Department of Defense
DIRECTIVE

April 6, 1990
NUMBER 5210.63

USD(P)

SUBJECT: Security of Nuclear Reactors and Special Nuclear Materials

References: (a) DoD Directive 5210.63, subject as above, April 24, 1978 (hereby canceled)
(b) DoD Directive 5210.41, "Security Policy for Protecting Nuclear Weapons," September 23, 1988
(c) Title 10, Code of Federal Regulations, Part 73
(d) Department of Energy (DoE) Order 5632.2A "Physical Protection of Special Nuclear Material and Vital Equipment," February 9, 1988
(e) through (q), see enclosure 1

A. REISSUANCE AND PURPOSE

This Directive reissues reference (a) to update policy, responsibilities, procedures, and minimum standards for safeguarding DoD nuclear reactors and special nuclear materials (SNM).

B. APPLICABILITY AND SCOPE

This Directive:

1. Applies to the Office of the Secretary of Defense (OSD); the Military Departments; the Chairman, Joint Chiefs of Staff and Joint Staff; the Unified and Specified Commands; the Defense Agencies having responsibility for the protection of nuclear reactors and SNM; and the DoD Field Activities (hereafter referred to collectively as "DoD Components").

2. Applies to all land-based nuclear reactors at fixed sites or in transit, research and test reactors under the direct control of DoD Components, and space-borne nuclear reactors located on DoD installations.

3. Applies to all SNM, regardless of form or whether incorporated in reactor cores or in other items under the direct control of DoD Components, except:

a. Self-protecting SNM; that is, SNM that are not readily separable from other radioactive material and that have a total external radiation dose rate in excess of 100 rems per hour at a distance of 3 feet from any accessible surface without intervening shielding. SNM in a single unit that weighs in excess of 5,000 pounds may have reduced security measures upon approval of the cognizant agency.

b. SNM in a quantity not exceeding 350 grams of uranium-235, plutonium, or combination possessed in any analytical, research, quality control, metallurgical, or electronic laboratory.

4. Does not apply to nuclear weapons. Because of the unique requirements associated with nuclear weapons, separate guidance regarding their security is provided in DoD Directive 5210.41 (reference (b)).

5. Does not apply to nuclear reactors or SNM on board U.S. Navy ships. (See paragraph E.4.c., below.)

6. Does not apply to those nonactive or decommissioned DoD nuclear reactor facilities or nuclear propulsion systems on Navy ships when no fissile material is present.

7. Does not abrogate or abridge the:

a. Authority or responsibility of a commander to provide equivalent or better standards than those applied to licensed facilities or materials or to apply more stringent security standards required by other DoD Directives during emergencies, or at any time the threat to DoD nuclear reactors or SNM indicates additional protection measures are necessary.

b. Responsibility of DoD Components operating nuclear reactors under Nuclear Regulatory Commission license or processing SNM to comply with the requirements of 10 CFR 73 (reference (c)), and DoE Orders 5632.2A and 5632.1A (references (d) and (e)).

C. DEFINITIONS

Terms used in this Directive are defined in enclosure 2.

D. POLICY

It is DoD policy to ensure that nuclear reactors and SNM receive special protection because of their operational importance and the serious consequences of unauthorized possession or use of nuclear materials. The conservation of SNM; the safety of the public, operating personnel, and property; and the protection of SNM from sabotage, theft, loss, or diversion are of paramount importance during all phases of operations.

E. RESPONSIBILITIES

1. The Under Secretary of Defense (Policy) (USD(P)), in coordination with the Assistant to the Secretary of Defense for Atomic Energy (ATSD(AE)), has the authority and responsibility for DoD security policy for DoD nuclear reactors and SNM.

2. The Assistant to the Secretary of Defense (Atomic Energy) (ATSD(AE)) has the authority and responsibility for standards and guidance on defense nuclear energy matters.

3. The DoD Physical Security Review Board, as established by DoD Directive 5100.76 (reference (f)), shall advise and assist the Deputy Under Secretary of Defense (Security Policy) (DUSD(SP)) and ATSD(AE) on matters involving the security of nuclear reactors and SNM.

4. The Heads of DoD Components shall:

a. Effect necessary programming, budgeting, and accounting actions to ensure fulfillment of nuclear reactor and SNM security requirements.

b. Develop site-specific security instructions, procedures, and plans, applicable to nuclear reactors and SNM facilities in accordance with this Directive.

c. Provide a security operational concept for each new type of plant or new class of ship possessing a nuclear propulsion system for coordination with the DUSD(SP) and ATSD(AE).

