

Army Regulation 190-54

Military Police

Security of Nuclear Reactors and Special Nuclear Materials

**Headquarters
Department of the Army
Washington, DC
30 April 1993**

Unclassified

SUMMARY of CHANGE

AR 190-54

Security of Nuclear Reactors and Special Nuclear Materials

This revision-

- o Provides requirements for the recovery of lost, seized, or stolen special nuclear material (para 2-1b).
- o Prescribes that unclassified information pertaining to plans, procedures, and equipment for the physical protection of nuclear reactors and special nuclear material will be safeguarded as DoD Unclassified Controlled Nuclear Information (para 2-1f).
- o Requires the conduct of a vulnerability assessment at each facility where special nuclear material is used or stored (para 2-2a).
- o Provides that Headquarters, U. S. Army Materiel Command will develop the postulated threat as the basis for the vulnerability assessment (para 2-2b), as well as the standardized format for documenting the results of the assessment and for the after action reports (para 2-2h).
- o Designates special nuclear material as inherently dangerous to others for use of force purposes (para 2-4a).
- o Prescribes minimum storage standards for special nuclear material (para 3-1).
- o Provides for the protection of vital equipment (para 3-3).
- o Explains the concept of the required security system for nuclear reactors and special nuclear material (para 4-2).
- o Establishes specific physical security standards for the protection of nuclear reactors and special nuclear material (para 4-4), to include required access controls (para 4-5).
- o Prohibits the locksmith from being designated as the key control officer or lock custodian (para 4-5g(25)).
- o Provides guidance on meeting requirement to continuously man two alarm monitoring facilities (para 4-6b).
- o Allows continued use of monitoring console systems installed prior to publication of this regulation that do not meet the map or video display requirement (para 4-6g(1)).
- o Provides guidance for testing the perimeter intrusion detection system (para 4-6n(2)).

- o Requires appropriate security personnel be trained to manually start the standby generator if the automatic starter fails to function properly (para 4-9b(4)).
- o Provides that the size, composition, and response time of the response force will be set by the major subordinate commander and approved by the Commanding General, U. S. Army Materiel Command (para 4-10c(1)).
- o Requires that the postulated threat and site vulnerability assessment be used as the criteria for determining the minimum response force requirements (para 4-10c(1)).
- o Requires security force weapons and ammunition be randomly checked to ensure tampering has not occurred (para 4-10i).
- o Provides that waivers and exceptions will be evaluated and approved by a general officer, or member of the Senior Executive Service, assigned to HQ, AMC (para 6-3a).
- o Requires that security forces are made aware of deviations and required compensatory measures in effect in the area where they are assigned security duties (para 6-4b).
- o Requires force-on-force training exercises at least every 18 months for security forces assigned at nuclear reactor facilities (para 7-8).
- o Provides guidance in conduct of vulnerability assessment with regard to the internal threat during nuclear reactor operations (app B, para B-3).
- o Defines the term "armed" with reference to security force members, as being equipped with a loaded weapon (glossary).
- o Defines the term "sabotage" as used in this regulation (glossary).

Effective 31 May 1993

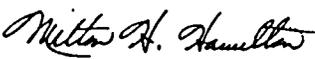
Military Police

Security of Nuclear Reactors and Special Nuclear Materials

By Order of the Secretary of the Army:

GORDON R. SULLIVAN
General, United States Army
Chief of Staff

Official:


MILTON H. HAMILTON
Administrative Assistant to the
Secretary of the Army

History. This UPDATE printing publishes a revision of this publication. Because the publication has been extensively revised, the changed portions have not been highlighted.

Summary. This regulation prescribes policy, responsibilities, procedures, and minimum standards for safeguarding Army nuclear reactors and special nuclear

materials. It implements Department of Defense Directive 5210.63.

Applicability. This regulation applies to the Active Army.

Proponent and exception authority. The proponent of this regulation is the Deputy Chief of Staff for Operations and Plans (DCSOPS). The DCSOPS has the authority to approve exceptions to this regulation that are consistent with controlling law and regulation.

