT REDUCTION AGENCY (DTRA). Under the authority, direction, and control of the ASD(NCB), the Director, DTRA:

a. (U) Executes the DoD-sponsored nuclear security policy evaluations and activities and administers Joint Staff inspections as specified in Section 6.

b. (U) Conducts an annual DoD nuclear weapons security deviation analysis and provides a report of the analysis to the Deputy Assistant Secretary of Defense for Nuclear Matters (DASD(NM))

2.3. (U) DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA). Under the authority, direction, and control of the Under Secretary of Defense for Intelligence, the Director, DIA, annually reviews and updates relevant threat capability assessments, as necessary.

2.4. (U) GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE. The General Counsel of the Department of Defense reviews nuclear weapon security policy and guidelines for legal sufficiency.

2.5. (U) SECRETARIES OF THE MILITARY DEPARTMENTS. The Secretaries of the Military Departments who are involved with nuclear weapons in DoD custody and their associated systems or components, or who provide nuclear weapons support to designated Combatant Commanders or other DoD Component heads:

a. (U) Implement this volume and make it part of their normal assurance and assessment process, including DoD Component Inspector General assessments as specified in Section 5.

b. (U) Use this manual, DoDD O-5210.41, and the NSTCA as the primary nuclear weapon security planning references.

c. (U) Size, organize, train, arm, and equip location specific response forces (RF) and initial and subsequent backup forces (BF) to maneuver as tactical elements as a combined force capable of defeating an adversary force.

d. (U) Direct responsible commanders at locations with nuclear weapons to conduct annual vulnerability and risk analyses, in accordance with the procedures outlined in this volume. Such analyses must address all relevant factors, including:

(1) (U) Weapons location.

(2) (U) The configuration in which the weapons are maintained (e.g., storage, transport, maintenance, on alert).

(3) (U) The nature and capabilities of potentially hostile forces.

(4) (U) The reliability and capabilities of personnel responsible for working with or protecting nuclear weapons.

e. (U) Provide a security concept of operations for new or modernized security systems (e.g., electronic security system (ESS) or subsystem, entry control and circulation control system or subsystem, area protection system or subsystem, facility protection system or subsystem, weapon movement protection system or subsystem, security force composition, or response times) to the ASD(NCB) for review.

f. (U) Adhere to the minimum security criteria and standards for denying unauthorized access to nuclear weapons.

g. (U) Comply with the concepts and procedures, described in detail in this manual, for denying unauthorized access to nuclear weapons. Implement procedural requirements immediately.

h. (U) Take all necessary actions to maintain control of U.S. nuclear weapons and components in emergency circumstances, even if these actions do not meet the prescribed standards in this manual.

i. (U) May issue supplementary instructions, when necessary, to provide for unique requirements within their respective Departments. Forward two copies of any additional guidance issued to the DASD(NM) through CJCS, within 30 days of publication and after each subsequent change.

j. (U) Direct and ascertain compliance that improvements to storage facilities requiring construction effort or procurement are accomplished in accordance with Section 3.

k. (U) Provide operating units with access to commercially available modeling and simulation tools to validate local security plans.

2.6. (U) CJCS. The CJCS:

a. (U) Provides nuclear weapon recapture and recovery guidance for lost, stolen, or missing nuclear weapons or nuclear components.

b. (U) Upon receipt, forwards to the DASD(NM) supplemental guidance to this volume issued by the Military Departments and Combatant Commands.

2.7. (U) COMBATANT COMMANDERS WITH NUCLEAR RESPONSIBILITIES. The Combatant Commanders with nuclear responsibilities:

a. (U) Support the full, applicable range of nuclear weapon security policy.

b. (U) Through the component commands, ensure physical security and protection against physical damage, misuse, and theft of nuclear weapons and nuclear components under their control.

c. (U) Coordinate the development of plans and procedures for the nuclear weapons security program, and provide resources to work with other organizations to recover lost, stolen, or missing nuclear weapons or nuclear weapon components.

d. (U) Advocate for emerging nuclear security requirements submitted by DoD organizations by giving due analysis and consideration including these requirements in the integrated priority lists.

e. (U) Increase security protection as necessary and ensure continuity of efforts between nuclear weapon security, installation and Ship Submersible Ballistic Nuclear force protection, and operational missions

f. (U) May issue supplementary instructions, when necessary, to provide for unique requirements within their Command. Forward any supplemental instructions to the DASD(NM), through the CJCS, within 30 days of publication and after each subsequent change.

2.8. (U) COMMANDER, U.S. SPECIAL OPERATIONS COMMAND (USSOCOM). The Commander, USSOCOM:

a. (U) *Classified information removed.*

b. (U) *Classified information removed.*

c. (U) *Classified information removed.*

d. (U) Has direct liaison authority with all organizations involved in order to facilitate mission support.

e. (U) In coordination with the USD(AT&L) and the Under Secretary of Defense (Comptroller)/Chief Financial Officer, delineates funding requirements and responsibilities for USSOCOM support to DTRA to identify resource requirements and support the development of program decision memorandums.

SECTION 3: (U) GENERAL NUCLEAR WEAPON PHYSICAL SECURITY REQUIREMENTS

3.1. (U) GENERAL. These requirements apply to the protection of nuclear weapons in storage, transit, or operational configurations. Weapon system-specific requirements are outlined in Sections 3 through 9 of Volume 3 of this manual. Security force requirements are described in Section 7 of Volume 1 of this manual. Unless modified or exempted in the weapon system-specific Sections of Volume 3, the requirements of this section will apply to **all** weapon configurations.

3.2. (U) AREA PROTECTION SYSTEM.

a. (U) Topographic Features.

(1) (U) Vegetation. Remove underbrush and low hanging tree branches, which obstruct security force observations or help conceal intruders and thin forested areas. Retain a sufficient number of trees to form a natural impediment to incursion by helicopters or other aircraft. Ground vegetation may be retained; however, it will be kept trimmed to permit use of wide area detection, tracking, and surveillance systems and preclude intruder concealment.

(2) (U) Terrain.

(a) (U) Fill in ravines, gullies, sink holes, and other depressions not necessary for drainage or erosion control, or place obstacles to impede quick movement and prevent giving a tactical advantage to intruders. Don't fill in depressions that provide a tactical advantage to the security force, as long as the security force plans cover such depressions with direct or indirect fire if they become occupied by hostile forces.

(b) (U) Grade or reshape existing terrain and geological features to minimize their capacity to conceal intruders. Examine depressions approaching the limited area and, as required, modify them to limit use by intruders as avenues of approach or areas of concealment or observation.

b. (U) Perimeter Boundary Barrier Subsystem.

(1) (U) Composition. The perimeter boundary barrier subsystem will consist of:

(a) (U) Perimeter boundary fencing.

(b) (U) Clear zones.

(c) (U) Final denial and perimeter defensive positions.

(d) (U) Area warning system.

(e) (U) Vehicle barriers.

(2) (U) Perimeter Boundary Fencing.

(a) (U) Requirements. Perimeter boundary fencing must:

1. (U) Identify physical limits of the site, deter unauthorized entry, and define the point at which intruders may be subject to deadly force

2. (U) Create a physical and psychological deterrent to unauthorized entry.

3. (U) Facilitate detection and allow the security force to apprehend or neutralize any intruders before they can gain unauthorized access.

4. (U) *Classified information removed.*

(b) (U) Physical Boundary Fencing. Locate permanent physical boundary fences (considering required clear zones, terrain features, property lines, and building layouts) no less than 30 feet (9.1 meters (m)) from buildings or objects being protected. New boundary fencing will be constructed greater than 100 feet (30.48 m) from nuclear storage and maintenance facilities.

(c) (U) Boundary Fence Requirements. Use two boundary fences separated by at least 30 feet and no more than 150 feet (approximately 9 to 46 m). In some environments, single boundary fences are permitted if they meet the specifications of Paragraph 3.2.b.(2)(d). For single boundary fence systems, consider installation of an animal control fence at least 30 feet (9.1 m) outside the site boundary fence if conditions warrant.

(d) (U) Fencing Specifications. Fencing used in the perimeter security system will meet the requirements of U.S. Federal Specification RR-F-191K/GEN and be constructed and configured as described in Paragraphs 3.2.b.(2)(d)1 through 3.2.b.(2)(d)9.

1. (U) Fabric. The perimeter fences must be chain link, 2-inch (5.1 centimeters (cm) square mesh, woven 9-gauge (0.1483 inches/3.8 millimeter (mm)) steel wire fabric. In each instance, the steel core will measure 9-gauge, not including any coating. Fences may be painted with a non-reflective substance to reduce glare.

2. (U) Mountings. The fence fabric will be mounted on metal posts set in concrete, with additional bracing and fasteners as necessary at corners and gate openings. In areas where metal posts are not available, substitute with reinforced-concrete posts. Locate posts, bracing, and other structural members on the inside (i.e., the site side) of the fence fabric.

3. (U) Height. The minimum height of the top of the mesh fabric above the ground surface will be 7 feet (approximately 2.13 m).

4. (U) Topping. Install two 15-inch (38.10 cm) long outriggers, each with three strands of barbed wire, along the top of each fence. Install the outriggers at 45 degree angles in a "Y" configuration. Nuclear sites employing an approved taut wire sensor system or equivalent service approved detection capability on top of the fence are exempt from the requirements of this paragraph alleviating the requirement for a deviation submission.

5. (U) Top Rails or Reinforcing Wire. Install top rails or taut reinforcing wire at the top of the fence fabric, below the outriggers or taut wire sensor, to stabilize the fabric.

6. (U) Anchoring. The bottom of the fence fabric will extend to within 2 inches (5 cm) of firm ground and be anchored to prevent intruders from lifting the fabric to create an opening more than 5 inches (12.7 cm) in height. Use horizontal bottom rails, concrete curbs or sills, sheet piling, piping, or other cost-effective anchoring devices to accomplish this. Use wire to anchor the fence fabric to the bottom rails or similar device of equal or greater gauge than the fence fabric and locate it on the inside of the fence fabric.

7. (U) Stabilization. Surfaces will be stabilized in areas where loose sand, shifting soils, or surface waters can cause erosion and thereby assist an intruder in penetrating the perimeter security system. Where surface stabilization is not possible or is impractical, provide concrete curbs or sills, or other similar type of anchoring devices, extending below ground level.

8. (U) Gates. The perimeter fence will have the minimum number of vehicular and pedestrian gates consistent with operational requirements. Gates will be structurally comparable, provide the same resistance to penetration as the adjacent fence, and be designed to keep the traffic through them under positive control of the security force. If necessary to facilitate their operation, gates may be equipped with vertical arm brackets and locking systems. Such brackets will be 18 inches (45.7 cm) long with at least three strands of 12-gauge (2.68 mm) barbed wire on 5-inch (12.7 cm) centers.

9. (U) Perimeter Drainage Openings. Drainage structures and water passages penetrating the perimeter fence will be barred with material equivalent to the fence itself to prevent unauthorized entry. Openings to drainage structures with a cross-sectional area greater than 96 square (sq) inches (approximately 619 sq cm) and a smallest dimension greater than 6.4 inches (approximately 16.3 cm) must be protected by securely fastened, welded bar grills. As an alternative, drainage structures can be constructed of multiple steel pipes, each pipe having an inside diameter of 10 inches (25.4 cm) or less. Multiple steel pipes of this diameter also may be placed and secured in the "in-flow" end of a drainage culvert to prevent intrusion into the area. New and upgraded boundary sensor systems will include sensor coverage employing dual phenomenology of boundary openings larger than 96 sq inches.

(e) (U) Building Walls. In rare circumstances, building walls may be incorporated in the perimeter security system if they are subjected to visual assessment. However, walls of structures housing weapons, alert weapon systems, or alert forces will not fulfill boundary fence requirements as a barrier. In such cases, the issue will be included in the unit vulnerability assessment and steps taken to eliminate the vulnerability. Deviation requests will be required as stated in Section 6.

(f) (U) Secondary Locks and Seals.

1. (U) Use padlocks meeting the requirements of U.S. Federal Specification FF-P-2827A to secure frequently used perimeter gates, manhole covers (that provide access to spaces that penetrate the perimeter fence with a cross-sectional area greater than 96 sq inches (approximately 619 sq cm) and a smallest dimension greater than 6.4 inches (approximately 16.3 cm) within the limited area or a space large enough for a person to obtain cover or concealment), access panels, culvert gratings, and alarm junction boxes. These locks may be master keyed or keyed alike.

2. (U) Infrequently used perimeter gates, manhole covers, access panels, culvert gratings, and alarm junction boxes within the limited area, if not similarly padlocked, melded, or welded, will be secured with seals meeting the requirements of Style D, Type 12, two-piece cable seal, or Style E, Type 13, unthreaded bolt lock seal contained in U.S. Federal Specification FF-S-2738A, or with uniquely keyed locking bolts. Other locks and seals may be used if they provide an equivalent level of delay.

3. (U) Obtain approval to substitute equivalent locks and seals from the DASD(NM) before installation or use.

(g) (U) Overhead Lines. Power and utility lines (wires) crossing over the top of the area fences are prohibited. Where it is necessary for power or utility lines to cross over the limited area boundary, positive measures will be provided that deny their use in circumventing the perimeter fence. A deviation is required as stated in Section 6 of this volume.

(3) (U) Clear Zones

(a) (U) General

1. (U) Fence Lines. Clear zones will consist of an area extending a distance of 30 feet (9.1 m) on either side of the site perimeter fence. For areas using two fence systems, the clear zone will consist of an area extending 30 feet (9.1 m) outside the outer fence, the entire area between the fences, and an area extending 30 feet (9.1 m) inside the inner fence. The clear zone will clearly delineate the zone of protection associated with limited areas and provide an unobstructed view to aid the security force in detecting any approaching threat.

2. (U) Entry Control Points (ECP). Clear zones will be established at personnel and vehicle entry areas extending 30 feet (9.1 m) outside the outer fence and gate and 30 feet (9.1 m) inside the inner fence and gate and include the entire area between the gates and fences.

(b) (U) Concept. Clear zones will:

1. (U) Facilitate detection and observation of an intruder.

2. (U) Deny protection and concealment to the intruder.

(c) (U) Topographical Features. Clear zones will be free of all obstacles and topographical features. Vegetation needed for erosion control or for legal reasons will not

exceed 8 inches (20.3 cm) in height and must be trimmed or pruned to eliminate concealment. Vegetation may be further trimmed to accommodate performance of the intrusion detection system (IDS) and assessment systems employed. Variations in the topography will be graded to permit reliable detection performance of the IDS and to aid observation.

(d) (U) Facilities Inside Clear Zones. Perimeter light poles, fire hydrants, steam pipes, or other similar objects, and entry control buildings that are within the clear zone and do not preclude assessment or facilitate unauthorized entry, do not violate the requirements of a clear zone alleviating the requirement for a deviation submission. They will be included in the vulnerability assessment.

(4) (U) Natural Barriers. Natural barriers, such as rough terrain or bodies of water, are not acceptable security protection for limited areas. Further, since the penetration of such barriers would not necessarily indicate willful intent to trespass, a perimeter security system must be provided even when there are natural barriers.