F. PROCEDURES

1. General

a. Each DoD Component shall develop procedures to ensure adequate protection is afforded nuclear reactors and SNM and to comply with statutory accountability requirements. Procedures shall provide protection against theft, sabotage, diversion, and other hostile acts that could impact adversely on national security and on the health and safety of operating and security personnel and the public.

b. The level and strategy of protection shall be consistent with the category of SNM involved, the standards described in enclosures 3 and 4, radiation levels, the applicable threat, operational requirements, and potential risks. Physical security procedures must constitute a balanced, in-depth system that is responsive to all credible potential vulnerabilities.

c. Nuclear reactors and components without SNM shall be protected consistent with the highest level of classified information they contain.

d. Security-related equipment shall be protected from unauthorized access consistent with its importance to the protection of nuclear reactors and SNM.

e. Unclassified information pertaining to security plans, procedures, and equipment for the physical protection of nuclear reactors and SNM shall be safeguarded as described in the DUSD(SP) Memorandum (reference (g)).

f. General access to nuclear reactors and SNM shall be restricted to authorized personnel with established need. Access shall be kept to a minimum and appropriate entry control and identification procedures shall be established to ensure need for access.

g. Any operator or security individual in a position that would allow the individual, acting alone, the opportunity to divert or cancel the diversion of Category I or Category II quantities of SNM shall be subject to extensive screening and continuing evaluation by supervisors and co-workers in accordance with DoD Directive 5210.42 (reference (h)).

2. Physical Security and Vulnerability Assessment

a. A physical security and vulnerability assessment shall be prepared for existing facilities where Category I or II SNM is used or stored, and during the planning, design, and full-scale development phases of such proposed facilities.

b. The Military Services, through their intelligence and law enforcement services, shall develop and coordinate with appropriate commanders a postulated threat as the basis of the assessment. A design basis for the postulated threat is contained in Section 73.1 of 10 CFR 73 (reference (c)).

c. The assessment shall ensure that all credible potential vulnerabilities are addressed and that appropriate consideration has been given to changing requirements and new technologies.

d. Additional guidance may be found in MIL-STD-1785 (reference (i)) and MIL-HDBK-1013/1 (reference (j)), or other sources with similar depth and coverage.

e. The assessment shall be reviewed at least annually and updated as required.

f. Factors to be considered in assessing security requirements for nuclear reactors include:

(1) Location of the reactor.

(2) Configuration in which the reactor is maintained.

(3) Category of SNM contained in the reactor.

(4) Nature and capabilities of potential threats.

(5) Availability and protection of other equally attractive targets at other facilities.

(6) Reliability and qualification of security and operating personnel.

g. Factors to be considered in assessing security requirements for SNM include:

(1) Degree of enrichment, activity level, and category of the SNM.

(2) Quantity and configuration of the SNM.

(3) Availability and protection of equally attractive material at other facilities.

(4) Difficulties associated with removal of the SNM from the site.

3. Physical Security Plan

a. Upon completion of the physical security and vulnerability assessment, a site security plan shall be developed and implemented that prescribes

the minimum standards and procedures and that complies with 10 CFR 73 (reference (c)) and this Directive. The plan shall consider:

(1) Minimum physical security criteria and standards for protecting nuclear reactors and SNM prescribed in enclosures 3 and 4.

(2) Emergency and contingency procedures as well as protection strategies and measures to prevent radiological sabotage and the theft or diversion of SNM.

(3) Requirements for security equipment unique to security or for monitoring nuclear reactors and SNM described in DoD Directive 3224.3 (reference (k)).

b. Security plans shall be reviewed at least annually in conjunction with review of the vulnerability assessment, current intelligence, and other relevant factors, and shall be updated as required or when facilities are modified. In addition, security programs shall be reviewed as necessary to ensure adequate protection at all times.

4. Use of Force

a. In accordance with DoD Directive 5210.56 (reference (l)), Categories I and II quantities of SNM are designated as vital to the national security whose loss, damage, or compromise would seriously prejudice national security or jeopardize the fulfillment of an essential national defense mission. Security force personnel shall be armed and all possible actions shall be taken, including the use of deadly force within the limitations of reference (l), to prevent the theft, sabotage, or unauthorized control of SNM from a site or shipment where Category I and II quantities of SNM are known or reasonably believed to be present.

b. All security force personnel shall be trained on the use of deadly force. Training shall include specific scenarios, tailored to individual locations, that require security force members to detail their responses to representative situations involving the use of deadly force as outlined in reference (l).

5. Reporting Incidents

All incidents and threats related to radiological sabotage, theft or diversion of SNM, or to damage to nuclear reactors shall be reported in accordance with DoD Instruction 0-7730.12 (reference (m)). A copy of the report shall be provided to the DUSD(SP) and the ATSD(AE).