Army management control process. This regulation is subject to the requirements of AR 11-12. It contains internal control provisions, but does not contain checklists for conducting internal control reviews. These checklists are contained in DA Circular 11-89-2.

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval of HQDA (DAMO-ODL), Deputy Chief of Staff for Operations and Plans, 400

Army Pentagon, Washington, DC 20310-0400.

Interim changes. Interim changes to this regulation are not official unless they are authenticated by the Administrative Assistant to the Secretary of the Army. Users will destroy interim changes on their expiration dates unless sooner superseded or rescinded.

Suggested improvements. Users are invited to send comments and suggested improvements through appropriate command channels on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to HQDA (DAMO-ODL), Deputy Chief of Staff for Operations and Plans, 400 Army Pentagon, Washington, DC 20310-0440.

Distribution. Distribution of this publication is made in accordance with DA Form 12-09-E, block 2514, intended for command level D for the Active Army; none for the Army National Guard and U.S. Army Reserve.

Contents (Listed by paragraph and page number)

Chapter 1

Introduction, page 1

Purpose • 1-1, page 1

References • 1-2, page 1

Explanation of abbreviations and terms • 1-3, page 1

Responsibilities • 1-4, page 1

Chapter 2

Policy and Planning, page 1

General • 2-1, page 1

Physical security and vulnerability assessment • 2-2, page 2

Physical security plan • 2-3, page 2

Use of force • 2-4, page 3

Reporting incidents • 2-5, page 3

Inventory discrepancies • 2-6, page 3

Waivers and exceptions • 2-7, page 3

Public release of information • 2-8, page 3

Chapter 3

Special Nuclear Material Protection Standards, page 3

Minimum storage standards at fixed facilities • 3-1, page 3

Transportation of SNM • 3-2, page 3

Vital equipment • 3-3, page 3

Security classification of SNM • 3-4, page 3

Chapter 4

Physical Security Standards for Nuclear Reactors and SNM,

page 3

Introduction • 4-1, page 3

Security system concept • 4-2, page 3

Threat considerations • 4-3, page 4

Physical security standards • 4-4, page 4

Access controls • 4-5, page 4

Intrusion detection systems • 4-6, page 6

Communications equipment • 4-7, page 8

Lighting • 4-8, page 8

Power sources • 4-9, page 8

Security force • 4-10, page 8

Chapter 5

Recovery Operations, page 9

General • 5-1, page 9

Planning • 5-2, page 9

Communications • 5-3, page 9

Chapter 6

Security Criteria Deviation Program, page 9

General • 6-1, page 9

Deviation categories • 6-2, page 9

Review and approval of requests • 6-3, page 10

Compensatory measures • 6-4, page 10

Security force considerations • 6-5, page 10

*This regulation supersedes AR 190-54, 12 November 1986.

Contents—Continued

Chapter 7

Training, page 10

General • 7-1, page 10

Training program • 7-2, page 10

Specialized training • 7-3, page 11

Continuing training • 7-4, page 11

Training records • 7-5, page 11

Response force (RF) training • 7-6, page 11

Augmentation force (AF) • 7-7, page 11

Force-on-force training • 7-8, page 11

Weapons training • 7-9, page 11

Training evaluation • 7-10, page 11

Appendixes

A. References, page 12

B. Physical Security and Vulnerability Assessment, page 13

C. Physical Security Plan Outline, page 14

Glossary

Index

Chapter 1 Introduction

1-1. Purpose

a. This regulation prescribes policy, responsibilities, procedures, and minimum standards for safeguarding Army nuclear reactors and special nuclear material (SNM).

b. This regulation—

(1) Applies to the nuclear reactors and SNM stored or used at the two existing nuclear reactor facilities assigned to the U.S. Army Materiel Command (AMC). Organizations, or activities planning to use or store nuclear reactors and SNM at other nuclear reactor facilities will request security guidance through command channels from Headquarters, Department of the Army (HQDA) (DAMO-ODL), Deputy Chief of Staff for Operations and Plans, 400 Army Pentagon, Washington DC 20310-0400.