(5) (U) Defensive Positions. The configuration of the individual storage or operational areas, coupled with the capability of area personnel to react to attempted penetrations, may dictate the need for permanent final denial or perimeter defensive positions. When permanent final denial or perimeter defensive positions are necessary, they will be constructed as fighting positions, protect against small arms fire, and have communications equipment as described in Paragraph 3.2d(2)(b).

(a) (U) Where it is necessary to provide immediate lethal fire onto entrances or openings to exclusion areas, final denial fire positions must be manned as required. These positions will be located to provide a clear field of fire to deny access to nuclear weapon exclusion areas.

(b) (U) As the perimeter defensive concept is designed to preclude area penetration, responsible commanders will, on a site-by-site basis, determine the need for perimeter defensive positions. These positions need not be located on the perimeter. They should be located in the most advantageous positions inside these areas to channel the adversary's attack and provide a clear field of fire to protect storage facilities.

(c) (U) *Classified information removed.*

(6) (U) Warning Systems.

(a) (U) Concept. Provide a warning system to caution persons that the area is restricted and that trespassing may invoke the use of deadly force. Warnings must be communicated visually (signs) and audibly (by challenging) with sound amplification equipment.

(b) (U) Warning Sign Specifications. Install warning signs along the entire perimeter fence and at each entry point so they can be seen readily and understood by anyone approaching the perimeter. In areas where English is not commonly spoken, warning signs will contain the local languages in addition to English. Wording on the sign will denote warning of a restricted area. Suggested warning signs are depicted in Figures 1 and 2. At sites where military working dogs (MWD) are used, attach the sign depicted in Figure 2 immediately below the perimeter warning signs. Replace signs through attrition to comply with the requirements stated below. Signs will be constructed and positioned to these criteria:

1. (U) Colors. Signs will have a white background. The words "WARNING" and "USE OF DEADLY FORCE AUTHORIZED" must be in bright red; the remaining letters in dark blue or black. Lettering of the type shown in Figure 1 will be used and be legible from 50 feet (15.2 m) away. The use of reflective material is encouraged.

2. (U) Sizes. Signs will have a minimum surface area of 288 sq inches (1,858 sq cm) (for example, a minimum of 17 inches X 17 inches or 22 inches X 13.5 inches). Continue to use signs already in use that differ in size or color but conform to or can be neatly modified to satisfy the language requirement in the illustration until unserviceable, alleviating the requirement for a deviation submission.

3. (U) Positioning. Position signs on or outside the outer perimeter fence at not greater than 100-foot (30.5 m) intervals. Do not mount signs on fences equipped with IDS equipment. Position or hang signs so they do not aid in the concealment of an intruder, obstruct visual assessment, or contribute to degraded performance or circumvention of the IDS equipment.

Figure 1. (U) Perimeter Warning Sign (Applicable Sites)

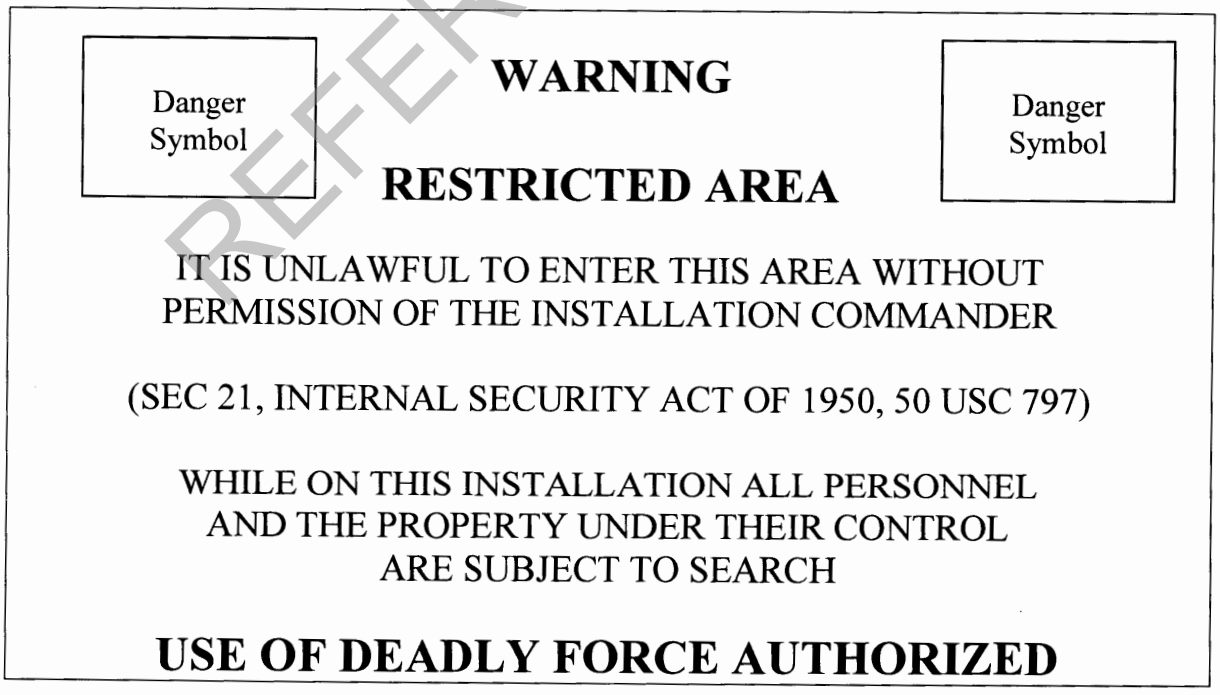

Figure 2. (U) MWD Warning Sign

PATROLLED BY MILITARY WORKING DOG TEAMS

(c) (U) Sound Amplification Equipment. Provide an operating sound amplification system to ensure audible coverage of the area perimeter. This system is to assist in warning intruders that the area is restricted and that trespassing may result in the use of force, including deadly force. This system may consist of hard-wired, wireless, or combination components.

(7) (U) Airborne Assault Threats. Take measures to maintain the nuclear weapon security standard (NWSS) against an airborne threat. Airborne assault protection may be:

(a) (U) Providing the security force with appropriate weapons and ammunition to defeat an airborne assault (include provisions for timely detection and warning).

(b) (U) Installing obstacles to airborne landings; or detection and warning systems for low altitude approaches by airborne threats.

(c) (U) Ensuring planners include communication protocols with the airspace controlling authority.

(d) (U) Ensuring Military Departments restrict airspace above permanent nuclear weapons storage or operational areas and develop the appropriate security force notification procedures. Designated installations with operational runways designated as controlled airspace (Class Bravo, Charlie, or Delta) is sufficient for this requirement.

(e) (U) Equipping the on-duty security force with the ability to visually warn encroaching aircraft to immediately depart the protected airspace and if hostile intent is displayed, visually hinder the ability of the aircraft to engage the security force.

(8) (U) Vehicle Barriers. Install appropriate vehicle barriers to prevent vehicle penetration of the perimeter at likely avenues of approach. Commanders may evaluate their storage areas to determine the locations most likely to be subject to vehicle penetration (for example, the immediate area around entry control points, streets, or roads), and provide barriers accordingly. Use existing force protection vehicle barrier system standards and protocols. For detailed requirements, see DoDI 2000.16.

c. (U) Area Lighting Subsystem.

(1) (U) Concept.

(a) (U) Lighted Sites. Provide security lighting for nuclear weapons areas to: discourage unauthorized entry and create a psychological deterrent to potential intruders; detect intruders approaching or attempting to gain entry into these areas by enhancing observation of the perimeter and clear zone; facilitate apprehension or neutralization if persons attempt to

penetrate the site; and enhance performance of other security functions during periods of darkness and reduced visibility.

(b) (DCNI) Backup Power. A backup power source is required to compensate for commercial power interruptions. Lighting must be a maintenance priority commensurate with the resource being protected.

(c) (U) Unlighted Sites. Permanent areas may be operated in an unlighted mode where night vision equipment is integrated into the site IDS and the security force is equipped with personal night vision devices and weapons sights, and trained in night combat tactics. Unlighted sites may optionally employ continuous or on-call lighting as described in Paragraph 3.2.c.(2).

(2) (U) Lighting System Specifications for Permanent Sites Employing "Lights On" as a Normal Mode of Operation. Position lighting within the site, along the perimeter, and at entry-control gates to provide adequate illumination of ECP areas for personnel identification, and in areas immediately surrounding the site according to the following criteria:

(a) (U) The lighting system will have an instant restart capability or uninterruptible power supply capable of restoring lighting fixtures to provide lighting sufficient to facilitate threat identification via video surveillance or posted sentry.

(b) (U) Perimeter lighting circuit design will assure that failure of one or more lights does not affect the operation of the remaining lights.

(c) (U) Provide gates and entrances with sufficient lighting to facilitate closed circuit television (CCTV), camera, or posted sentry surveillance during normal and reduced visibility conditions such that an intruder can be detected at 30 feet (9.1 m) from the outer boundary of the limited area.

(d) (U) Only light patrol roads or paths to reduce driving or personnel hazards.

(e) (U) Position perimeter and ECP lighting to preclude glare that blinds or silhouettes sentries at stationary guard posts.

(f) (U) Install perimeter lighting controls to enable activation at the Site Security Control Center (SSCC) or by security patrols, but take precautions to preclude easy access by unfriendly forces.

(g) (U) Position light poles and fixtures to preclude unauthorized use in circumventing the sensor field and the fence, or in concealing an intruder.

(h) (U) Design and position perimeter lighting to enable detection of persons in the entire clear zone 30 feet (9.1 m) inside the inner perimeter fence, between the fences, and 30 feet (9.1 m) outside the outer perimeter fence.

(i) (U) The requirement to light the inner clear zone does not apply where on-call lighting is provided and is activated on demand by site security personnel.

(3) (U) Illumination Requirements for Permanent Sites Employing "Lights Out" as a Normal Mode of Operation. Provide lighting consisting of 0.2 foot-candles (2 lux) illumination measured on the horizontal plane or 0.4 foot-candles (4 lux) illumination measured on the vertical plane. The measurements will be taken 6 inches (15.2 cm) above the ground during normal visibility conditions at a point 30 feet (9.1 m) from the outer fence.

(a) (U) Design the lighting system to provide uniform illumination. Ensure the ratio of the brightest to darkest regions is not more than 6:1, measured as described in Paragraph 3.2.c.(3). Design illumination to eliminate "hot" (comparatively much brighter) spots or "dark" (minimum allowed illumination) spots which could affect visual detection of an intruder by creating artificial shadows.

(b) (U) Provide lighting system controls at the SSCC or for security patrols for use. Boundary lighting sectors may be activated by the corresponding IDS alarms.

(4) (U) Illumination Requirements for Permanent Sites Employing Thermal Imaging Cameras in CCTV Systems for Boundary Surveillance and Alarm Assessment. Lighting systems are not required for proper operation of these systems. To support emergency security operations, lighting systems will be as described for "lights-out" operations in Paragraph 3.2.c.(3). Provide lighting systems controls at the SSCC.

(5) (U) Illumination Requirements for Permanent Sites Employing Visible or Very Near Infrared (VNIR) CCTV Systems for Boundary Surveillance and Alarm Assessment. VNIR lighting systems will provide a minimum illumination of 5 microwatts per square cm in the band from .8 to 1.1 microns measured horizontally 6 inches from the ground. The maximum to minimum light ratio will not be more than 6:1. The power output of VNIR light sources will be at least 90 percent of rated output within one half second after being switched on. For VNIR CCTV systems, the VNIR light sources will be controlled automatically from the alarm display and control console or manually by the alarm monitor operator. Low light and no light systems require a visible light capability to aid response forces.

d. (U) Area Command and Control Subsystem.

(1) (DCNI) Security Forces Communication System. Nuclear weapon sites require redundant and diverse communication systems for site security. Security forces protecting nuclear weapon sites will be equipped with multiple dedicated and reliable types of communications equipment. These communication systems will assure rapid contact among security personnel at the site, the SSCC, and the security response forces.

(2) (U) Criteria. In establishing the required communication system:

(a) (DCNI) At least two independent systems of communication will exist between the nuclear areas and the location responsible for notifying response forces. One of these systems will be encoded radio.

(b) (DCNI) Provide at least two independent systems of communication within the nuclear areas linking all fixed security force locations. One system will be encoded radio.

The second system will be a direct line type of telephone network or telephone with programmed auto dial to the fixed security force locations.

(c) (DCNI) The sentry telephone network will connect each permanent sentry post and the SSCC. The central telephone station will have a capability to call all telephones located in fixed sentry locations, separately or simultaneously. Equip storage structures and maintenance facilities either with a permanently installed receiver or with a phone jack, and include the capability for the central station to call any or all such facilities when occupied.

(d) (DCNI) Provide two-way radio communication between all patrols, including foot and mobile, and all other site security force vehicles and the SSCC. Equip every security force member with a two-way radio.

(e) (DCNI) The radio system must have the capability for uninterrupted operation. To provide uninterrupted operation of the base station, the SSCC will be provided with an interim power source. The power source will operate the radio communication system when commercial power is lost or until the standby generator can accept the load.

(f) (DCNI) The radio communication system will include repeater equipment when required. Provide repeaters the same level of physical protection, power stability, and security as the rest of the communications system.

(g) (DCNI) Radio equipment must use encoded voice communications. New radio equipment should include frequency hopping capability to preclude jamming.

(h) (DCNI) Alternate radio frequencies or separate means of communication will be available to the security force to enable continued communications during jamming or interference conditions. Train the security force to recognize radio jamming and methods to work through it, including implementing alternate methods of communication while the condition exists.

(i) (U) If using wireless security, the following requirements must be met:

1. (U) The minimum required security controls for information assurance for all nuclear physical security systems employing wireless technologies for the protection of unclassified information will adhere to the guidance contained in DoDI 3224.03.

2. (U) The nuclear physical security system will use two types of authentication with each type enforced by a Federal Information Processing Standard-validated or a National Security Agency-approved mechanism. The first type will authenticate the hardware device to the network. The second type will authenticate the user to the network.

3. (U) There are several applications and characteristics of a nuclear physical security system that will determine the level of encryption needed. A major component of security posture is connectivity to another network or networks. Systems can either be stand-alone or connected. Wireless systems are inherently more vulnerable than wired systems. Therefore, the integration of a wireless with a wired network results in more risk to the merged

network. Given compliance with the requirements in DoDI 3224.03, the merged network can be secured to an acceptable level of managed risk, ultimately evaluated by the system's authorizing official.

(3) (U) Communications Procedures. Enforce communication discipline for all radio and land line transmissions on the security force communications nets. Require security forces to contact a central communications point to verify the security communications networks operability and functional integrity as well as sentry and response force readiness state. Make contacts at the beginning of each shift and periodically throughout the shift, at intervals determined by the security forces commander, but no more than 30 minutes. The 30-minute requirement does not apply during real-world emergency conditions such as weapon recapture or recovery operations.

3.3. FACILITY PROTECTION SYSTEM.

a. (U) General. The components of the facility protection system include the facility barrier subsystems and criteria for support facilities. Whenever designated temporary storage facilities contain nuclear warheads or nuclear components, institute compensatory measures that afford a level of security comparable to permanent structures.

b. (DCNI) Facility Barrier Subsystem. The structural protection design concept specifies structure protection design criteria and equipment requirements for nuclear weapons storage structures and maintenance facilities. Keep doors, windows, and other openings in the structure to the minimum number and size necessary. Design storage structure components, including walls, ceilings, roofs, floors, doors, windows, and other openings (e.g., ducts and conduits) to resist penetration. When combined with other site security measures (e.g., perimeter barrier, delay and denial systems) these measures will prevent unauthorized access to nuclear weapons. Use Military Handbook 1013/1-A to design these facilities.