6. Inventory Discrepancies

When an assessment of SNM status reveals an inventory discrepancy, statutory reporting requirements must be followed and the DUSD(SP) and ATSD(AE) shall be informed of such discrepancies.

7. Variances and Waivers

When it is neither practical nor cost-effective to meet a specific physical security standard, variances or waivers may be reviewed and approved as described in enclosure 5.

8. Public Release of Information

Public release of information regarding incidents and threats related to radiological sabotage and the theft or diversion of SNM shall be governed by DoD Directive 5230.16 (reference (n)) and DoD Instruction 5210.67 (reference (o)).

G. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective immediately. Forward two copies of the implementing documents to the Deputy Under Secretary of Defense (Security Policy) within 120 days; forward one copy of changes to implementing documents within 60 days of publication.

Donald J. Atwood
Deputy Secretary of Defense

Enclosures - 5
1. References
2. Definitions
3. Special Nuclear Material (SNM) Protection Standards
4. Physical Security Standards for DoD Nuclear Reactors and Category I and II Quantities of Special Nuclear Material
5. Variances, Waivers, and Exceptions

REFERENCES, continued

(e) Department of Energy (DoE) Order 5632.1A, "Protection Program Operations," February 9, 1988
(f) DoD Directive 5100.76, "Physical Security Review Board," February 10, 1981
(g) Deputy Under Secretary of Defense (Security Policy) Memorandum, "Interim Guidance for Identifying and Controlling Unclassified Controlled Nuclear Information (UCNI)," September 13, 1989
(h) DoD Directive 5210.42, "Nuclear Weapon Personnel Reliability Program," December 6, 1985
(i) MIL-STD-1785, "System Security Engineering Program Management Requirements," January 31, 1988
(j) MIL-HDBK-1013/1, "Design Guidelines for Physical Security of Fixed Land-Based Facilities," March 1983
(k) DoD Directive 3224.3, "Physical Security Equipment (PSE) Assignment of Responsibility for Research, Development, Testing, Evaluation, Production, Procurement, Deployment, and Support," February 17, 1989
(l) DoD Directive 5210.56, "Use of Force by Personnel Engaged in Law Enforcement and Security Duties," May 10, 1969
(m) DoD Instruction 0-7730.12, "Notification Procedures for Accidents and Significant Incidents Involving Nuclear Weapons, Reactors, and Radioactive Materials," August 1, 1976
(n) DoD Directive 5230.16, "Nuclear Accident and Incident Public Affairs Guidance," February 7, 1983
(o) DoD Instruction 5210.67, "Special Nuclear Material Information, Security Classification Guidance," December 3, 1982
(p) DoD C-5210.41-M, "Nuclear Weapon Security Manual (U)," September 1987, authorized by DoD Directive 5210.41, September 23, 1988
(q) JCS Pub. 1-02, "DoD Dictionary of Military and Associated Terms," June 1, 1987

DEFINITIONS

1. Access. Close physical proximity to nuclear reactors and/or SNM in such a manner as to allow the opportunity to tamper with, steal, or damage such items. Normally, a person is considered not to have access if an escort or guard is provided when the person is in close proximity to the reactor or SNM (DoD C-5210.41-M (reference (p))).

2. Clear Zone. (Also referred to as an isolation zone.) An area adjacent to a physical barrier, clear of all objects that could conceal or shield an individual (10 CFR 73 (reference (c))).

3. Delay. The effect achieved by physical features, technical devices, or security measures and forces that impedes an adversary from gaining access to a nuclear weapon. Normally expressed as a function of time, it is a major consideration in the design and development of nuclear weapon security systems (DoD Directive 5210.41 (reference (b))).

4. Duress System. A system that can covertly communicate a situation of duress to a security control center or to other personnel who can notify a security control center (DoE Order 5632.1A (reference (e))).

5. Exclusion Area. A designated area immediately surrounding the nuclear reactor and/or the SNM. Normally, the boundaries of an Exclusion Area are the walls, floor, and ceiling of a structure or are delineated by a permanent or temporary barrier. In the absence of positive preventive measures, unescorted entry to the Exclusion Area constitutes access to the nuclear reactor and/or the SNM vault or storage container (DoD Directive 5210.41 (reference(b))).

6. Limited Area. A designated area immediately surrounding one or more Exclusion Areas. Normally, the area is between the boundaries of the Exclusion Area and the outer or inner barrier or boundary of the perimeter security system (reference (b)).

7. Material Access Area. An area containing Category I quantities of SNM specifically defined by physical barriers, located within a protected area, and subject to specific access controls (reference (e)).