(2) Does not apply to nuclear weapons. Because of the unique requirements associated with nuclear weapons, separate guidance regarding their security is provided in AR 50-5-1.

(3) Does not abrogate or abridge the—

(a) Authority or responsibility of a commander to apply more stringent security standards during emergencies or at any time the threat to nuclear reactors or SNM indicates additional protection measures are necessary.

(b) Responsibility of a commander operating nuclear reactors under Nuclear Regulatory Commission license or processing SNM to comply with the requirements of section 73, title 10, Code of Federal Regulations (10 CFR 73) and the Department of Energy (DOE) Orders 5632.1A and 5632.2A, as amended or changed.

1-2. References

Required and related publications and prescribed and referenced forms are listed in appendix A.

1-3. Explanation of abbreviations and terms

Abbreviations and special terms used in this regulation are explained in the glossary.

1-4. Responsibilities

a. The Assistant Secretary of the Army (Installations, Logistics, and Environment) (ASA (I,L&E)) will maintain oversight of physical security at the facilities with nuclear reactors and SNM.

b. The Deputy Chief of Staff for Operations and Plans (DCSOPS) will establish policy, procedures, and minimum standards for physical security of nuclear reactors and SNM.

c. The Deputy Chief of Staff for Intelligence (DCSINT) will maintain current, evaluated information concerning the hostile intelligence and terrorist threats to the security of nuclear reactors and SNM, and disseminate the information to the appropriate commanders and law enforcement officials.

d. The Commanding General, U.S. Army Criminal Investigation Command (USACIDC), will—

(1) Maintain current, evaluated information concerning the criminal threat to the security of nuclear reactors and SNM, and disseminate the information to the appropriate commanders and law enforcement officials.

(2) Conduct preliminary investigations into losses or recovery of SNM, regardless of dollar value, to determine if criminality occurred.

(3) Conduct investigations of actual or attempted break-ins or armed robberies of nuclear reactor facilities and in-transit; and monitor investigations conducted by civil law enforcement agencies when such incidents involve in-transit movements of SNM that are not under military control.

(4) Provide copies of USACIDC reports of investigations (ROI) (or a letter reflecting the results of investigations that are prepared pertaining to *(b)* and *(c)*) above to HQDA (DAMO-ODL), Deputy Chief of Staff for Operations and Plans, 400 Army Pentagon, Washington DC 20310-0400. Copies of ROIs prepared by civil law enforcement agencies will be obtained for military use, as required.

(5) Using the results of completed investigations, crime prevention surveys, or physical security inspections, assist HQDA (DAMO-ODL) and the commander concerned in evaluating existing security measures and recommending corrective action to improve security of nuclear reactors and SNM.

e. The Commanding General, U.S. Army Materiel Command (CG, AMC) will be responsible for the overall security of the nuclear reactors and SNM assigned to AMC and will—

(1) Provide command oversight, direction, guidance, and assistance as necessary to ensure compliance with the provisions of this regulation.

(2) Plan, program, budget, and allocate resources for the implementation of the physical security requirements in this regulation.

(3) Develop the postulated threat for the nuclear reactors and SNM and forward it to HQDA (DAMO-ODL), Deputy Chief of Staff for Operations and Plans, 400 Army Pentagon, Washington DC 20310-0400, for review and approval.

(4) Develop the site vulnerability assessment procedures and standardized format for documenting the assessment and after action results.

(5) Publish plans for the recovery of lost, seized, or stolen SNM.

f. The Commanding General, Forces Command (CG, FORSCOM) will, in coordination with CG, AMC, provide an augmentation force to support security forces at the nuclear reactor facilities covered by this regulation.

g. Commanders, directors, and custodians of nuclear reactor facilities and SNM will—

(1) Comply with this regulation.

(2) Ensure positive measures are taken for the complete physical security control of SNM during all phases of their life cycle.

(3) Implement plans for the recovery of seized, stolen, or lost SNM.