(1) (DCNI) Storage Structures. Incorporate delay and denial systems into storage structures to contribute to the security system concept of 30 minutes of access delay.

(2) (U) Walls. When combined with all other barriers and security measures, the walls must provide enough delay against bulk explosives; unlimited hand, power, and thermal tools; and forced entry explosive devices, to adequately support the security system concept of 30 minutes of access delay.

(3) (U) Ceilings and Roofs. The penetration resistance of ceilings and roofs should be at least equivalent to the performance requirements for walls. The shielding capacity of ceilings and roofs, when combined with other barriers and security measures, should protect assets from damage by standoff weapons and bulk explosives.

(4) (U) Floors. Floors will be of reinforced concrete construction.

(5) (U) Structure Doors.

(a) (U) Secure doors that are not used for entry from within.

(b) (U) Equip emergency exit doors to alarm when they are opened and install "panic hardware" on the inside. When the facility is unoccupied, secure emergency exit doors with a deadbolt or similar locking device.

(c) (U) Hinges will meet structural, operational, and environmental requirements for their specific application. Hinges must provide forced entry resistance equivalent to the rest of the structure only if the door does not have hinge side protection or inherent design components which provide protection equivalent to the rest of the structure. Hinge side protection is positive interlocking hardware for coupling the hinge side of the door to the door frame.

(d) (U) Equip windows and openings greater than 96 sq inches (619 sq cm) or with a smallest dimension greater than 6.4 inches (16.3 cm) (less entrances) in structures in which nuclear weapons or components are stored or maintained with physical barriers (e.g., bar and grill work) that provide resistance to forced entry and standoff attack equivalent to the surrounding walls. Provide a high-security locking system or high-security deadbolt locking system to movable windows and opening covers.

(6) (U) Structure Locking Systems

(a) (U) Concept. Design locking systems for storage structures as complete systems so that each element is operationally compatible and structurally equivalent to the entire system, offering a uniform degree of resistance to forced entry.

(b) (U) Replacement. Continually evaluate and modernize locking systems in accordance with DoDI 3224.03.

(c) (U) Types of Locking Systems. Use only high security deadbolt locking systems and hasps to protect nuclear weapons in storage and maintenance structures. In permanent storage structures, use an anti-intrusion barrier and external locking systems with two keys or two combinations to support the two-person rule. Padlocks will meet military specification MIL-DTL-43607J, and hasps will meet MIL-DTL-29181C.

(d) (U) Storage Structure Key and Lock Control. Control keys to nuclear weapon storage structures and maintenance facilities as SECRET. Maintain lock serviceability in accordance with Military Department direction.

1. (U) Custodian. Appoint a key and lock custodian to ensure the proper custody and handling of keys and locks used on nuclear weapon storage structures or maintenance facilities.

2. (U) Key Control Register. Maintain a key and lock control register to identify keys for each lock and their current location and custody. Control keys so that no single individual has access to both sets of keys to a storage structure and maintenance facility.

3. (U) Key Audits. Audit keys and locks at least monthly.

4. (U) Key Inventory. Inventory keys with each change of custodian.

5. (U) Key Removal. Do not remove keys to currently installed locks from the site.

6. (U) Key Containers. Protect keys and spare locks in secure containers when not needed for authorized operational purposes. Use containers constructed to withstand forced entry and covert entry against common break-in methods. Keep the containers in a controlled area that limits access to only those necessary as designated in Military Department guidance. Keep "A" and "B" keys in separate containers.

7. (U) Lock Changes. Change or recylinder locks at least annually, and replace or recylinder operable keys that are lost or compromised.

8. (U) Master Keying. **Never** create a master key of nuclear weapons storage structure locks.

9. (U) Key Destruction. Control and accomplish destruction of keys, using two individuals verified by the key and lock custodian, and recorded in the key control register or in a similar manner.

b. (U) Support Facility Criteria.

(1) (U) General Guidance. In facilities normally associated with a nuclear weapon storage site, planners responsible for design or modification of the areas must consider all aspects necessary to optimize security, safety, and efficiency. Construct facilities to be permanently manned by security forces to preclude exposure to adverse weather, including temperature extremes.

(2) (U) SSCC.

(a) (U) Concept. Each nuclear weapons site will have an SSCC. The SSCC will provide overall command and control of the security force. The security vehicle and response force alert facilities may also be located in the SSCC facility.

(b) (U) New Construction. Construct SSCCs to provide protection from small arms, stand-off weapons, and bulk explosives. If located inside a facility that affords this protection, the SSCC requirement is met. Modifications to existing facilities must meet the same criteria. The SSCC will include the capability to employ final denial fire when the facility is in proximity to exclusion areas.

(3) (U) Alarm Monitor Station. Each permanent nuclear weapon site will have an alarm monitor station. The primary alarm display and control console equipment, assessment system monitors, and related controls for all delay and denial, perimeter, facility, and structure detection and visual surveillance equipment will be located within the alarm center. Locate the alarm center within the SSCC.

(4) (DCNI) Response Force and Security Force Facilities. Provide an alert facility or facilities for response force personnel not actively patrolling within the limited area when that is the concept of operation. Build this facility (walls, doors, windows, and exterior barriers) to

protect response force personnel from small arms fire, include the capability to employ final denial fire, and locate centrally within the limited area. Protect security personnel tactically deploying from the alert facility from small arms fire while exiting the facility.

(5) (U) Security Vehicle Protection. Provide facilities for all stand-by security response force alert vehicles. Assure availability of use during emergency situations requiring initial backup force response. Facilities will afford protection from inclement weather, theft, sabotage, and other harassing acts; and obscuration from small arms fire.

(6) (U) Hardened Fighting Position. When a personnel hardened fighting position is determined to be necessary, construct it to protect response force personnel from small arms fire, grenades, and mortar round fragmentation. Protect the position's avenues of entry and exit against small arms fire. Security forces will develop plans to neutralize personnel and vehicle fighting positions should they become occupied by intruders.

(7) (U) Power Sources.

(a) (U) Electrical Power. Primary power sources will be of sufficient capacity to carry the connected load with minimum voltage fluctuation. If the voltage of primary power sources fluctuates beyond tolerable limits for essential equipment, automatic voltage regulators will be installed.

(b) (U) Standby Power. All sites containing nuclear weapons will have a standby emergency power source for all functions affecting security and communications. Standby emergency power sources will incorporate an automatic or remote start capability and will be located within a limited area or an enclave providing the same level of security. Locate remote start control in the SSCC. Sources without uninterruptible power supplies will be capable of assuming the full essential on-site load as soon as possible, but in no case will it exceed 65 seconds.

(c) (U) Battery Power.

1. (U) Provide for automatic switchover of sensor, alarm, delay or denial, and radio communication systems to a dedicated battery power source in case of alternating current (AC) power failure. Provide an audible and visual indication of an AC power failure and subsequent restoration at the sensor data display monitor location. Monitor temperature levels and, if necessary, install climate control equipment.

2. (U) Battery power capacity is designed to be doubly redundant and will be adequate to operate sensor, alarm, delay or denial, and communication components (not including CCTV systems and perimeter lighting) for a period of 4 hours when operating in a reasonable maximum demand situation. When the system is operating on AC power, the batteries will "float" and be maintained at full charge.

3. (U) The battery power supply may be centrally located at one system point, or it may be located in the system as required by component grouping. The batteries and charging systems will be physically located within the protected site and either placed under continual

surveillance or contained in a locked enclosure with an IDS installed to protect against tampering and unauthorized access. Protect batteries and their charging systems from the effects of small arms fire. Perimeter security field distribution boxes housing batteries as a tertiary power supply where the degradation of a field distribution box would only affect individual zones of the security system do not require ballistic protection.

(d) (DCNI) Protection of Power Sources. Protect the standby emergency power source, the central power distribution system (including transformer and junction box), and fuel tanks against small arms fire. Remote junction boxes to individual units or zones of physical security equipment do not require protection against small arms fire. The line distribution grid that transmits the emergency power and the fuel tanks for the standby emergency power source should be underground.

d. (U) Entry Control Facility (ECF). ECFs are designed to assist the security forces in controlling entry to and exit from limited areas. The basic configuration of the entry control facility will include a hardened gatehouse that provides protection for security forces from small arms fire, a personnel entry gate, inspection equipment, and a vehicle entrapment area. The ECF is part of the area boundary subsystem of the perimeter security system. Where an automated entry control system (AECS) is used, the facility will provide sufficient space and utilities to support this equipment. The facility will be lighted to permit personnel and vehicle identification and inspection in any weather condition. The facility will have a minimum field of view of 180 degrees toward the exterior of the site. Existing facilities not meeting the minimum field of view requirements may continue to be used until replacement or modification of the facilities are deemed necessary. A deviation is not required. ECF requirements are:

(1) (U) Provide direct landline communication from the ECF to the SSCC.

(2) (U) Protect entry controllers (ECs) from the elements by equipping ECFs with heating, cooling systems, light, and ventilation.

(3) (U) ECFs will have the ability to protect ECs and assistant ECs from small arms fire when they are performing entry control duties outside the protected gatehouse. Hasty or improvised fighting positions, barriers, body armor, or other locally constructed items may be used for providing protection.

(4) (U) Construct the gatehouse portion of the ECF to protect security force personnel from small arms fire. Modify existing gatehouses to provide this protection. The gatehouse will also serve as a fighting position for security personnel. The structure will include facilities for controlling entry to the limited area and the gatehouse and necessary accommodations for assigned personnel. Equip the structure with a duress alarm system and a communications system. This facility may contain the alarm center, the SSCC, the perimeter visual assessment facility, or the response force alert facility. Temporary gatehouses intended to control entry at temporary restricted areas (e.g., temporary aircraft generation area), if not hardened, will be provided with hardened fighting positions constructed as directed by the applicable Military Department to provide protection from small arms fire while allowing ECs to defend against attack.

(a) (U) Inspection Equipment. Inspect vehicles and personnel (as required by Paragraph 3.5) to preclude introduction of unauthorized personnel and material, explosive devices, contraband, etc. Incorporate undercarriage inspection systems and human and explosive detector capabilities into the entry control function, along with other force protection vehicle inspection capabilities.

(b) (U) Vehicle Barriers. Install vehicle barriers at all vehicle entrapment areas to preclude high speed attack through the entry point. Determine security force overwatch positions and randomly occupy them.

(5) (U) Configure the personnel entry gate or door and entry route to ensure that personnel pass the ECF and enter the area one at a time through remotely operated gates, doors, turnstiles, or portals controlled by the entry controller (EC) or AECS console from within the gatehouse. Construct the facility so that the number of personnel approaching the EC or badge exchange area or automated ECP are under the positive control of the security force at all times.

(6) (U) Construct the vehicle entry area with two gates so that when a vehicle enters, the outer gate is opened while the inner gate remains closed. The outer gate will then be closed behind the vehicle before the inner gate is opened to permit the vehicle to enter. Follow the reverse procedure for vehicles exiting the area. Intercontinental ballistic missile (ICBM) facilities and vehicles that are part of a nuclear weapons movement are exempt from this requirement. Construct or modify both portal gates to incorporate a positive locking feature when closed. Use remotely operated and controlled gates that provide an override capability so these gates can be opened simultaneously to facilitate rapid entry during emergencies.

(7) (U) Where an AECS is used, provide a positive controlled means for dismounted vehicle drivers to directly access the ECP from the vehicle entrapment area. Provide equipment beside the vehicle entry and exit lane to permit mounted drivers to log out from the AECS during exit, while remaining under positive control of the security force. Use the AECS to operate the vehicle gates.

(8) (U) The vehicle entry area must provide resistance against unauthorized vehicle penetration.

e. (DCNI) Security Forces Armory. Store security forces weapons, ammunition, and equipment in a room or facility that meets the requirements identified in DoD 5100.76-M. Establish an alternate arming point that stores enough weapons and ammunition to equip at least one backup force. The alternate facility must be physically separated from the primary armory to be tactically effective.

3.4. (U) ELECTRONIC SECURITY SYSTEMS (ESS).

a. (U) General. Military Departments will develop a pre-planned, phased improvement and replacement program for ESS. ESS supports the security concepts of the area perimeter boundary detection and assessment subsystems and the facility detection and assessment subsystems. The electronic intrusion detection, assessment, and response equipment deployed

for the security and protection of nuclear weapons is divided into four categories according to application. These categories are interior sensor equipment, exterior sensor equipment, alarm display and control console and display equipment, and alarm assessment equipment.

b. (U) Development. Pursue development of new equipment under joint service programs in accordance with Military Detail Specification, MIL-DTL-29181C. Introduce new systems as they become available.

c. (U) IDS Concept. IDSs will:

(1) (U) Increase the detection capability of the security force by alerting security personnel to an approach, intrusion, or attempted intrusion.

(2) (U) Provide in-depth detection capability and assessment capabilities through the use of detection and assessment devices at the area perimeter and intrusion detection devices on storage structures.

(3) (U) Safeguard against human or mechanical failure.

(4) (U) Compensate for elements of physical security that cannot be used because of building layout, safety regulations, operational requirements, costs, or other reasons.

d. (U) Deviations. When deviations are required from these ESS requirements, the appropriate Military Service headquarters must approve other suitable systems. In such cases, document Military Service headquarters approval as a technical deviation

e. (U) System Configuration Criteria. The basic ESS will consist of both interior and exterior sensors integrated via data transmission links into a single alarm display and control console and display subsystem, and a remote alarm display and control console and display. General specifications for joint-Service standardized physical security equipment are contained in the DoD Base Installation Security System specification BIS-SYS-10000A, and the Joint-Service Security Equipment Integration Working Group series specifications.

(1) (DCNI) At an above ground weapon storage area, interior sensors will be at each nuclear storage structure with exterior sensors at the perimeter.

(2) (DCNI) At a land-based missile silo, the interior sensors are positioned at key points throughout the launch facility (LF) access system and interior. The exterior sensors make up the outer zone of coverage on the topside portion of the LF.

(3) (DCNI) For weapons storage and security system (WS3), the vault sensors are the interior sensor zone and the protective aircraft shelter (PAS) sensors are the exterior zone.

f. (U) Interior Sensor Equipment. All permanent structures and facilities that temporarily or permanently house unattended nuclear weapons, nuclear weapon components, or alert nuclear weapon delivery systems will have an approved IDS. The system must be able to detect the physical opening of all entryways into the structure and the specific area within the structure containing the nuclear weapon, as well as intruder movement within the specific area of the

structure containing the nuclear weapon. Additionally, all alarm control units associated with the structure interior IDS will be locked and alarmed with tamper switches or devices that annunciate at the alarm panels. In facilities where the control unit is located other than inside the exclusion area IDS protection zone, implement additional measures and include in the site security plan. All alarms emanating from legacy control units located outside the exclusion area require immediate armed response both to the control unit and the controlled facility.