8. Material Surveillance Procedures. Procedures to ensure the observation of an area containing SNM by at least two cleared and knowledgeable authorized persons who may be doing other work but who can give an alarm in time to prevent unauthorized removal or diversion of the SNM or an act of sabotage involving SNM (reference (e)).

9. Nuclear Reactor. A facility in which fissile material is used in a self-supporting chain reaction (nuclear fission) to produce heat and/or radiation for both practical application and research development (JCS Pub. 1-02 (reference (q))).

10. Postulated Threat. An estimate of potential adversary types, acts, capabilities, and combinations thereof that could constitute a risk to a facility or asset. A postulated threat is necessary when a specific threat cannot be determined or when an existing threat may change or grow during the projected life cycle of an asset or system faster than security improvements can be

developed and implemented. The postulated threat allows for the consideration of future growth in adversary capabilities and is used as the basis for the design of security systems, equipment, and facilities (DoD Directive 5210.41 (reference (b))).

11. Protected Area. An area encompassed by physical barriers and to which access is controlled (10 CFR 73, reference (c)).

12. Radiological Sabotage. Any deliberate act directed against a nuclear reactor, SNM facility, or transport that could directly or indirectly endanger public health and safety by exposure to radiation (reference (c)).

13. Safe. A burglar-resistant cabinet or chest having a body of steel at least 1/2-inch thick and a built-in, three position, changeable combination lock in a steel door at least 1-inch thick, exclusive of bolt work and locking devices (DoE Order 5632.1A (reference (e))).

14. Security Container. A security cabinet that bears a test certification label on the inside of the locking drawer or door and is marked "General Services Administration-Approved Security Container" on the outside of the top drawer or door (reference (e)).

15. Special Nuclear Materials (SNM). Plutonium, uranium-233, uranium enriched in the isotope-233 or in the isotope-235, and any other material that is determined to be special nuclear material, except source material, or any material artificially enriched by any of the foregoing (reference (c)).

16. Special Nuclear Material Vault. A penetration-resistant, windowless enclosure that has: (a) walls, floor, and ceiling substantially constructed of materials that afford forced penetration resistance at least equivalent to that of 8-inch thick reinforced concrete; (b) any openings greater than 96 square inches in area and over 6 inches in the smallest dimension protected by imbedded steel bars at least 5/8 inches in diameter on 6-inch centers both horizontally and vertically; (c) a built-in combination lock in a steel door that in existing structures is at least 1-inch thick exclusive of bolt work and locking devices and that for new structures meets the Class 5 standards set forth in Federal Specification AA-D-6008 of the Federal Specifications and Standards cited in Title 41 CFR Part 101. (See reference (e).)

17. Vault. A burglar-resistant, windowless enclosure that meets the definition of an SNM vault. Additionally, vaults shall include an intrusion alarm activated by an opening of the door (reference (e)).

18. Vault-Type Room. A room having a combination-lock on its door or doors protected by an intrusion detection system activated by penetration of walls, floors, ceilings, openings, or motion within the room (reference (e)).

19. Vital Area. A security area located within a Protected Area for the protection of vital equipment (reference (e)).

20. Vital Equipment. Equipment, systems, or components whose failure or destruction would cause unacceptable interruption to a national security program or an unacceptable impact to the health and safety of the public (DoE Order 5632.1A (reference (e))).

21. Waste. SNM that are no longer useful, economical, or feasible to recover, including that which has become radioactive to the extent that material itself exhibits radioactivity of such a level that it must be handled and disposed of by special methods to protect the general public (reference (e)).

SPECIAL NUCLEAR MATERIAL (SNM) PROTECTION STANDARDS

A. GENERAL

1. The level of protection afforded nuclear reactors and SNM shall be consistent with the category of SNM involved, including radiation levels, regardless of form or whether incorporated in other items, reactor cores or facilities under the direct control of DoD Components. Figure 3-1 identifies the categories of SNM.

2. Additional protective measures may be required than those indicated in this enclosure in those cases where SNM quantities from lesser protected multiple locations within a facility or Protected Area have the potential for being rolled up by an adversary into a higher category of SNM.

B. MINIMUM PROTECTION STANDARDS AT FIXED SITES

1. Category I quantities of SNM

a. Category I quantities of SNM shall be used, processed, or stored only within a Material Access Area enclosed within a Protected Area.

b. Category I quantities of SNM shall be stored in vaults or vault-type rooms equipped with intrusion detection systems (IDS).

c. Category I quantities of SNM in use or process shall be under material surveillance procedures or in process under alarm protection.

d. Category I quantities of SNM shall be protected by a security force capable of responding to a security alarm and neutralizing adversaries in less time than adversaries require to complete their objective. Response times shall be specified in the site security plan.

e. Category I quantities of SNM shall be controlled at all times to prevent theft or diversion by a single authorized individual. Control may be achieved by material surveillance procedures.

f. Access controls, intrusion detection systems, communications equipment, and testing and maintenance programs shall meet the applicable requirements of enclosure 4.