(4) Immediately report incidents and threats related to sabotage, seizure, theft, or loss of SNM (actual or suspected) or damage to nuclear reactors to the HQDA Army Operations Center (AOC) or through the most expeditious means available. Provide facts and circumstances in writing as soon as possible to HQDA (DAMO-ODL), Deputy Chief of Staff for Operations and Plans, 400 Army Pentagon, Washington DC 20310-0400.

(5) Ensure timely submission of Serious Incident Reports (SIR) according to requirements in AR 190-40.

(6) Conduct prompt investigations per AR 15-6 of losses or recovery of SNM after a decision by the USACIDC that criminal acts were not involved.

(7) Ensure a formal site physical security and vulnerability assessment is conducted at each facility initially and revised annually or more frequently as new vulnerabilities become apparent; and provide a copy of the completed assessment and updates through command channels to HQDA (DAMO-ODL), Deputy Chief of Staff for Operations and Plans, 400 Army Pentagon, Washington DC 20310-0400.

Chapter 2 Policy and Planning

2-1. General

a. It is Department of Defense (DoD) and Department of the Army (DA) 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, diversion, unauthorized access, or seizure, are of paramount importance during all phases of operations.

b. Commanders will develop procedures to ensure adequate protection is afforded nuclear reactors and SNM and to comply with statutory accountability requirements. Procedures will provide protection against theft, sabotage, diversion, unauthorized access, or

seizure, 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. Requirements for the recovery of lost, seized, or stolen SNM are contained in chapter 5.

c. The level and strategy of protection will be consistent with the SNM involved, 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.

d. Nuclear reactors and components without SNM will be protected consistent with the highest level of classified information they contain (AR 380-5).

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

f. Unclassified information pertaining to security plans, procedures, and equipment for the physical protection of nuclear reactors and SNM will be safeguarded as DoD Unclassified Controlled Nuclear Information (DoD UCNI) as described in DoD Directive (DoDD) 5210.83. HQDA will be advised through command channels when information not in the guidelines in enclosure 4 to DoDD 5210.83 is determined to be DoD UCNI. The following information will be provided to HQDA (DAMO-ZXA-S), Deputy Chief of Staff for Operations and Plans, 400 Army Pentagon, Washington DC 20310-0400—

(1) Identification of the information to be controlled as DoD UCNI.

(2) Justification for identifying the type of information to be controlled as DoD UCNI, based on the guidelines in enclosure 4 to DoDD 5210.83.

(3) Certification that only the minimal information necessary to protect the health and safety of the public or the common defense and security is being controlled as DoD UCNI.

g. Procedures contained in AR 25-55 will be followed when processing Freedom of Information Act (FOIA) requests for release of DoD UCNI. Initial denial authority for such FOIA requests will be the Deputy Chief of Staff for Operations and Plans (per AR 25-55). Such FOIA requests will be submitted to HQDA (DAMO-ZXA-S) for processing.

h. General access to nuclear reactors and SNM will be restricted to authorized personnel with established need. Access will be kept to a minimum and appropriate entry control and identification procedures will be established to ensure need for access. The two-person concept in AR 50-5 will apply.

i. Any operator or security individual in a position that would allow the individual, acting alone, the opportunity to divert or conceal the diversion of SNM will be subject to extensive screening and continuing evaluation by supervisors and co-workers according to DoDD 5210.42 and AR 50-5.

2-2. Physical security and vulnerability assessment

a. A physical security and vulnerability assessment will be prepared for each facility where SNM is used or stored.

b. HQ, AMC, through intelligence and law enforcement services, will 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, title 10, Code of Federal Regulations (10 CFR 73), which includes the insider threat (see para 4-3 for additional guidance). The postulated threat prepared by HQ AMC will be forwarded to HQDA (DAMO-ODL), Deputy Chief of Staff for Operations and Plans, 400 Army Pentagon, Washington DC 20310-0400 for review and approval. HQ AMC will direct implementation of the approved postulated threat. Additionally, a copy of the postulated threat will be maintained on file by each nuclear reactor facility. Consistent with policies in AR 381-10 and AR 380-13, supporting military counterintelligence and criminal investigative agencies will provide commanders or organizations responsible for security of nuclear reactors and SNM with current intelligence threats to nuclear reactors and SNM.