(1) (U) Sensor Coverage. Total sensor system coverage of the entire interior of some facilities is difficult to achieve, and substantially constructed structures such as hardened storage structures and PAS are adequate to protect against covert penetration of floors, walls, and ceilings. Non sensored areas or dead zones are allowed as long as intruders approaching from walls, floors, or roofs cannot reach the weapon before setting off an alarm.

(2) (U) Point Detection. Movable facility openings (doors, windows, hatches) that exceed 96 sq inches (619 sq cm) with the smallest dimension greater than 6.4 inches (16.3 cm) must have an approved entryway detection sensor installed. This sensor will consist of an approved balanced magnetic switch or other type of sensor capable of detecting intrusions at the opening.

(3) (U) Motion Detection. Provide the interior of each facility with an approved IDS capable of detecting the movement of an intruder through likely avenues of approach. Design the system so that it cannot be compromised before producing an alarm and detecting intruders and generating an alarm before they can reach the weapon This requirement does not apply to ICBM launch facilities.

(4) (U) Stay Behind Threat. Sensor systems are often not positioned to detect an individual staying behind in a facility after it is closed and secured. Owner-users will purge the facility before securing it to mitigate this threat.

g. (U) Exterior Sensor Equipment.

(1) (U) Early detection and near-real-time assessment are essential for a prompt and effective reaction to any attempt to penetrate the perimeter security system. Employ a fully integrated system, including detection, assessment, communications, and display subsystems.

(2) (U) Provide all sites that temporarily or permanently house nuclear weapons with an approved boundary intrusion detection subsystem capable of electronically detecting the surface crossing of humans and vehicles. The system will report valid intrusion attempts and reject false and nuisance alarms, be self-protecting, and be able to initiate a rapid response to a possible security threat. The system will be designed to perform reliably, operate continuously, and complement the capabilities and procedures of the site security force.

(3) (U) Secure the limited area boundary in accordance with the requirements of this Section. The detection capability using a sensor or combination of sensors will be capable of detecting all specified intrusions of that zone. Reasonable intrusion modes include vehicles crossing and humans running, jumping, walking, or crawling through or over the detection zone.

The IDS will be designed to detect and alert the site security force of a site boundary incursion consisting of at least one person on foot or in a vehicle.

(4) (U) Exterior IDS on the boundary of the site will provide two continuous lines of detection using two separate lines of sensors using different detection technologies. For example, a fence mounted sensor that detects bending of light waves transmitted through a cable to detect climbing, cutting, or lifting of the fence fabric, and a buried line sensor that detects changes in an electro-magnetic field caused by attempts to walk, run, crawl, or leap through the sensor field. Waterside detection system requirements are specified in Section 6 of Volume 3 of this manual. ICBM detection system requirements are specified in Section 5 of Volume 3 of this manual.

(5) (U) Place perimeter exterior sensors where they are most effective, depending on assessment subsystem, terrain conditions, and barriers used to delay intruders.

(6) (U) At the primary entry control point, the IDS zone or zones that cross personnel and vehicle entrapment areas may be placed in the access mode during shift changes and other high activity periods, provided the zones are observed by at least one security force member. This also applies at IDS-equipped aircraft shelters when the storage vault is unlocked and an exclusion area EC is assigned to control entry and exit at the PAS. This requirement does not apply to ICBM launch facilities.

h. (U) Transmission Line Security.

(1) (U) Protection Level. Protect control and data transmission media at the same level of sensitivity of the information being protected.

(2) (U) Transmission Links. Control or data transmission media may include hardwired or optical fiber data transmission links (land lines) or radio (wireless) (both omni-directional (broadcast) and directional (microwave and light wave)). If radio waves are used, IDS alarms must not be lost due to radio frequency interference. The use of wireless technologies in the application of security systems is authorized providing the technology meets nuclear certification requirements as necessary and meets and complies with applicable National Security Agency (NSA) certifications and rules in accordance with the NSA memorandum, "Wireless Security Requirements for Nuclear Physical Security Systems."

(3) (U) Line Supervision. Use only Class I or Class II accepted line supervision. When the transmission line leaves the limited area and traverses an uncontrolled area, protect with Class I line supervision. When the transmission line remains within the limited area, Class II line supervision may be used.

(a) (U) Class I. Class I line supervision is achieved through the use of advanced encryption system (AES) or an algorithm based on the cipher feedback or cipher block chaining mode of encryption. Certification by the National Institute for Standards and Technology or another testing laboratory is required. The certificate will be retained by the major command for the duration of the operation of the system. Current systems equipped and deployed with data encryption standard line supervision are still acceptable but will be replaced with AES (or

equivalent) compliant systems as existing systems are replaced. Systems installed after the implementation of this volume will meet the AES Class I standard.

(b) (U) Class II. Class II line supervision are systems in which the transmission is based on pseudorandom generated tones or digital encoding using an interrogation and response scheme throughout the entire communication, or Underwriters Laboratory Class AA line supervision. The signal will not repeat itself within a minimum 6-month period. Class II supervision will be impervious to compromise using resistance, voltage, current, or signal substitution techniques.

(4) (U) Physical Protection of System Cabling.

(a) (U) Internal Cabling. The cabling between the sensors and the controlling unit, termed the detection loop, will be dedicated to IDS, routed in rigid pipe (electrical metallic tubing or polyvinyl chloride) or equivalent raceways, and comply with national electric code standards.

(b) (DCNI) External Cabling. Permanently installed exterior communications cable data links and circuits will be physically protected using conduit, direct burial, or aerial installation methods. IDS cables located outside of sensor protected areas will be routed through metal conduit at a minimum height of 10 feet (3 meters) above the ground or at the normal burial depth for cables. In environmentally challenging installations such as corrosive marine locations, the Military Department may determine the most effective conduit in consultation with installation engineers and install conduit that meets the concept to protect exterior cabling from surreptitious line supervision interception and manipulation. The Military Department will document the determination to use non-metallic cabling and a deviation is not required.

(c) (DCNI) Terminal and Junction Boxes. Permanent junction boxes, field distribution boxes, and cable terminal boxes and cabinets used to terminate, splice, and group interior or exterior IDS sensor input, and that would allow spoofing, bypassing, or other surreptitious defeat of the system, will be locked and alarmed with tamper switches or devices that annunciate at the alarm panels. Junction box hinges should be equivalent in penetration resistance to the lock used to secure the box. If the junction box is within the exclusion area protection zone of the IDS, the box need only be sealed or locked.

(5) (U) Temporary and Re-locatable System Protection. Temporary or re-locatable radio communication data link cables will be protected by a local sensor detection zone or be otherwise physically secured and tamper protected. The security criteria in Paragraph 3.4.h.(3) apply.

(6) (U) Temporary and Re-locatable System Configurations. Temporary or re-locatable radio communication data links will transmit a coded message only to report an alarm, to respond to a self-test command, to send status messages, or to relay control signals.

(7) (U) Radio Communication Equipment. Protect radio communication equipment at the same level as the alarm data communications network.

i. (U) Alarm Display, Control Console, and Display Equipment. An integrated command, control, and display subsystem will be incorporated into the SSCC to provide complete operational control of the site IDS. This subsystem will have the capability to display structure and exterior sensor activations, respond to operator inputs, provide for operator interaction with entry control subsystems, activate response devices (e.g., remote denial devices or security force alerting systems), and support the operation of other security subsystems that may be supplied. Minimum provisions to incorporate are:

(1) (U) Audio and visual indications of alarms, shown on a map depicting the layout of the sensor field in relation to the site configuration, or otherwise graphically displayed.

(2) (U) Audio and visual indications of line or radio data link supervision status, including warning of detected radio channel jamming.

(3) (U) Visual indications of access or secure status for structure and exterior sensor zones.

j. (U) Capability to Initiate a Remote Self-Test of Individual Sensors. Computer-based systems with the inherent capability of constant polling and status display meet the intent of "self-test."

k. (U) Remote Annunciation and Display. Provide a remote, independent alarm display and control console with redundant display when the alarm center and the response force are not located at the same place within the limited area. Remote alarm display and control consoles will include:

(1) (U) The same features as the primary and mirror the primary alarm display and control console functions by displaying alarm indicators, facilities, AECS status, map displays, and other information that shows on the primary alarm display and control console display.

(2) (U) The capability for the remote operator to take operational control of a sensored area from the primary operator. Taking operational control can be accomplished either by operator command, or automatically upon failure of the primary alarm display and control console.

(3) (U) Remote alarm display and control consoles must include an automatic warning device to advise the operator when an alarm is not acknowledged at the primary display or when the primary operator places a structure in access.

(4) (U) Backup battery power supply, independent of primary and standby sources.

(5) (U) The control and display subsystem will accommodate all communications media employed at the site.

(6) (U) The control and display console equipment will be designed to maximize operator efficiency.

l. (U) Computer- Based Alarm Display and Control Console Alarm Event Priority. Computer-based IDS alarm display and control consoles must display alarms in order of priority. The Military Departments will determine the priority of alarms based on the types and locations of the nuclear or nuclear-related material being protected. Establish priority starting from the exclusion area, working outwards.

m. (U) Additional Displays and Monitors. Mobile security forces response elements or fixed security posts may use additional alarm data receivers to enhance alarm response capabilities. These can be portable alarm data receivers such as hand-held monitors. Additional displays and monitors may not be used to perform the functions of primary or remote alarm display and control consoles.

n. (U) Perimeter Boundary Assessment Subsystem.

(1) (U) Provide a means by which the cause of all alarms generated at the perimeter security system can be assessed in near-real-time, visually or remotely through an electro-optical imaging system. Use of electro-optical imaging systems, such as CCTV, low-light-level television, infrared, thermal imagery, and radar, are preferred. Sites with perimeter alarm systems will have assessment coverage for 100 percent of the perimeter boundary. For those sites without electro-optical systems, manned assessment posts are required.

(2) (U) Real-time visual assessment may be enhanced by providing sector indicators either embedded on the camera lens or positioned in the camera field-of-view so that when the camera displays a view at alarm annunciation locations, the operator can determine what sector they are seeing on the monitor. Post sector indicators at or near the area boundary. Sector indicators should be reflective and viewable by responding security forces.

(3) (U) Provide surveillance of the site perimeter beyond the clear zone, as permitted by national law.

(4) (U) Harden manned facilities used for immediate visual assessment against small arms fire. Individual cameras, image sensors, and scanners do not require hardening.

(5) (U) New electro-optical perimeter assessment systems will incorporate video storage capability that provides the operator a playback video scene showing the sensor zone during alarm condition. This capability will display the playback scene either automatically or at the manual request of the operator. The video storage subsystems enhance the security force's ability to assess sensor alarms in situations where imaging systems are limited in the number of alarm zones that can be displayed at any one time. Add video storage subsystems to existing imaging systems.

(6) (U) New electro-optical systems will be capable of displaying an alarm scene based on user priority or by sequence of arrival.

(7) (U) Lighting is a paramount consideration when television-based systems are employed for automatic and remote assessment. When employed, imaging system lighting requirements take precedence over human visual lighting requirements.

(8) (U) Employ "lights out" imaging systems, such as infrared and infrared filtered lighted CCTV systems, when reduced site lighting is necessary, desired, or mandated.

(9) (U) Maintenance priority for lighting and alarm assessment equipment should be commensurate with the resource being protected.

(10) (U) Post sentries at any area assessed by electro-optical system components which have failed or are severely degraded, and cannot otherwise be assessed.

(11) (U) Equip and train security force personnel in the use of standard military night vision equipment and weapon sights for maximum night time effectiveness.

(12) (U) Military Departments will develop procedures to ensure that base perimeter assessment or other force protection functions complement nuclear security related assessment systems.

o. (U) Invalid Alarms. Design and maintain IDS to minimize invalid (false and nuisance) alarms, while assuring a high probability of detection. Implement compensatory measures for IDS not meeting false and nuisance alarm rate standards.

(1) (U) False Alarms. False alarms are those for which no cause can be determined.

(2) (U) Nuisance Alarms. Nuisance alarms are created by an influence the sensor was designed to detect such as an animal or act of nature, but not related to an intrusion. Identify what is causing a nuisance alarm and immediately reset it. If the cause of the alarm cannot be quickly identified and reset it is considered a false alarm.

(3) (U) False and Nuisance Alarm Rates. Interior and exterior false and nuisance alarm rates must be computed separately and are averaged per sensor region or zone. Unacceptable rates will be investigated and repaired as soon as possible. Interior false and nuisance alarms are averaged for 12 months (calendar year). Exterior false and nuisance alarms are averaged for 30 days (month).

(a) (U) Interior IDS. No more than one false alarm and three nuisance alarms per sensor region (zone, sector) a month are acceptable.

(b) (U) Exterior IDS. No more than one false alarm and three nuisance alarms per sensor region (sector, zone) a day are acceptable. Proactive measures such as animal control fences, wind filters, vegetation control, etc., may be required to maintain this standard.

p. (U) Test and Record Requirements.

(1) (U) Newly installed intrusion detection and access control systems will be tested and certified operational before being placed into service. To ensure proper operation, the sensor testing should use reasonable approximations of the types of actions that an intruder could be expected to use. The Military Departments will conduct such testing and certification.

(a) (U) At least semi-annually, each interior sensor will be tested by causing an actual alarm, unless technical specifications require more frequent testing or sensor testing will damage the sensor. Depending on the type of sensor, such alarm activation could include opening doors and windows, deliberate movement within the structure, or vibrating the walls and floors.

(b) (U) Randomly selected sections or zones of the perimeter exterior IDS will be tested by causing an actual alarm and in such a manner that the entire perimeter IDS is tested at least monthly.

(c) (U) At least annually, the tamper detection equipment of sensor equipment enclosures and cabinets located inside the coverage area of a sensor field (perimeter or structure) will be tested, unless technical specifications require more frequent testing.

(d) (U) Tests must be conducted to ensure annunciation and display segments of the system are functioning correctly and that remote area operators, where required, are proficient at taking control of and operating the system.

1. (U) Operators will check annunciation and display equipment at each shift change, or anytime they are relieved, to determine the operational status of the system.

2. (U) Remote circuit continuity will be tested at each shift change, if the alarm display and control console has this capability.

(e) (U) Vulnerability testing identifies and mitigates any system vulnerabilities to ensure the system continues to detect and assess intrusions effectively. IDS will be subjected to various adversarial or feasible "real-world" intrusion scenarios to determine overall system performance, reliability, working status, and availability. The results of these tests give the user a complete assessment of the IDS.

1. (U) Constructing Scenarios. System limitation data will be used to design adversarial testing scenarios and base scenarios on identified threats.

2. (U) Test Requirements. Units must conduct quarterly vulnerability tests. Testing must be planned to ensure that all installed interior and exterior IDS are tested annually. These tests form the basis for reporting security deficiencies to the owning Military Department. A minimum of three intrusion scenarios will be conducted per likely avenue of approach in each sensor sector or zone. Testing will be done via single and multiple intrusions while operating in primary and alternate power during all types of weather and times of day. Test results will be documented and included with the unit's annual vulnerability assessment.

3. (U) Interior IDS and Balanced Magnetic Switch (BMS) Sensors. The testing will consist of attempting to open doors, hatches, windows, etc. equipped with BMS sensors and gain access by spoofing or tampering with the sensor. The BMS must indicate an intrusion before an intruder can open the doors enough to tamper with the alarms or gain access to the structure.