2. Category II quantities of SNM

a. Category II quantities of SNM shall be used, processed, or stored within a Protected Area.

b. Category II quantities of SNM shall be stored in vaults, vault-type rooms, or security containers protected by IDS.

c. Category II quantities of SNM in use or process shall be under material surveillance procedures or in process under alarm protection.

d. Category II quantities of SNM shall be protected by a security force capable of responding to an alarm. Response times shall be specified in the site security plan.

e Access controls, intrusion detection systems, communications equipment, and testing and maintenance programs shall meet the applicable requirements of enclosure 4.

3. Category III quantities of SNM

a. Category III quantities of SNM shall be used, processed, and stored in a Protected Area or other security area that meets the following requirements:

(1) Clearly defined perimeter barriers.

(2) Personnel and vehicle access control at the entrance, administered by a security guard, receptionist, or other person assigned for that purpose.

(3) A personnel identification system.

(4) Establishment and maintenance of a visitor's log.

(5) Signs prohibiting trespassing posted around the perimeter at all entrances to the use or storage area, prohibiting the introduction of prohibited articles, and authorizing inspections and/or searches of vehicles, packages, or persons entering or exiting posted at all entrances to the use or storage areas.

b. Search procedures shall be established and documented in the site security plan.

c. When unattended, Category III quantities of SNM shall be stored in either a locked security container protected by IDS or within a locked room protected by IDS (or in a locked room without IDS patrolled by security forces at intervals not to exceed 2 hours). As an alternative, the security container containing Category III SNM may be stored in a vault or vault-type room containing Category I or II SNM.

d. Access to the material shall be limited to properly cleared personnel in positions that have been specifically designated as requiring access to Category III quantities of SNM in the course of assigned duties and to authorized visitors who are under continuous escort of personnel in such designated positions.

e. A security response force shall respond to verified intrusion alarms as specified in the site security plan.

4. Category IV quantities of SNM

Category IV quantities of SNM shall be used, processed, or stored in accordance with DoD Component guidance.

C. TRANSPORTATION OF SNM

1. Domestic shipments of SNM shall be in accordance with DoE and DoD agreement and consistent with Federal regulations and DoE Order 5632.2A (reference (d)). SNM transport, security, control, and accountability procedures shall be specified in the site security plan.

2. Nuclear reactor cores shall be transported and secured in accordance with DoE and DoD agreements and shall be specified in the site security plan.

3. Movement of SNM within a Protected Area shall be protected as described in the site security plan.

4. Movement of SNM between Protected or Staging areas at the same site.

a. Category I quantities of SNM

(1) Movement shall be under direct escort and surveillance of at least two armed security force personnel.

(2) Security force personnel shall inspect the route before transport to identify and eliminate any condition or situation that could result in delay or risk to the movement.

(3) Prior to movement, security force personnel shall conduct a detailed inspection and search of the transport vehicle to ensure the safety and security of the movement.

(4) Security procedures for the movement of SNM within staging areas shall be specified in the site security plan.

b. Category II quantities of SNM movement shall be under material surveillance procedures and protected as specified in the site security plan.

c. Category III and IV quantities of SNM

(1) Movement shall be accomplished as described in the site security plan and shall include protective measures consistent with the category of SNM involved.

D. PROTECTION OF VITAL EQUIPMENT

1. All vital equipment shall be contained in designated Vital Areas located within the Exclusion Area. Security procedures for the protection of Vital Areas shall be specified in the site security plan.

2. Access control, intrusion detection systems, communication equipment, and testing and maintenance programs shall meet the applicable requirements of enclosure 4.

E. SECURITY CLASSIFICATION OF SNM

Security classification policy guidance for DoD nuclear reactors and SNM are contained in DoD Instruction 5210.67 (reference (o)). In addition, information concerning DoD nuclear reactors and SNM may be controlled as unclassified controlled nuclear information as described in the DUSD(SP) Memorandum (reference (g)).