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

d. The vulnerability assessment will be conducted according to guidance contained in appendix B.

e. The assessment will be reviewed at least annually and updated as required. HQ, AMC will ensure that the assessments at the nuclear reactor facilities are conducted in a timely manner.

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) Quantities 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 type of 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.

h. HQ, AMC will develop a standardized format for documenting the site vulnerability assessment and after action results. The AMC standardized format will be used by the nuclear reactor facilities. The assessment, with exhibits, will be signed by the assessment team leader and forwarded to the commander concerned for information and appropriate action. The assessment will identify vulnerabilities found and recommend specific actions to eliminate or reduce the vulnerabilities. The commander's formal decision on such recommendations will be included in the assessment documentation. A copy of each vulnerability assessment, to include updates and annual reviews, will be forwarded through command channels to HQDA (DAMO-ODL), Deputy Chief of Staff for Operations and Plans, 400 Army Pentagon, Washington DC 20310-0400.

2-3. Physical security plan

a. Upon completion of the physical security and vulnerability assessment, a site security plan will be developed and implemented that prescribes the minimum standards and procedures and that complies with 10 CFR 73 and this regulation. The plan will consider—

(1) Minimum physical security criteria and standards for protecting nuclear reactors and SNM.

(2) Emergency and contingency procedures as well as protection strategies and measures to prevent radiological sabotage and the theft or diversion of SNM. A contingency plan for the defense of the facility will be prepared for each nuclear reactor facility to cover such protection strategies. The plan should follow the operation order format outlined in Field Manual 101-5. The plan may be attached as an annex to the site security plan. The plan will be exercised at a frequency which ensures adequate ability to execute the plan. A record of such exercises will be maintained.

(3) Requirements for security equipment unique to security or for monitoring nuclear reactors and SNM are described in DoDD 3224.3. (Implemented by memorandum, Office Assistant Secretary of the Army for Research, Development, and Acquisition, 21 Feb 90, same subject as DoDD. HQ, AMC will ensure this memorandum is provided to the reactor facilities.)

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

c. An outline of the physical security plan is contained in appendix C. The outline may be modified as necessary to facilitate use of

the plan; however, all applicable requirements prescribed by this regulation will be covered.

d. The plan will be signed by the facility commander. The next higher commander will formally review and approve the plan and any changes thereto. All reviews will be recorded and signed by the approving authority (commander, deputy commander, or chief of staff).

e. Physical security and contingency plans will be classified, if applicable, according to classification guidance in DoD Instruction (DoDI) 5210.67 and AR 380–5. See also requirements in paragraph 2–1*f* for control of unclassified controlled nuclear information pertaining to such plans.

2–4. Use of force

a. Per DoDD 5210.56, SNM is designated as inherently dangerous to others. Security force personnel will be armed and all possible actions will be taken, including the use of deadly force within the limitations of DoDD 5210.56 (AR 190–14), to prevent the actual theft, sabotage, or unauthorized control of SNM at a site.

b. All security personnel will be trained on the use of deadly force. Training will include specific scenarios, tailored to individual locations, that require security force members to respond with the appropriate use of deadly or nondeadly force as outlined in DoDD 5210.56 and AR 190–14.

2–5. Reporting incidents

All incidents and threats related to sabotage, theft, loss, diversion, or seizure of SNM, or to damage to nuclear reactors will be reported per requirements in paragraph 1–4*g*.

2–6. Inventory discrepancies

When an assessment of SNM status reveals an inventory discrepancy, statutory reporting requirements will be followed. (Reporting requirements in para 2–5 also apply.)

2–7. Waivers and exceptions

See chapter 6.

2–8. Public release of information

Public release of information regarding incidents and threats related to sabotage and the theft, loss, seizure, or diversion of SNM, and damage to nuclear reactors, will be governed by AR 360–5.