4. (U) Volumetric Sensors. Volumetric sensors detect running, walking, crawling, and overhead intrusion attempts. These sensors will be tested using all intrusion methods and normal movements from very slow to fast. Individuals of varying size and weight will be used to conduct the tests. Individuals testing the system will attempt to discover areas where coverage allows an undetected path to nuclear weapons in order to determine whether the system covers the designated area.

5. (U) Exterior IDS Line of Detection at the Clear Zone. Lines of detection at clear zones detect walking, running, rolling, crawling across, or jumping through the line of detection. The system will be tested using all intrusion methods and normal movements from very slow to fast. Individuals of varying size and weight will be used to conduct the tests. Individuals testing the system will attempt to walk around or zigzag through sensor junctions and areas where sensors overlap to test whether the system covers the designated areas. Individuals will also attempt to jump across the sensor field. For "beam-type" sensors, (e.g., bird's eye and radar beacon) individuals will attempt to walk and crawl through, between, and around beams.

6. (U) Interior IDS Line of Detection at the Fence Line. Lines of detection at fence lines detect cutting, climbing, and lifting of the fence fabric. Conduct scenarios that simulate cutting and aided and unaided climbing. Use individuals of varying size and weight to conduct the tests. Individuals will attempt to climb the fence using aided and unaided scenarios and varying rates of climbing speed. A test for cutting detection may involve weaving 9-gauge wire through fence fabric and cutting the woven wire. Check all areas (high and low) of fences, including corner braces, posts, and supports. Pay particular attention to areas below anti-ram cables, if installed. Test the fabric of the fence by having an individual lean against the fence and push it taut while a second person attempts to cut it. Testers should attempt to remove sensors from the fence fabric by cutting the wire ties that attach the sensor. Perform all tests in a non-destructive manner.

(2) (U) Maintain records at the unit for three years on all alarms (including false and nuisance alarms), malfunctions, and maintenance to allow for evaluation of the system.

q. (U) System Security. Protect the system design architecture as directed in the appropriate classification guide for the resource being protected.

r. (U) Selection and Approval of ESS. Before any ESS is acquired, the responsible Military Department will review the proposed project for conformance with current DoD standards and criteria. As applicable, follow the information assurance and information technology certification and accreditation processes outlined in DoDI 8510.01. Headquarters, U.S. European Command (USEUCOM) will ensure compatibility with NATO standards and criteria.

(1) (U) Make every effort to select DoD standardized equipment that has been developed and certified to meet requirements for optimum performance, minimum false alarm rate, and ease of maintenance. This includes procurement of current state-of-the-art, commercial off-the-shelf items that have been demonstrated by test to meet the minimum performance standards established by the government. Pay particular attention to software and firmware products.

(2) (U) Before certification for use, evaluate software programs for "spoofing" or "ghosting" elements. Military Departments will program for the replacement of ESS before it is 10 years old. Evaluate exterior sensor systems for adequacy every 5 years. DoD and Military Department information assurance certifications programs will be followed during software and firmware evaluations.

3.5. (U) ENTRY AND CIRCULATION CONTROL SYSTEM.

a. (U) Concept. Provide a system for controlling entry, exit, and circulation of authorized personnel and vehicles within limited and exclusion areas. Entry into an exclusion area is a separate process from entry into a limited area unless the limited and exclusion area boundaries are the same. Therefore, provide separate entry and circulation control systems for limited and exclusion areas. For locations where the limited and exclusion area boundary systems are the same, one entry and circulation control system are enough.

b. (U) Entry Control. Control of entry, exit, and internal movement of personnel, material, and vehicles through established limited and exclusion area entry control points and within limited and exclusion areas is required. Keep the number of personnel authorized entry to both limited and exclusion areas to a minimum. Employ automated or manual entry control procedures at both limited area and exclusion area boundaries to ensure identification of all personnel before entry and again upon exit. Both vehicle and pedestrian traffic, including dismounted drivers, will remain under the positive control of the security force during both entry and exit processing.

(1) (U) Exclusion Areas. Only personnel certified through the Nuclear Weapons Personnel Reliability Assurance Program (PRAP) or the host-nation equivalent at WS3 installations will be permitted unescorted entry into exclusion areas or will perform escort duties within exclusion areas. The two-person rule applies whenever such entry affords access to a nuclear weapon. Exclusion areas are described in Paragraphs 3.5.b.(1)(a) through 3.5.b.(1)(f) and may be expanded or reduced to accommodate local or unique operational situations. Both members of a two-person team cannot be host-nation personnel. U.S. custodial personnel will maintain control of nuclear weapons at all times unless otherwise directed.

(a) (U) In weapons storage areas, the exclusion area is the interior of structures and maintenance bays containing nuclear weapons. These exclusion areas may be reduced to a portion of the interior of such structures and maintenance bays when operationally necessary. Such reductions will be of short duration and will not be routinely taken for expediency to circumvent the stringent requirements of exclusion area entry and circulation control.

(b) (U) For land-based strategic missile systems, the exclusion area is the below-ground portions of launch facilities (excluding the launcher support building) that provide access to the warhead or the interior of the payload transporter van when weapons are present. The launch control center is not designated an exclusion area.

(c) (U) For the WS3, the exclusion area is defined as the interior of the weapon vault when in the down and locked position. The interior of the PAS containing an unlocked weapon

vault is defined as an exclusion area. However, if operationally necessary, the exclusion area within a PAS with an unlocked or up positioned weapon vault may be reduced to that area immediately surrounding the vault (size determined by operational and security requirements) or the interior of the weapons maintenance truck.

(d) (U) For sea-launched strategic missile systems, when a mated missile is installed within the missile tube, the exclusion area extends upward from the upper-most surfaces of the missile's equipment section (aft equipment section deck), along the interior of the missile tube, to the interior surface of a closed missile muzzle hatch. When the missile muzzle hatch is open with a mated missile in place, the exclusion area includes the immediate area surrounding the missile muzzle hatch opening and a buffer zone is established immediately adjacent to the expanded exclusion area. Ship submersible ballistic nuclear (SSBN) topside exclusion area requirements are further delineated in Section 6 of Volume 3 of this manual.

(e) (DCNI) For vehicles transporting nuclear weapons, the exclusion area boundary will normally be the physical outer surface of the vehicle while the weapon is in motion, and Military Departments may further define the boundary requirements when the vehicle is stopped.

(f) (U) For aircraft containing a nuclear weapon (prime nuclear airlift force (PNAF), alert aircraft), the exclusion area is that area bounded by the aircraft exterior and, if necessary, the area surrounding the aircraft no closer than 10 feet and no farther than 60 feet from any exterior point of the aircraft. Aircraft located inside an aircraft shelter or hangar may not allow a minimum of 10 feet. In such cases, the Military Department will determine the no-closer-than distance. In such cases, the Military Department will also ensure procedures are established that allow sentries responsible for enforcing the aircraft exclusion area controls to identify and interdict threats within the space constraints imposed by the shelter dimensions.

(2) (U) Limited Areas. Generally, only PRAP-certified (or host-nation equivalent at WS3 installations) personnel will be given unescorted entry into limited areas. Examples of limited areas are described in Paragraphs 3.5.b.(2)(a) through 3.5.b.(2)(f).

(a) (U) The limited area in weapons storage areas is the area between the outer boundary of any exclusion areas and the limited area perimeter fence (above ground storage area) or boundary walls and designated entry portal (underground storage facility).

(b) (U) The limited area in a nuclear regeneration area is the area between the outer boundary of any exclusion areas (individual nuclear-loaded aircraft or aircraft shelters containing nuclear-loaded aircraft) and the limited area perimeter.

(c) (U) The limited area for WS3 vaults is the interior of the vault when it is down and locked. Before unlocking a vault, establish a larger limited area, usually encompassing the interior of the PAS.

(d) (U) The limited area for a PNAF aircraft is the area between the exclusion area perimeter (the interior of the aircraft or the area surrounding the weapons when located outside the aircraft) and the permanent or temporary limited area boundary.

(e) (U) For land-based strategic missile systems, when the launch facility is locked and secured, the limited area boundary and the exclusion area boundary are the same (the below-ground portion of the launch facility that provides access to the missile warhead). Once the launch facility is penetrated or unlocked, the limited area boundary is extended to encompass the launch facility top side fenced in boundary.

(f) (U) For vehicles transporting nuclear weapons, the limited area boundary will normally be the same as the exclusion area boundary while the weapon is in motion, and Military Departments will further define the boundary requirements when the vehicle is stopped.

(g) (U) The U.S. commander responsible for the weapons may permit unescorted entry into limited areas to those personnel not certified in the U.S. PRAP who are in one of the following categories:

1. (U) U.S. military personnel and U.S. DoD civilian employees who have a need to know and at least a CONFIDENTIAL security clearance.

2. (U) Employees of U.S. contractors engaged in a related classified contract, provided such employees have at least a CONFIDENTIAL security clearance.

(3) (U) Limited and Exclusion Area Entry and Circulation Control. All personnel not otherwise specified in Paragraphs 3.5.b.(1) and (2) will be escorted inside limited and exclusion areas. If the entry is to the limited area, the U.S. escort will have unescorted entry authority into the limited area. If the entry is to the exclusion area, the U.S. escort will have unescorted entry authority into the exclusion area. Escorts for exclusion areas must also be certified through the PRAP (or host-nation equivalent at WS3 installations). The U.S. commander responsible for the weapons, as part of the entry authorization process, decides whether or not to arm the escorts based on local propriety, threat, and weapon systems vulnerabilities at the time of the entry.

(a) (U) Do not assign personnel performing escort duties other duties. Persons performing escort duties are not tasked any other functions so they may fully concentrate on the task of properly providing surveillance and control over the persons under escort. Inside an exclusion area where a two-person team is required and the sole responsibility of that two-person team is to be present to meet the two-person rule, one person from the two-person team may act as the escort official if that person has escort authority, the two-person team is familiar enough with the task to be performed to detect an unauthorized act, and the team is performing no other task except providing surveillance and control over the persons under escort. When the responsible commander has determined that arming of escorts is not necessary, DoD contractors who meet all other requirements are allowed to escort. All escorts will be periodically trained and certified capable of escort duties and responsibilities.

(b) (U) At sites located in the United States, DoD civilian personnel with at least a CONFIDENTIAL security clearance may perform escort duties within limited areas.

(4) (U) Escort Ratio. The ratio of personnel to be escorted to the number of escorting personnel will be such that escorting personnel can satisfactorily perform continuous surveillance and control. Since this number is a function of the tasks to be performed and the

physical layout of the area or facility at which the escort is performed, the escort official is responsible for determining and, as necessary, limiting the number of people under escort control. Although the Military Departments may prescribe an upper limit on the number, the escort official is responsible for determining if a lower limit is more appropriate for the task, area, or facility.

(5) (U) Minimum Procedures. At a minimum, the procedures instituted for limited and exclusion areas will include:

(a) (U) Controlled picture badge system and entry control and authorization roster. During aircraft regeneration operations, the entry control and authorization roster may be located at locations where the information is available for reference by entry control personnel.

(b) (U) Visitor escort system.

(c) (U) Duress system.

(d) (U) Inspection (as required by Paragraph 3.5.h. or applicable environment-specific sections of Volume 3 of this manual).

(6) (U) Entry Control Roster. When an exchange badge system is in use and the badge contains sufficient information to assure identification of the bearer, it may be used in lieu of an entry control or authorization roster. When an AECS is employed, the authorized personnel access database and automatic event logging capability of the system may be substituted for the entry control or authorization roster.

(7) (U) Group Entry. Except as a temporary expedient for weapon movements and other special circumstances, entry and exit from a limited or exclusion area will be at a single point and by one person or driver and vehicle at a time. The U.S. commander responsible for the weapons may authorize the security force to enter or exit the limited area as a group provided that individual identification is attested to by the group leader, a roster is provided in advance, and vehicle entry and inspections are conducted as stated in Paragraph 3.5.g..

(8) (U) Emergency Entry. Prescribed entry control procedures may be modified to facilitate realistic, rapid entry or exit into limited or exclusion areas during the response to an actual emergency or related training exercise conducted to demonstrate a team's or force's emergency response capability. In any event, the safety and security of nuclear weapons will not be jeopardized. Other emergency forces may also be allowed rapid entry under the same conditions. Implement measures to compensate for this modification of normal entry procedures. It is not the intent to limit the installation or Strategic Weapons Facility (SWF) commander's ability to command and control nuclear operations. Therefore, during emergencies or time-sensitive, urgent events known by the security force, the installation commander or SWF commander responsible for the weapons may use these procedures to enter limited or exclusion areas if they possess unescorted entry authority, are certified under the PRAP, and are preannounced to the responsible security force. Visitors whose presence is required by an actual emergency only may enter with the commander provided they are part of the preannouncement,

vouched for, and personally escorted by the commander. Include compensatory measures and specific procedures for this modification in Military Department supplements.

(9) (U) Special Circumstances. For weapon movements that do not involve nuclear weapons but pose special security considerations, the SWF commanding officer or wing commander may authorize specific procedures and exemptions for group entry of personnel and vehicle inspections.

(10) (U) Non-Duty Entry Announcements. Security personnel (posted on watch) inside the limited area will be notified whenever personnel enter or exit during non-duty hours.

c. (U) Two-Person Rule. A lone individual will not have access to a nuclear weapon, nuclear weapon system, or critical component. Each organization that has a nuclear mission or function will enforce the two-person rule. The two-person rule requires each organization to ensure that at least two authorized persons who meet the requirements in Paragraph 3.5.c.(1) are present during any operation that requires entry into an exclusion area.

(1) (U) To meet the two-person rule, each member of the team will:

(a) (U) Be certified under the PRAP.

(b) (U) Be familiar with the safety and security requirements of the task to be performed.

(c) (U) Know the task well enough to detect an incorrect act or unauthorized procedure. Team members may have different job specialties or skill levels.

(d) (U) Have successfully completed nuclear surety training. Nuclear surety training must encompass, at a minimum:

1. (U) The importance of and need for a U.S. nuclear capability.

2. (U) Nuclear mishap prevention responsibilities of personnel who work with nuclear weapons and components.

3. (U) Possible adverse impact of a serious nuclear mishap on U.S. nuclear capability.

4. (U) General security requirements.

5. (U) The two-person rule and associated requirements and procedures.

6. (U) PRAP requirements.

7. (U) Mishap and hazard reporting.

8. (U) Additional topics commensurate with the unit's nuclear duties; for example, safe haven procedures, sealing of nuclear components, local situations that increase the

risk of nuclear mishaps, and nuclear weapon system safety rules in accordance with DoDM 3150.02.

(2) (U) Personnel authorized inside an exclusion area will:

(a) (U) Enforce the two-person rule while the task or operation is being performed, and until the team is relieved by authorized personnel, or the nuclear weapon, system, or components are secured.

(b) (U) Take steps to stop an observed incorrect act or unauthorized procedure.

(c) (U) Immediately report violations of these procedures.

(3) (U) The two-person rule has been violated when a lone individual in an exclusion area has had the opportunity to tamper with or damage, in a way that could go undetected, a nuclear weapon, nuclear weapon delivery system, or certified critical component. Inadvertent, momentary breaches of the exclusion area are not considered violations of the two-person rule if the individual did not have the opportunity to perform an incorrect act or unauthorized procedure. Report and investigate two-person rule violations.