Attachments - 2

1. Figure 3-1, Special Nuclear Material Protection Categories
2. Figure 3-2, Reportable Quantities of Special Nuclear Material

SPECIAL NUCLEAR MATERIAL PROTECTION CATEGORIES

FORM OF SNM	PU/U-233 PROTECTION CATEGORY				CONTAINED U-235 (≥20%) PROTECTION CATEGORY			
	I	II	III	IV	I	II	III	IV
WEAPONS Assembled Weapons and Test Devices	All Quantities				All Quantities			
PURE PRODUCTS Pits, Buttons, Major Components, Ingots, Recastable Metal, Directly Convertible Materials	≥2	≥0.4, <2	≥0.2, <0.4	<0.2	≥5	≥1, <5	≥0.4, <1	<0.4
HIGH-GRADE MATERIAL Carbides, Oxides Solutions (>25 grams/liter)Nitrates, etc., Fuel, Elements and Assemblies, Alloys and Mixtures, UF_4 or UF_6 (≥50% E)	≥6	≥2, <6	≥0.4, <2	<0.4	≥20	≥6, <20	≥2, <6	<2
LOW-GRADE MATERIAL Solutions (1-25 grams/liter), Recyclable Process Residues, Moderately Irradiated Material, Pu^{238} (Except Waste), UF_4 or UF_6 (≥20%, <50% E)		≥16	≥3, <16	<3		≥50	≥8, <50	<8
ALL OTHER MATERIALS Highly Irradiated Forms, Solutions (≤1 gram/liter), Uranium Containing Less Than 20% U-235 (Any Form)				Reportable Quantities	**NOTES:** 1. Quantities in kilograms 2. Reportable quantities for Category IV are shown at Figure 3-2.			Reportable Quantities

Figure 3-1. Protection Categories of Special Nuclear Materials

REPORTABLE QUANTITIES OF SPECIAL NUCLEAR MATERIAL

MATERIAL	REPORTING WEIGHT UNIT	ELEMENT	WEIGHT % ISOTOPE	ISOTOPE
Enriched Uranium	Whole Gram	Total U	U-235	U-235
Plutonium-242	Whole Gram	Total Pu	Pu-242	Pu-242
Plutonium	Whole Gram	Total Pu	Pu-240	Pu-239 + Pu-241
Uranium-233	Whole Gram	Total U	U-232(ppm)[1]	U-233
Plutonium-238	Gram to Tenth	Total Pu	Pu-238	Pu-238

[1] Parts per million

Figure 3-2. Reportable Quantities of Special Nuclear Materials

PHYSICAL SECURITY STANDARDS FOR DoD NUCLEAR REACTORS AND CATEGORY I AND II QUANTITIES OF SPECIAL NUCLEAR MATERIAL

A. INTRODUCTION

The standards outlined in this enclosure are provided to assist DoD Components in the development, design, and implementation of protective measures for nuclear reactors and SNM. The protective measures used for each location must be based on site-specific considerations and should address all of the areas in this enclosure.

B. SECURITY SYSTEM CONCEPT

1. The goal of a security system for nuclear reactors and SNM is to apply efforts and resources in such a manner as to preclude radiological sabotage and the theft or diversion of SNM. To achieve this goal, a security system shall provide the capability to deter, detect, assess, delay, respond to, and neutralize the intended actions of the adversary.

2. The components of a security system each have a function and a related security objective. Together, the visible components should attempt to deter a potential adversary. Detection, accomplished through human or electronic measures, identifies possible threats and penetration attempts against the security system in sufficient time to allow the remaining portions of the security system to defeat the adversary. Assessment, through the use of closed-circuit television (CCTV) subsystems, patrols, and fixed personnel, assists in determining the size and intention of an intrusion. Delay, consisting of active and/or passive security measures using various barriers, provides sufficient time for the appropriate response to be made by the security force.

3. Response, consisting of security and law enforcement personnel, is provided to the target in such a manner as to prevent the adversary from accomplishing its goal. Response is accomplished by the use of specifically designated, trained, and properly equipped security forces. Neutralization, consisting of apprehending, forcing retreat, or eliminating the adversary, is the final objective.

C. THREAT CONSIDERATIONS

1. The development of a security system is guided by a response to actual validated threats or to postulated threats that may arise. The threat is based on data derived from intelligence and investigative sources and may include overt activities or groups, either internal or external, using sophisticated equipment, arms, and methods. The intent of the threat may range from a person or group of persons demonstrating to make a political statement to persons desiring to obtain some SNM to fabricate a nuclear weapon or threaten the public with the potential of radiological contamination. The Defense Intelligence Agency (DIA) provides intelligence products that cover the range of threats mentioned above. In addition, the DIA is available to review plans for development of security systems for DoD nuclear reactors and SNM.

2. The minimum standards contained in this enclosure define what shall be required in designing a security system to protect nuclear reactors and SNM based on postulated threats. It is the responsibility of commanders at nuclear reactor and SNM facilities to define the local threat and to respond with commensurate measures.