(4) (U) Deviations from the two-person rule may be necessary if an emergency presents an immediate threat to the safety of personnel or to the security of nuclear weapons, systems, or components. In these instances, once the immediate threat is eliminated, priority will be given to re-establish the exclusion area and the two-person rule. War plan exercises or scenarios are **not** considered emergencies. For other than emergency situations, deviations from this regulation are allowed only if specified by the nuclear weapon system safety rules in DoDM 3150.02. Report and investigate all violations.

(5) (U) Establish procedures to preclude unauthorized entry into an exclusion area. Normally, the boundaries of the exclusion area are the walls, floors, and ceilings of a structure. The boundary may also be delineated by a permanent or temporary barrier. Do not use signs or devices to identify areas or facilities externally as exclusion areas or as requiring the two-person rule. However, signs reading "Exclusion Area" or "Two-Person Rule in Effect" may be used at internal entry points to these areas.

(6) (U) Additional conditions will also apply:

(a) (U) Contractor personnel may form a two-person team if PRAP requirements have been met.

(b) (U) The two-person rule remains in effect for exclusion areas even when an authorized two person team is not present at the exclusion area. When an authorized two-person team is not present and entry control to the exclusion area is being performed by a sentry physically posted at the exclusion area entry control point, the exclusion area entry control personnel will maintain visual contact with one other person to the extent that they both can detect a lone individual in the unoccupied exclusion area. This requirement can be met by either posting a second individual with the EC or by "pairing" the EC at the exclusion area with an

individual at another area if both individuals are in position to directly observe each other. If an authorized two-person team occupies an exclusion area, this requirement for paired entry controllers does not apply. Exclusion area entry controllers will not be used as the second person to form a two-person team inside the exclusion area.

d. (U) Personnel Entry.

(1) (U) Duress System.

(a) (U) Institute a system by which personnel who are permitted unescorted entry to limited and exclusion areas, and those who control entry into, vouch for, or escort visitors into a limited or exclusion area, can covertly communicate a duress situation to other personnel. Only those personnel with a need to know will have access to duress codes.

(b) (U) Change the duress code as frequently as necessary to assure code integrity.

(c) (U) The duress communication will be oral or electronic, or both. AECS will have the capability to accept and process the covert entry of a duress code by any system user. The system will alert all other on-line operators of the duress condition.

(2) (U) AECS Equipment. Where AECS equipment is used, provide separate exit lanes with the appropriate equipment to control and log exit from the area. Final exit from the limited and exclusion area will be under positive control of the EC.

e. (U) Identification Badges.

(1) (U) Provide controlled picture badges for personnel authorized unescorted entry to limited and exclusion areas. Positive identification will be accomplished. Change the distinctive badge system when any event or circumstance indicates the possibility of compromise of the badge system.

(2) (U) Wear badges in a conspicuous and readily identifiable location on the outer garment at all times while inside the limited and exclusion areas. Remove badges used exclusively for limited area entry or access when outside the limited area. Military Departments will prescribe procedures to ensure positive identification of personnel while in these areas when safety considerations prohibit the wearing of such items.

(3) (U) The badge will have distinctive markings easily recognized by an authorized individual observing the badge.

(4) (U) When an AECS is employed, an electronically generated badge may be used. These badges will incorporate a means of recording information required by the automated equipment. When AECS is in use, badge exchange procedures are not required.

(5) (U) Incorporate measures into badge production that ensure badges cannot be easily counterfeited.

f. (U) Vehicle Entry. All passengers will exit the vehicle and proceed through the ECP as pedestrians prior to the vehicle entering or exiting the limited or exclusion area boundary or ECF entrapment area.

g. (U) Vehicle and Material Handling Equipment Control. Only essential government vehicles or those used for official military duties in lieu of government vehicles will operate in limited and exclusion areas.

(1) (U) Vehicles and material handling equipment remaining in limited or exclusion areas after duty hours will be secured to assure that they are not readily usable by a hostile force. No vehicle or handling equipment will be parked within the inner or outer clear zone of the limited area.

(2) (U) Signs will be displayed, except where host-nation laws are sufficient, requiring removal of ignition keys or immobilization of unattended vehicles and materials and material handling equipment parked within or just outside of limited or exclusion areas so they cannot be readily used by a hostile force.

h. (U) Inspections.

(1) (U) Vehicles. Security personnel will inspect all vehicles entering and leaving a limited area or exclusion area for unauthorized personnel and readily detectable prohibited and contraband items. Each vehicle will be given at least a visual inspection of readily accessible areas (e.g., driver and passenger compartments, cargo carrying area, engine compartment, and undercarriage). Units will leverage existing force protection equipment and procedures and adapt them for use at limited and exclusion area entry points.

(2) (U) Persons and Hand-Carried Items. The organization responsible for the limited and exclusion areas will provide a list and description of prohibited items to the security force. Designated items may be exempted from this inspection. The Military Service designated commander will approve exemptions which will be kept to an absolute minimum commensurate with operational requirements. If a list of approved exemptions is on hand, there is no need to submit a request for deviation.

(a) (U) Upon entering and leaving a limited area:

1. (U) All individuals granted unescorted entry authority and their hand-carried items will be subject to inspection by security personnel for readily detectable prohibited materials and contraband items.

2. (U) All individuals being escorted into the area and their hand-carried items will be inspected by security personnel for readily detectable prohibited materials and contraband items.

(b) (U) Upon entering and leaving an exclusion area:

1. (U) All individuals granted unescorted entry authority and their hand-carried items will be subject to inspection for readily detectable prohibited materials and contraband items.

2. (U) All individuals being escorted into the area and their hand-carried items will be inspected for readily detectable prohibited materials and contraband items.

(3) (U) Automated Inspections. Automated means of inspecting personnel and hand carried items may be used in place of manual procedures.

(4) (U) Security Forces Inspections. At limited areas only, inspections of assigned on-duty security forces may be carried out separately by the officer or noncommissioned officer in charge of the unit.

(5) (U) Nuclear Weapon Movement. Personnel and vehicles directly associated with an ongoing operational or emergency movement of a nuclear weapons are exempt from the inspection requirement upon entering or leaving limited and exclusion areas while delivering, removing, or escorting the nuclear weapon from or to the area.

(a) (U) Such persons and vehicles must have been subjected to an inspection and the vehicles maintained sanitized and controlled before the start of the movement.

(b) (U) This exemption is only applicable while directly carrying or escorting nuclear weapons into or out of a limited or exclusion area. They are not exempt from these inspection requirements upon normally entering the area to prepare for a weapon movement or upon departure from the area at the conclusion of the movement.

(c) (U) During alert force regeneration operations, consecutive weapon movement operations by the same movement escort team (all team members, drivers, and passengers) do not require personnel and vehicle inspections while traveling between limited or exclusion areas in preparation for the next weapon movement, as long as all personnel and vehicles remain under the constant supervision of the weapon movement commander, remain on a secure route, and are preannounced into or out of the area by the weapon movement commander.

(d) (U) Inspection is required upon entry in preparation for the initial movement and upon departure from the area following the last movement.

(6) (U) U.S. Treaty Obligations. Persons entering nuclear weapon limited and exclusion areas under U.S. treaty obligations will be subjected to the provisions of such treaties and, if a condition of the treaty, be exempted from the inspection requirements of this volume and Volume 3 of this manual. U.S. commanders responsible for the weapons should consider and implement mitigation strategies to limit vulnerabilities (if any) to the weapons. Under no circumstances will a U.S. treaty inspector be allowed entry to an exclusion area unless a suitable two-person team is present.

i. (U) AECSs.

(1) (U) General. An AECS may provide an integrated capability for entry and circulation control of all personnel authorized entry into areas containing nuclear weapons, systems, and components. The AECS may remove or lessen the impact of the EC's subjective judgment through automated identification. Military Departments will prescribe which levels of AECS are authorized for specific situations (e.g., entry into the limited and exclusion areas).

(2) (U) System Performance Requirements.

(a) (U) Identification Authentication Process. One of three separate levels of personal identification, as described in Paragraphs 3.5.h.(2)(a)1., 2., and 3. will be used to authenticate an individual's authorization to enter the area. Upon reassignment, transfer, change in status within the PRAP, or termination, or when an individual's access is suspended, revoked, or downgraded to a level lower than required, promptly remove the individual's authorization to enter the area.

1. (U) Level 1: Personal Identification Card or Badge. This level requires an identification card coded for each individual and a card reader. The card or badge will use embedded sensors, integrated circuits, magnetic strips, or other means of encoding data resistant to tampering or modification that identifies the facility and the individual to whom the card is issued.

2. (U) Level 2: Identification Card and Personal Identification Number (PIN). This level requires an identification card and a PIN. The PIN will be separately entered by each individual using a keypad device and will consist of four or more digits, randomly selected with no known or logical association with the individual. The PIN will be changed when it is believed to have been compromised or threatened with compromise.

3. (U) Level 3: Identification Card, PIN, and Personal Identity Verification (PIV). This level requires an identification card, a PIN, and a PIV. PIVs (biometric identifiers) identify an individual by some unique personal characteristic.

(b) (U) Security Considerations. Establish and continuously maintain physical security protection for all devices and equipment that constitute the AECS. The level of protection may vary depending on the type of devices and equipment being protected with the intent of using the security controls already in effect within the facility.

1. (U) Protect locations where authorization data, card encoded data, and personal identification or verification data is entered, stored, processed, or recorded so that the integrity of the entry control system is not compromised.

2. (U) Card readers, keypads, communication, or interface devices located outside the entrance to a limited area (or exclusion area when the limited and exclusion area boundary are the same) will have tamper resistant enclosures, be securely fastened to a wall or other structure, and be protected by a tamper alarm. Control panels located within a limited area require only the minimal degree of physical security protection sufficient to preclude unauthorized access to the mechanism.

3. (U) Design and install keypad devices so that an unauthorized person in the immediate area cannot observe the selection of input numbers. Future AECS installations and modifications or upgrades will use scramble keypad technology.

4. (U) Systems that use transmission lines to carry access authorization, personal identification, or verification data between devices and equipment located outside the limited area will receive a minimum of Class I line supervision.

(3) (U) Interface Requirements. AECS will be integrated into the overall site security operations.

(4) (U) Other Considerations. Other considerations in planning for an AECS include communications and computer requirements (i.e., information assurance), safety, power, survivability, and interface with other planned security systems. The system must address human engineering requirements in a nuclear, chemical, biological environment, and extreme weather conditions or environments, day and night.

SECTION 4: (U) NUCLEAR WEAPON INCIDENTS

4.1. (U) GENERAL.

a. (U) In accordance with DoDI 3150.10, any unexpected event, intentional or accidental, involving a U.S. nuclear weapon will be considered to be the result of hostile acts until proven otherwise.

b. (U) An incident involving nuclear weapons or components necessitates implementation of specific and effective security measures as rapidly as possible. Although security and weapon safety concerns should not preclude or interfere with the performance of basic medical and humanitarian response to accident victims, the need for appropriate security for the weapon and its components and for the public safety is an important aspect of nuclear incident response.

c. (U) Depending on the location and scope of the nuclear weapon incident, a wide range of Federal resources may be activated and deployed. The Department of Energy, Federal Bureau of Investigation (FBI), Department of State, and Department of Homeland Security, as well as host nation authorities in outside the continental United States (OCONUS) events, will be primary partners for DoD in incident response. The DoD Incident Commander must ensure that the appropriate interagency teams are granted access to the incident site. To the maximum extent possible, security requirements should be adhered to; however, technical and investigative personnel will not be denied access to the site.

d. (U) This Section summarizes security requirements and considerations for planning and conducting security operations at the scene of a nuclear weapon incident. Overall DoD procedures for the response to nuclear accidents, including specific implementing security procedures, are contained in DoDI 3150.10 and DoDM 3150.08.

e. (U) *Classified information removed.*

f. (U) Recapture and recovery operations are conducted in accordance with CJCS Instruction 3261.01C and apply to each nuclear weapon storage and operational site, unit, weapon or logistics movement, facility, or military installation.

4.2. (U) SECURITY REQUIREMENTS. The minimum security requirements at the site of a nuclear incident include:

a. (U) Protect nuclear weapons and components.

b. (U) Provide effective security and circulation control of the incident area.

c. (U) Counter potential terrorist and radical group activities or intelligence collection efforts.

d. (U) Protect other classified materials and information.

e. (U) Protect government property.

f. (U) Provide effective coordination with civil law enforcement agencies or host-nation agencies.

g. (U) Provide necessary operations security.

4.3. (U) INCIDENT OUTSIDE A U.S. MILITARY INSTALLATION. Incidents occurring outside a continental United States military installation may require the establishment of a National Defense Area (NDA) (DoD control) or a National Security Area (NSA) (DOE control) to permit control of civilian land by military forces.

a. (U) Even with the establishment of an NDA or NSA, close coordination with civil law enforcement agencies is necessary and essential.

b. (U) NDAs are not used in an overseas environment off of U.S. military installations. The on-scene or initial response force commander will coordinate with civil authorities to establish a security area or disaster cordon to restrict entry and to provide for the public safety.

c. (U) OCONUS incident commanders must establish close coordination with local officials and the Department of State. Authority will be in accordance with bilateral agreements with the host nation in effect at the time; however, the United States will maintain control of the weapons and classified components.

4.4. (U) SECURITY RESOURCES.

a. (U) Initial Response Force (IRF). The security element of the IRF, which should respond from the nearest DoD installation or activity, will take immediate actions to establish an exclusion area and entry control, perimeter security, entry and exit control, and protection of classified material and information. The IRF security forces will likely require augmentation.

b. (U) Response Task Force (RTF). The RTF, a designated force consisting of military, civilian, and possibly DOE or other agency or host-nation personnel, includes a security element. When deployed, the RTF security element will be prepared to meet all security requirements on a continuous 24-hour basis.

c. (U) Civilian Response. Civilian law enforcement response depends on the location of the incident site, but would likely include local police or State police assisted by fire and rescue personnel, any or all of whom may be first on the scene of an incident if it occurs off of a military installation. Commanders are expected to develop strong working relationships with civilian law enforcement and emergency response leadership to facilitate integration. Prepare local integrated response plans and coordinate with civilian agencies for this purpose.

4.5. (U) SPECIAL SECURITY CONSIDERATIONS. During the initial response, emphasis will be on saving lives and mitigating the risk of further casualties. However, certain special security considerations are required because of the presence of nuclear weapons or components. These include:

a. (U) Components of nuclear weapons that may reveal classified information due to their shape or outline; therefore, classified components will be protected from sight and overhead surveillance under the guidance of qualified explosives ordnance disposal personnel.

b. (U) The routine DoD requirement is to neither confirm nor deny the presence or absence of nuclear weapons or nuclear components at any specific location. However, exceptions exist when nuclear incidents occur. Public affairs policy during nuclear incidents is in DoDM 3150.08.

c. (U) The two-person rule will be observed and enforced when control of the weapon has not been lost.

d. (U) During an actual emergency, the incident commander will establish entry control procedures consistent with this volume. PRAP requirements may be waived during the early stages of the response due to an initial lack of PRAP-certified personnel. As they become available, PRAP-certified personnel will be used to control entry to limited and exclusion areas. Waiver of PRAP requirements is not authorized during exercise events.

4.6. (U) RECAPTURE AND RECOVERY REQUIREMENTS.

a. (U) *Classified information removed.*

(1) (U) Recapture. *Classified information removed.*

(2) (U) Recovery. Military forces will be prepared to continue the recovery mission as directed by the Secretary of Defense.

(a) (DCNI) Domestic. Forces assigned to recovery operations will pursue seized nuclear weapons off a military installation when still militarily or visually engaged with the adversaries stealing the weapon, until control is regained or until relieved by the coordinating agency (CA). In domestic situations, the FBI is the CA unless otherwise directed by the President. Under these circumstances, presentation of valid credentials verifies that FBI Special Agents hold a TOP SECRET security clearance and information can be released to them.

(b) (DCNI) Foreign. Recovery operations will be coordinated with the CA in the country or countries involved and conducted in a matter that respects the laws of the host nation and consistent with any applicable bilateral agreements. OCONUS, the Department of State is the CA, with DoD in the lead for tactical operations, unless otherwise directed by the President, in accordance with Presidential Policy Directive-25.

b. (DCNI) The presence of hostages will not deter the taking of decisive action to prevent unauthorized access to or capture or removal of a nuclear weapon. Commanders will take any and all actions, including the use of deadly force, to regain control of the weapons immediately.

4.7. (U) RECAPTURE AND RECOVERY PROCEDURES.

a. (U) Recapture and recovery plans will be built as specified in DoDI 3150.10 and will include specific actions to take, procedures to follow, personnel required, tactics, and weapons to use for all likely potential recapture and recovery situations or scenarios for the site and nuclear weapons concerned.

b. (U) Each installation that stores or routinely supports transit of nuclear weapons will conduct semi-annual recapture and recovery exercises. At a minimum, recapture and recovery exercises will include the participation of all military agencies and forces that would be expected to assist in the recapture and recovery of a weapon in the given scenario of the exercise. Responsible civilian agencies and forces will be invited to participate (e.g., CA, local authorities). One of these exercises may be a table top exercise that stresses planning and communications issues.

c. (DCNI) Make security forces aware of the effect of using their weapons or explosives in the recapture or recovery of the nuclear weapons at their location.

(1) (DCNI) This does not preclude using weapons in the recapture or recovery operation; however, where possible, make available the best weapons for the job, considering any potential danger, to security forces. The possible effects of selected weapons and ammunition are contained in the DTRA Handbook, DTRA-48-M-2H.

(2) (U) *Classified information removed.*

d. (U) *Classified information removed.*

SECTION 5: (U) NUCLEAR WEAPON SECURITY EVALUATIONS

5.1. (U) PROCEDURES. All DoD organizations with a nuclear weapons mission will undergo periodic nuclear weapons performance and security evaluations.

a. (U) The primary performance criterion is if the evaluated unit meets the NWSS. Compliance criteria are designed to ensure DoD nuclear weapons physical security policies are met. Nuclear weapon security evaluations will ensure that:

(1) (U) Nuclear weapons, components, and other critical items are properly secured in accordance with DoD nuclear weapons security directives.

(2) (U) Security for nuclear weapons is commensurate with the DIA and localized TCA scenarios and assessed capabilities, local threat and vulnerability assessments, and intelligence.

(3) (U) Threat, vulnerability, and risk assessments are conducted for locations where nuclear weapons are stored or maintained.

(4) (U) Nuclear weapon security is properly integrated into force protection operations and other security disciplines to produce defense-in-depth security systems.

(5) (U) All personnel involved with the security of nuclear weapons are qualified for their nuclear responsibilities and duties and have the resources to perform the duties.

b. (U) In accordance with DoDD S-5210.81, the CJCS is tasked to establish nuclear weapons technical inspection (NWTI) policy and monitor implementation of the inspection system. Joint Staff policy and procedures are established in CJCS Instruction 3263.05A.

c. (U) The DoD NWTI system, as defined in Joint Publication 1-02, prescribes standard procedures for conducting NWTIs of all nuclear capable units. All DoD Components will establish evaluation programs to ensure:

(1) (U) All subordinate organizations with a nuclear mission are certified as capable of performing their mission.

(2) (U) Operations and procedures are conducted in accordance with applicable DoD, Military Department, and NATO security directives.

(3) (U) Nuclear weapons under their control are maintained in a safe and secure environment.

5.2. (U) PERFORMANCE AND EVALUATION CRITERIA. The ability of a unit to meet the NWSS is the primary and overriding consideration of the security evaluation. Inspection terms will be determined by:

a. (U) Primary Criteria. Ability to meet the NWSS. Evaluations will use "performance-based" events to determine if a unit can meet these standards.

b. (U) Secondary Criteria. Ability to meet the technical requirements mandated in this volume. These "criteria-based" factors will be used with the performance-based factors to determine the effectiveness of a unit's integrated security system and their ability to meet the NWSS.

SECTION 6: (U) SECURITY CRITERIA DEVIATION PROGRAM

6.1. (U) PURPOSE. The standards and requirements in this volume are the absolute minimums required to be implemented. Any circumstances that prohibit full implementation constitutes a deviation from established security criteria. A request to deviate detailing the condition, compensatory measures, and the plan to bring the condition into compliance must be submitted for review and approval. The purposes of the security criteria deviation program are to:

a. (U) Ensure that deviations from established criteria are systematically and uniformly identified and approved by the proper level of command so that informed risk decisions are made.

b. (U) Provide a management tool to monitor corrective actions taken to ensure established security standards are maintained. Generally, deviations require compensatory measures that provide an equivalent level of security.

c. (U) Ensure timely and aggressive actions are taken to correct deviations from security standards and resources are applied, as necessary.

d. (U) Ensure systems are evaluated to determine vulnerabilities and mitigation methods since deviations by themselves may create a security system vulnerability.

6.2. (U) CATEGORIES OF DEVIATIONS. Deviations from established security criteria are categorized as technical, temporary, or permanent deviations, apply to physical security facilities, plans, procedures, equipment, and monitoring standards established in this volume.

a. (U) Technical. A technical deviation is the approved continuation of a non-standard condition that technically varies from established requirements but essentially affords the same level of security.

b. (U) Temporary. A temporary deviation is the approved continuation of a non-standard condition temporarily, which deviates from an established security standard. Temporary deviations require compensatory measures. A temporary deviation will be approved for a period not to exceed 12 months. Extensions are permissible provided the provisions of Paragraph 6.6.a.(3) are met.

c. (U) Permanent. A permanent deviation is the approved continuation of a non-standard condition, which varies from an established security standard and creates a vulnerability and when correction of the non-standard condition is judged to be not feasible or cost effective. Permanent deviations require compensatory measures. All permanent deviations will be reviewed by the approving authority every year.

6.3. (U) DEVIATION APPROVAL.

a. (U) Requests for technical, temporary, and permanent deviations will be initiated by the local commander and evaluated and approved by higher headquarters. Specifically, the approval authority for nuclear weapon security deviations is the Combatant Commander concerned, the component commander, or the chief of the Service component, respectively. The deviation approval authority for all deviations may be delegated to a single official of at least O-9 or equivalent Senior Executive Service (SES) grade on the respective commander's staff. If the approval authority so delegates, the O-9 or SES equivalent exercising delegated approval authority may approve all deviations until the approval authority commander can provide final approval in the annual (March 15) deviation report (Paragraph 5.5).

(1) (U//FOUO) Within 60 days of deviation approval, the deviation approval authority will provide a copy of the deviation for situational awareness to the nuclear enterprise stakeholders (i.e., supported commanders, Combatant Commanders where nuclear forces operate within their areas of responsibility, Military Departments, and Service Component Commanders).

(2) (DCNI) Security deviations from NATO-established criteria will follow USEUCOM-prescribed approval processes. Because U.S. nuclear weapons in Europe assigned to NATO forces remain in U.S. custody and control, there will be a dual track deviation approval process. USEUCOM will establish procedures, in conjunction with their NATO nuclear partners, for timely notification and correction of security deviations. Such deviations will be included in the annual deviation report as outlined in Paragraph 5.5.

(3) (U) When considering a deviation request for a particular site, the approving authority will review all other approved deviations currently in effect for that site. This review is to ensure that the collective deviations do not establish an overall site vulnerability greater than the designated compensatory measures.

(4) (U) Each deviation will be evaluated and approved on a case-by-case basis. Blanket deviations (one deviation covering multiple environments, multiple installations, or multiple deviations within a single environment) are not authorized.

(5) (U) Technical deviation requests are not required for a 10 percent deviation from all measurable standards, such as clear zone distances, fence height, etc.

(6) (U) If circumstances prohibit full implementation of a standard or requirement in this volume and the circumstances will be corrected in 30 calendar days or less from the date of discovery by the Wing, SWF, or SSBN squadron commander, a formal deviation approval need not be requested. Military Departments, in coordination with applicable entities, will establish the review and approval process to be followed for a short-term deviation. These procedures must ensure effective compensatory measures are implemented. Include a summation of any such short-term deviation conditions in the annual deviation report prescribed in Paragraph 5.5.

b. (U) Any Military Department-developed forms used to approve deviations will contain the statement "I have been briefed and accept the risk associated with the foregoing deviation from security policy" in the signature block of the risk acceptance approving official.

c. (U) Any level in the chain of command may disapprove a request for deviation and return the request to the originator. Disapprovals will be based on the adequacy of compensatory measures or the appropriateness of identified corrective measures.

6.4. (U) COMPENSATORY MEASURES.

a. (U) Institute compensatory measures for each temporary and permanent deviation. If appropriate, one compensatory measure may suffice for more than one deviation. Institute compensatory measures whenever two or more technical deviations, taken together, are determined to constitute a vulnerability in the security system. For example, a fence that is a few inches below the required height does not by itself constitute a vulnerability; therefore, no compensatory measures are necessary. However, if there are additional technical deviations at the site (e.g., clear zones and perimeter lighting), which, taken together, are determined to create a vulnerability, then compensatory measures are required.

b. (U) The approving authority will review each deviation to ensure that adequate compensatory measures have been established. The criteria for developing effective compensatory measures involve an assessment of the threat or vulnerability that has resulted from the condition that necessitates a deviation. The compensatory measures will be designed to specifically enhance the security posture in light of the deficient situation. Compensatory measures that consist primarily of instructions to the security force to increase their alertness or frequency of patrols are not acceptable.

6.5. (U) ANNUAL NUCLEAR WEAPON SECURITY DEVIATION REPORT.

a. (U) The nuclear weapon security risk acceptance authority (the Combatant Commander concerned, the commander of the component command, or the chief of the Service component) will annually report all nuclear weapon security deviations, with a remediation plan for extended temporary deviations, through appropriate channels to the respective Military Service Chief or Vice Chief and forwarded to the DASD(NM), through the Director, DTRA. This annual deviation report and the deviation remediation plan may be delegated to a single official of at least O-10 or equivalent SES grade on the respective commander's staff.

b. (U) The annual nuclear weapon security deviation report will be submitted to the Director, DTRA, by March 15 and include all deviations (temporary, permanent, and technical) valid during the reporting period. The data period covered by the report will be January 1 through December 31. The Director, DTRA, will forward a quantitative and qualitative analysis of the deviation reports to the DASD(NM) by April 15.

c. (U) If a temporary deviation is approved and continued for a second year, the risk acceptance authority will include in the annual nuclear weapon security deviation report submission to the DASD(NM), with a courtesy copy to the Director, DTRA, their plan for remedying the deviation (remediation plan). The plan must include a threat and vulnerability

assessment as well as compensatory measures for each of these deviations. Strategies for funding and implementing the solution to the problem must be included. The plan must include consideration and impact of any permanent deviations in effect.

d. (U) A record of technical deviations that do not necessitate compensatory measures will be maintained by the approving authority. This record will fully explain the justification for each deviation and the reasons that compensatory measures are not required.

6.6. (U) RISK MANAGEMENT. Commanders at all levels must ensure risks to nuclear weapons are known and understood and establish procedures to manage such risks.

a. (U) Military Departments and commanders will assess the entire integrated, multi-layered security system protecting nuclear weapons against the adversary capabilities identified in the DIA and local TCA document to identify security system vulnerabilities. Identified vulnerabilities will be prioritized and potential mitigators identified and evaluated for effectiveness in reducing those vulnerabilities.

(1) (U) Risk will be considered when designing and operating nuclear weapon security systems. Risk is calculated by a thorough understanding of adversary capabilities against the existing integrated nuclear security systems (also known as vulnerability), added to the adversary opportunity to exploit that integrated security system and the steps taken to counter those activities. Risk is the gap between what vulnerabilities are mitigated and those that remain. Military Departments will utilize validated risk models for nuclear weapon security system planning and programming activities.

(2) (U) Adversary intent is irrelevant when assessing risk as intent can, and does, change quickly. Security forces will understand and counter adversary capabilities and limit adversary opportunity to eliminate the importance of adversary intent.

(3) (U) The Combatant Commander concerned, the commander of the component command, or the chief of the Service component (U.S. Air Force Major Command Commander or first O-10 in the chain of command) is the risk acceptance authority for nuclear weapons security. DoD Components will annually certify to DASD(NM) that the risk acceptance authority was informed of any identified nuclear weapons security vulnerabilities and the assessed risk. Record this certification and any resulting risk acceptance decisions and risk reduction strategies in the annual nuclear weapon security deviation report.

b. (U) Combatant Commanders will be consulted on all risk management decisions affecting the combat capability of assigned nuclear forces. Include risk reduction strategies in the Combatant Commander's Integrated Priority List.

c. (U) The DASD(NM) will review all technical deviations through the Security Policy Verification Committee and, if warranted, include the condition in this volume as acceptable with its appropriate compensatory measures.

GLOSSARY

G.1. (U) ACRONYMS. (The acronyms in this Glossary are UNCLASSIFIED)

AC	alternating current
AECS	automated entry control system
AES	advanced encryption system
ASD(NCB)	Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs
BMS	balanced magnetic switch
CA	coordinating agency
CCTV	closed circuit television
cm	centimeter
DASD(NM)	Deputy Assistant Secretary of Defense for Nuclear Matters
DIA	Defense Intelligence Agency
DoDD	DoD Directive
DoDI	DoD Instruction
DoDM	DoD Manual
DOE	Department of Energy
DTRA	Defense Threat Reduction Agency
EC	entry controller
ECF	entry control facility
ECP	entry control point
ESS	electronic security system
FBI	Federal Bureau of Investigation
FOUO	for official use only
ICBM	Intercontinental Ballistic Missile
IDS	intrusion detection system
IND	improvised nuclear device
IRF	initial response force
m	meter
mm	millimeter
MWD	military working dog
NATO	North Atlantic Treaty Organization
NC2	nuclear command and control
NDA	National Defense Area
NSA	National Security Area

NSTCA	nuclear security threat capabilities assessment
NWSS	nuclear weapon security standard
NWTI	Nuclear Weapons Technical Inspection
OCONUS	outside the continental United States
PAS	protective aircraft shelter
PIN	personal identification number
PIV	personal identity verification
PNAF	Prime Nuclear Airlift Force
PRAP	Personnel Reliability Assurance Program
RTF	response task force
SES	Senior Executive Service
SNM	special nuclear materials
sq	square
SSBN	Ship Submersible Ballistic Nuclear
SSCC	Site Security Control Center
SWF	Strategic Weapons Facility
TCA	threat capabilities assessment
U//DCNI	DoD Unclassified Controlled Nuclear Information
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USEUCOM	U.S. European Command
VNIR	very near infrared
WS3	Weapon Storage and Security System

G.2. (U) DEFINITIONS. Unless otherwise noted, these terms and their definitions are for the purpose of this issuance. The definitions in this Section are UNCLASSIFIED.

access. Close physical proximity to a nuclear weapon in such a manner as to allow the opportunity to tamper with or damage it.

authorized access. Close physical proximity within the nuclear weapon exclusion area obtained through proper control measures to accomplish specific authorized missions.

unauthorized access. Close physical proximity to a nuclear weapon in such a manner as to allow the opportunity to tamper with or damage it. In the absence of positive control and preventative measures, presence within the exclusion area constitutes unauthorized access.