D. PHYSICAL SECURITY STANDARDS

Physical security measures for the protection of DoD nuclear reactors and SNM shall be accomplished in accordance with the following standards:

1. Physical Barriers

a. Physical barriers consisting of fences, walls, and doors shall be designed to impede and aid in the detection of attempted entry and to provide sufficient delay to intrusion, thereby providing security response forces adequate time to apprehend and neutralize intruders.

b. Physical barriers shall be designed to ensure a means of limiting ingress and egress of personnel and vehicles to a central point, thereby facilitating identification and control procedures.

c. Physical barriers shall be used to define the perimeter of the Protected Area and Material Access or Exclusion Areas within the Protected Area. Both Exclusion Areas and Material Access Areas shall be located within the Protected Area so that access to vital equipment and SNM stored within these areas requires passage through at least two physical barriers.

d. An illuminated clear zone shall be maintained adjacent to the physical barrier at the perimeter of the Protected Area and shall be large enough to permit unobstructed observation on either side of the barrier to detect activities and any penetration.

e. A warning system, consisting of warning signs and a loudspeaker capability to warn intruders of the consequences of unauthorized entry, shall be established as an integral part of the physical barrier system.

f. Guidance on construction techniques and materials for an effective physical barrier system is contained in MIL-HDBK-1013/1 (reference (j)).

2. Access Controls

a. Material Access and Exclusion Areas shall be designed to positively identify and control all authorized individuals granted unescorted or escorted access to the nuclear reactor and SNM. All personnel without access authorization and their vehicles, packages, and material to be taken in or out of the Protected Area shall be identified, controlled, and searched. All personnel authorized access and their hand-carried packages shall be searched on at least a random basis. The access control system shall be designed to ensure prompt ingress and egress during emergency conditions and ensure access to vital equipment. Access control procedures shall be specified in the site security plan.

b. Verification of identity shall be conducted by security personnel at area entrances using a numbered picture badge identification system for all personnel authorized access to the Protected Area without escort. Personnel

not authorized entry to the Protected Area without escort shall be escorted and shall be badged to indicate that an escort is required. Additional levels of identification using other human, mechanical, or electronic means shall be used when dictated by an increased threat.

c. The access control system shall be designed to prevent unauthorized entry of prohibited items, such as firearms, explosives, or incendiary devices, into areas containing SNM or a nuclear reactor. The system should also prevent the exit of SNM from areas containing Category II or greater quantities of SNM.

d. Vehicle access to protected areas shall be restricted and controlled. All vehicles, except under emergency conditions, shall be searched for prohibited items before entry to the Protected Area. Emergency vehicles shall be kept under positive control by security forces while in the Protected Area and shall be searched before departing the area upon termination of the emergency.

e. All keys, locks, combinations, and related equipment used to provide access to Protected, Material Access, Vital, and other restricted access areas shall be controlled to reduce probability of compromise.

f. The Material Access, Exclusion, and Vital Areas shall be contained within the Protected Areas and their access controls shall be specified in the site security plan.

3. Intrusion Detection Systems (IDSs)

a. An intrusion detection system (IDS) shall be provided to detect and assess unauthorized personnel, activities, or conditions and to communicate with a central alarm monitoring activity so that an appropriate response can be initiated. The IDS shall provide the capability of early detection and near real-time assessment of any penetration into a nuclear reactor or SNM facility.

(1) Rooms, buildings, or portions of a building within a Material Access Area or controlled and alarmed process containing unattended Category I quantities of in-process SNM shall be equipped with an IDS.

(2) Doors to vaults and vault-type rooms used to store Category I or II quantities of SNM shall be protected with an IDS.

(3) Vault-type rooms used to store Category I or II quantities of SNM shall be equipped with an interior IDS sufficient to detect unauthorized intrusion.

(4) All unmanned exits from the Protected Area, Material Access Area, Exclusion Area, or Vital Area shall be equipped with an IDS.

b. All IDS alarms shall annunciate in a continuously manned central alarm monitoring facility located within the Protected Area and in at least one other independent continuously manned on-site station (not necessarily within the Protected Area) so that a single act could not interfere with the capability of calling for assistance or responding to the alarm. The central alarm monitoring facility shall be located within a building so that its interior is not visible from the perimeter of the Protected Area. Entry to the monitoring facility shall be controlled.

c. All IDS alarm devices and alarm communication equipment shall be tamper-indicating and self-checking. All IDSs shall have an auxiliary power supply in the event of a loss of primary power. Changeover to auxiliary power shall be automatic and not result in an alarm condition or cause false alarms.

d. All IDS equipment and components shall have a regularly applied test, maintenance, and quality assurance program to ensure an effective operable system. This program shall be specified in the site security plan.