Possession or use of stand-off weapons or systems from outside the exclusion area does not constitute close physical proximity.

AECS. An automated entry control system where no man-in-the-loop is required to authorize access.

CA. Defined in Joint Publication 1-02.

clear zone. An area within the storage site perimeter and around the boundary of the storage site free of all obstacles, topographical features, and vegetation exceeding a specified height. The clear zone is designed to facilitate detection and observation of an intruder, to deny protection and concealment to an intruder, to maximize effectiveness of security force weapons, and to reduce the possibility of surprise attack.

custody. Defined in Joint Publication 1-02.

deadly force. Force which a reasonable person would consider likely to cause death or serious bodily harm.

defeat. The response by trained and equipped forces to immediately and, if necessary, violently defeat an opposing adversarial force that is attempting to or has gained unauthorized access to nuclear weapons.

delay. The effect achieved by physical features, technical devices, or security measures and forces that impede an adversary from gaining unauthorized access to a nuclear weapon.

denial. The effect achieved by security systems or devices that prevent a potential intruder or adversary from gaining unauthorized access to a nuclear weapon.

detect. The determination that an unauthorized action has occurred or is occurring; detection includes sensing the action, communicating the alarm to a control center, and assessing the alarm. Detection is incomplete without assessment.

deviation. A nonstandard condition that varies from established security criteria, further categorized as either a technical, temporary, or permanent deviation. Deviations do not always equate to system vulnerabilities.

duress (immediate, sufficient). Those actions, proportional to the threat, that disrupt the adversary and delay them from meaningful work in order to prevent theft, damage, sabotage, destruction, or detonation of a nuclear weapon.

duress system. A method by which personnel authorized entry into exclusion areas and those who authorize entry into or escort visitors into limited or exclusion areas can covertly communicate a situation of duress to a security control center or other operating, maintaining, or security personnel who will notify a security control center.

ESS. That part of physical security concerned with the safeguarding of personnel and property by use of electronic systems. These systems include, but are not limited to, intrusion detection systems, automated entry control systems, and video assessment systems.

exclusion area. A designated area immediately surrounding one or more nuclear weapons. Normally, the boundaries of the area are the walls, floors, and ceiling of a structure or are delineated by a permanent or temporary barrier. In the absence of positive preventive measures, access to the exclusion area constitutes unauthorized access to the nuclear weapons.

facility. Defined in Joint Publication 1-02.

false alarm. Activation of an alarm sensor by some influence that cannot be identified as related to an intrusion attempt or nuisance alarm.

final denial fire. The ability of the security forces to place effective fire on the entrances to facilities or platforms containing nuclear weapons. The intent is to deny an adversary unauthorized access.

ghosting. An unauthorized computer program or method which copies or clones a computer hard drive or individual hard drive partitions, with the intent of adding malicious coding or instructions to the cloned version and reinstalling the information back to the same machine from which it was originally copied in order to bypass, gain control of, or otherwise spoof the security system operated by the computer or computer system.

high security hasp. A security hasp meeting the specifications of DoD Base Installation Security Specification BIS-SYS-1OOOOA designed for use with a high security padlock and approved by DoD for the protection of nuclear weapons.

high security pad lock. A security key and lock meeting the specifications of DoDM 5100.76 and approved by DoD for the protection of nuclear weapons.

IDS. That portion of the ESS designed to detect the entry or attempted entry of a persons into the area protected by the system.

immediate. Occurring or accomplishing without loss of time and without any regard to factors that will inhibit full initiation of action.

inspection. At a minimum, a visual inspection of persons, hand carried items, and readily accessible areas of vehicles and equipment. As applied to the inspection of personnel, vehicles and equipment, an inspection is designed to detect unauthorized persons (vehicle and equipment inspections) and readily detectable prohibited and contraband materials (person, vehicle, and equipment inspections).

limited area. A designated area immediately surrounding one or more exclusion areas. Normally, the area is between the boundaries of the exclusion areas and the outer or inner barrier or boundary of the perimeter security system.

line of detection. A line of detection employs a sensor or sensors in combination to detect all reasonable intrusion scenarios, including surreptitious attempts to spoof and tamper with the line of detection. For example, where fence sensors are installed, the line of detection must detect cutting, climbing on, and lifting of the fence fabric.

lumen. A unit of luminous flux equal to the light emitted in a unit solid angle by a uniform point source of one candle intensity.

lux. A unit of illumination equal to the direct illumination on a surface that is everywhere one meter from a uniform point source of one candle intensity or equal to one lumen per square meter.

Military Department. Defined in Joint Publication 1-02.

NC2. The exercise of authority and direction by the President, as Commander in Chief of the U.S. Armed Forces, through established command lines, over nuclear weapon operations of military forces; as Chief Executive over all Government activities that support those operations; and as Head of State over required multinational actions that support those operations.

near real time. That period of time between notification of an event (such as an alarm) and the assessment of the event. The time should be as close to instantaneous as possible.

NSTCA. A DIA-led, intelligence community assessment of the capabilities and intentions of a variety of actors to gain unauthorized physical access to a U.S. nuclear weapon. The NSTCA forms the cornerstone of threat planning for nuclear security systems until updated or superseded.

nuclear regeneration. The return of a nuclear-capable unit or delivery platform to a state or posture of nuclear alert or readiness, or the reestablishment of a previously removed, lost, or destroyed nuclear capability at a specific location by the addition of nuclear weapons, delivery platforms, supporting equipment, or personnel.

nuclear weapon accident. Defined in Joint Publication 1-02.

nuclear weapon incident. A nuclear weapon accident or intentional hostile event involving a nuclear weapon, facility, or component.

nuclear weapon movement. The transport of nuclear weapons by any appropriate noncombat delivery vehicle.

nuisance alarm. Activation of an alarm sensor by some influence for which the sensor was designed to detect, but which is not related to an intrusion attempt.

NWSS. The standard of nuclear weapons security that requires measures be taken to deny unauthorized access to nuclear weapons; prevent loss of control; and prevent, to the maximum extent possible, radiological contamination caused by unauthorized acts. The fundamental tenets of nuclear security are to first deny unauthorized access to nuclear weapons and then, should

unauthorized access be gained, commanders will take any and all actions necessary to immediately regain control of nuclear weapons.

obscuration. To make dim or indistinct and to conceal by or as if by covering.

permanent deviation. The approved continuation of a nonstandard condition that varies from an established security standard and creates a vulnerability for the security system, thereby requiring compensatory measures.

radar beacon. A radar transmitter that upon receiving a radar signal emits a signal which reinforces the normal reflected signal or which introduces a code into the reflected signal especially for identification purposes.

recapture. Actions taken to regain control of a U.S. nuclear weapon within the boundaries of a storage or operational site, weapon movement, facility, or military installation where it has been seized by a hostile force or unauthorized persons.

recovery. Actions taken to locate, if necessary, and to regain control of a U.S. nuclear weapon outside the boundaries of a storage or operational site, weapon movement, facility, or military installation, from where it has been lost, removed, or seized by a hostile force or unauthorized persons.

restricted area. Defined in Joint Publication 1-02.

response force. A sufficient number of security force members (15 or more unless otherwise stated) sufficiently sized, armed and equipped, and designed and organized to maneuver tactically in defense of a nuclear weapons and capable of defeating an adversary force before they can gain unauthorized access to a nuclear weapon. The response force provides initial or follow-up response to those situations that threaten or affect the security of the nuclear weapons concerned. Security force members in fixed guard posts are not part of the response force.

risk. Defined in Joint Publication 1-02.

risk analysis. The assessment of operational and programmatic risk to nuclear weapons. Quantitative risk analysis methods are used to determine programmatic risk, while qualitative risk analysis methods are used to determine operational risk.

risk management. The process of identifying, assessing, and controlling acceptable operational and programmatic risk to nuclear weapons and making decisions and implementing actions that mitigate and balance risk cost with mission benefits.

security forces. Those designated persons whose duties are to protect nuclear weapons.

security system. A system composed of intrusion detection and assessment systems, entry control, physical barriers, fences, storage structures, delay mechanisms, denial devices, security forces, and the support personnel assigned to work in and around nuclear weapons.

site. Any location where nuclear weapons are stored, maintained, or on operational alert.

small arms. Light infantry weapons and ball ammunition smaller than .50-caliber.

spoofing. In the context of electronic security systems and computer security, an attack against the system in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage. In this instance the attack imitates multiple alarm activations to mislead the security force or mask legitimate alarms so the security force is unaware of an alarm occurrence.

standby emergency power source. A separate and distinct source of power, internal to the site and in addition to the site's primary electrical power source, normally an engine generator.

standoff attack. A deliberate and hostile action using long-range weaponry directed against nuclear weapons from outside the protected zone.

technical deviation. The approved continuation of a non-standard condition that technically varies from established requirements but essentially affords the same level of security.

temporary deviation. The approved temporary continuation of a non-standard condition that deviates from an established security standard and creates a vulnerability for the security system and, therefore, requires compensatory measures.

threat and vulnerability assessment. Defined in Joint Publication 1-02.

two person rule. Defined in Joint Publication 1-02.

uniform illumination. The elimination of "hot" (comparatively much brighter) spots or "dark" (minimum allowed illumination) spots that could affect visual detection of an intruder by creating artificial shadows.

vulnerability assessment. Defined in Joint Publication 1-02.

zone or sector. A group of alarm sensors that normally includes multiple sensors or consists of sensor points from a larger area that is divided into smaller subdivisions. The purpose of sensor zones or sectors is to permit selective access to some related groups of sensors while maintaining other groups of sensors in a secure mode and to permit identification of a specific boundary from which an alarm is activated.

(U) REFERENCES

Chairman of the Joint Chiefs of Staff Instruction 3261.01C, "Recapture and Recovery of Nuclear Weapons," January 31, 2014[1]

Chairman of the Joint Chiefs of Staff Instruction 3263.05A, "Nuclear Weapons Technical Inspections," August 9, 2013[2]

Defense Intelligence Agency, "Nuclear Security Threat Capabilities Assessment, 2011-2021," December 2011[3]

Defense Threat Reduction Agency-48-M-2H, "Emergency Response Forces Handbook," October 22, 2002[4]

DoD Base Installation Security System Specification BIS-SYS-1OOOOA[5]

DoD Directive 5134.08, "Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs (ASD(NCB))," January 14, 2009, as amended

DoD Directive O-5210.41, "Security Policy for Protecting Nuclear Weapons," January 22, 2015

DoD Directive S-5210.81, "United States Nuclear Weapons Command and Control, Safety and Security (U)," August 8, 2005

DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992

DoD Instruction 2000.16, "DoD Antiterrorism (AT) Standards," October 2, 2006, as amended

DoD Instruction 3150.10, "DoD Response to U.S. Nuclear Weapon Incidents," July 2, 2010

DoD Instruction 3224.03, "Physical Security Equipment (PSE) Research, Development, Test, and Evaluation (RDT&E)," October 1, 2007

DoD Instruction O-5210.63 "DoD Procedures for Security of Nuclear Reactors and Special Nuclear Materials (SNM)," November 21, 2006

DoD Instruction 5210.83, "DoD Unclassified Controlled Nuclear Information (UCNI)," July 12, 2012

DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014

DoD Manual 3150.02, "DoD Weapon System Safety Program," January 31, 2014, as amended

DoD Manual 3150.08, "Nuclear Weapon Accident Response Procedures (NARP)," August 22, 2013

---

[1] This document is classified. Direct questions to Joint Staff.
[2] This document is classified. Direct questions to Defense Technical Information Center, 8725 John J. Kingman Road, Ft. Belvoir, Virginia, 22060-6218
[3] This document is classified and has limited distribution. Direct questions to DIA.
[4] This is a limited distribution document. Request from DTRA J3/7, 8725 John J. Kingman Road, Ft Belvoir, Virginia, 22060
[5] This is a limited distribution document. Direct questions to 642 ELSS/FPT, 45 Arnold Street, Bldg 1600, Hanscom AFB, Massachusetts 01731.

DoD Manual 5100.76, "Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives," April 17, 2012

DoD Manual S-5210.92, "Physical Security Requirements for Nuclear Command and Control (NC2) Facilities," August 26, 2010

DoD Manual 8910.01, Volume 1, "DoD Information Collections Manual: Procedures for DoD Internal Information Collections," June 30, 2014

Department of Defense /Department of Energy Classification Guide-W-5, "Joint DOE/DoD Nuclear Weapon Classification Policy Guide," May 2004, as revised[6]

Federal Specification FF-S-2738A, "Seals, Antipilferage," March 30, 1999

Federal Specification FF-P-2827A, "Padlock, Key Operated, General Field Service," November 22, 2002

Federal Specification RR-F-19lK/GEN, "Fencing, Wire and Post Metal (And Gates, Chain-Link Fence Fabric, and Accessories) (General Specification)," May 14, 1990

Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," current edition

Joint Service Security Equipment Integration Working Group (SEIWG) series Specifications[7]

Military Detail Specification MIL-DTL-29181C, "HASP, High Security, Shrouded, for High and Medium Security Padlocks," March 10, 1998

Military Detail Specification MIL-DTL-43607J, "Padlock, Key Operated, High Security, Shrouded Shackles," July 29, 2010

Military-Handbook 1013/1-A, "Design Guidelines for Physical Security of Facilities," December 15, 1993[8]

National Security Agency Memorandum, "Wireless Security Requirements for Nuclear Physical Security Systems," May 3, 2011[9]

Presidential Policy Directive-25, "Guidelines for United States Government Interagency Response to Terrorist Threats or Incidents within the United States," January 17, 2014[10]

---

[6] This document is classified. DoD personnel, direct questions to Defense Technical Information Center, 8725 John J. Kingman Road, Ft. Belvoir, Virginia, 22060-6218.

[7] This is a limited distribution document. Direct questions to DASD(NM), 3050 Defense Pentagon, Room 3B884, Washington, DC 20301

[8] Document may be obtained from the Defense Technical Information Center, 8725 John J. Kingman Road, Ft. Belvoir, Virginia, 22060-6218.

[9] This is a limited distribution document. Direct questions to DASD(NM), 3050 Defense Pentagon, Room 3B884, Washington, DC 20301

[10] This document is classified. The Office of the Under Secretary of Defense for Policy is the DoD release authority for this document. All requests for copies will be made through the OUSD(AT&L) to the National Security Council staff.