4. Communications Equipment

a. Nuclear reactor and SNM facilities shall have communications equipment that provides dedicated, rapid, and reliable information exchange among security personnel at the site, the central alarm monitoring facility, security response forces, and with local law enforcement agencies.

b. There shall be at least two systems of communications between fixed security force locations, such as entry control facilities, and the central alarm monitoring facility. One of these systems shall be radio, and each system shall have an auxiliary power source.

c. Security personnel, both mobile and fixed, shall have access to a duress alarm or duress code system, as appropriate.

d. Communications equipment shall be tested daily and maintained on a regular schedule. Test schedule and procedures shall be specified in the site security plan.

5. Lighting

Adequate lighting shall be provided in clear zones and around other controlled access areas to discourage unauthorized entry, facilitate the detection of intruders, and assist in the identification of authorized personnel at entry control points during hours of darkness of reduced visibility. All security lighting shall have an auxiliary power source.

6. Security Force

a. A security force shall be established to perform the physical security requirements outlined in this enclosure and enclosure 3, in the site security plan, and in applicable regulations.

b. Members of the security force shall be trained, equipped, and qualified to perform each assigned security duty and to meet emergency situations. Sufficient security force members shall be readily available to react and respond to security alarms and incidents. (See DoD C-5210.41-M (reference (p)) regarding force on force training exercises associated with security of Category I SNM.)

c. Each facility shall have continuously on-site at least one full-time member of the security force with the authority and capability to direct physical protection activities and security response forces under emergency situations.

d. Security force management shall provide for the development, implementation, and enforcement of security procedures. These procedures shall be continuously assessed and revisions made when required by changed conditions.

VARIANCES, WAIVERS, AND EXCEPTIONS

A. GENERAL

Deviations from established security requirements shall be categorized as either a variance, waiver, or exception, and may be applicable to physical security facilities, plans, procedures, equipment, and monitoring standards established in this Directive or in any supplemental issuance.

1. A variance is the approved continuation of a nonstandard condition that technically varies from established requirements but essentially affords the same level of security.

2. A waiver is the approved temporary continuation of a nonstandard condition that deviates from an established security standard plus creates a security vulnerability to the security system and, therefore, requires compensatory measures. A waiver shall normally be approved for a period not to exceed 12 months and shall be extended only by the authority who granted the waiver and only after a review of the circumstances necessitating the extension.

3. An exception is the approved continuation of a nonstandard condition that varies from an established security standard plus creates a security vulnerability to the security system and, therefore, requires compensatory measures. Exceptions shall be granted only when correction of the nonstandard condition is adjudged to be not feasible or cost-effective. Exceptions shall be granted only after a careful and critical evaluation. All exceptions shall be reviewed by the granting authority at least every 2 years or when a major change in site configuration or mission offers the opportunity for corrective action to terminate the nonstandard condition. Exceptions shall be canceled unless it is found, by the approving authority, that the exception continues to be required and is justified.

B. REVIEW OF REQUESTS

Waivers and exceptions shall be evaluated and approved by the Commander of the Unified of Specified Command concerned (the respective heads of DoD Components for those sites not otherwise assigned to a Unified or Specified Command). This approving authority may be delegated in writing to a military officer of at least 0-7 grade on the staff. When considering a deviation request for a particular facility or site, the approving authority shall review all other waivers and exceptions currently in effect for that facility or site. This review is to ensure that, collectively, the deviations will not establish an overall vulnerability greater than the designated compensatory measures. Each waiver or exception shall be evaluated and approved on a case-by-case basis. Blanket waivers or exceptions are not authorized. A 10 percent deviation from all measurable standards, such as clear zone distances, fence height, etc., is permitted; therefore, such deviation does not require the submission and/or approval of a waiver or exception request.

C. COMPENSATORY MEASURES

1. A compensatory measure shall be instituted for each waiver or exception in effect. If appropriate, one compensatory measure may suffice for more than one waiver or exception. A compensatory measure shall also be instituted whenever

two or more variances, 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 variances at the facility or site; e.g., clear zones and perimeter lighting, which taken together are determined to create a vulnerability, then compensatory measures are required.

2. The approving authority shall review each waiver or exception to ensure that adequate compensatory measures have been established. Adequate compensatory measures may include additional security forces, procedures, and/or physical security devices such as additional locks, alarm, lighting, anti-intrusion devices, barricades, etc., which provide a level of security comparable to the required security standard. The criteria for accepting compensatory measures shall involve an assessment of the threat or vulnerability that has resulted from the condition that necessitates a waiver or exception. The compensatory measure shall 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 do not provide a comparable level of security.