Chapter 3 Special Nuclear Material Protection Standards

3–1. Minimum storage standards at fixed facilities

SNM will be—

a. Used, processed, or stored only within a material access area enclosed within a limited area.

b. Stored in SNM vaults or vault-type rooms equipped with intrusion detection system (IDS).

c. Under material surveillance procedures or in process under alarm protection.

d. 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 will be specified in the site physical security plan.

e. Controlled at all times to prevent theft or diversion by a single authorized individual. Control may be achieved by material surveillance procedures.

f. Meet applicable physical security standards for nuclear reactors and SNM prescribed in this regulation.

3–2. Transportation of SNM

a. Domestic shipments of SNM will be per Department of Energy (DOE) and DoD agreement and consistent with DOE Order 5632.2A. When applicable, the agreement will be maintained on file

at the respective nuclear reactor facility. SNM transportation, security, control, and accountability procedures will be specified in the site security plan (when applicable).

b. Nuclear reactor cores will be transported and secured per DOE and DoD agreements and will be specified in the site security plan (when applicable).

c. Movement of SNM within a limited area will be protected as described in the site security plan (when applicable).

d. Movement of SNM between limited areas or staging areas (transfer points) at the same site will be as follows (when applicable):

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

(2) Security force personnel will 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 will 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 between limited areas and staging areas, when applicable, will be specified in the site security plan.

(5) Secure voice radio requirements in paragraph 4–7*b* will apply.

3–3. Vital equipment

a. All vital equipment will be stored in designated vital areas. Vital equipment and vital areas (see glossary) will be identified in the physical security plan (app C).

b. Security procedures for the protection of vital areas will be specified in the site physical security plan.

c. Access controls, IDS, communications equipment, and testing and maintenance programs will meet the applicable requirements of chapter 4.

3–4. Security classification of SNM

Security classification policy guidance for nuclear reactors and SNM are contained in DoDI 5210.67. In addition, information concerning nuclear reactors and SNM may be controlled as unclassified controlled nuclear information as described in DoDD 5210.83 (see para 2–1*f*).

Chapter 4 Physical Security Standards for Nuclear Reactors and SNM

4–1. Introduction

The standards outlined in this chapter are provided to assist commanders 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 chapter.

4–2. Security system concept

a. The goal of a security system for nuclear reactors and SNM is to apply efforts and resources in such a manner as to preclude sabotage, theft, loss, diversion, unauthorized access, or seizure of SNM. To achieve this goal, a security system will be provided the capability to deter, detect, assess, delay, respond to, and neutralize the intended actions of the adversary.

b. Each component of a security system has a function and a related security objective. Together, the visible components should attempt to deter a potential adversary. Human or electronic measures detect 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. Closed-circuit television (CCTV) subsystems, patrols, and fixed personnel, assess the size

and intention of an intrusion. Active and or passive security measures using various barriers delay and provides sufficient time for the appropriate response to be made by the security force.

c. Specifically designated, trained, and properly equipped security forces respond to the intrusion and neutralize the adversaries by apprehension, forcing retreat, or elimination of intruders.

4-3. Threat considerations

a. The development of a security system is guided by a response to actual validated threats or to postulated threats that may arise (see para 2-2b). 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 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) and the Intelligence Threat Analysis Center, U.S. Army Intelligence and Security Command, provide 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. The supporting military intelligence unit will be contacted for assistance in this regard.

b. The minimum standards contained in this chapter define what will 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.

4-4. Physical security standards

Physical security measures for the protection of DoD nuclear reactors and SNM will meet the following standards:

a. Physical barriers consisting of fences, walls, and doors will be designed to impede entry 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. Active entrance doors to nuclear reactor facility buildings will be secured with two high-security padlocks (Military Specification (MIL-P-43607)) (National Stock Number (NSN) 5340-00-799-8248). Each high-security padlock will be mounted on a high-security shrouded hasp (MIL-H-29181) (NSN 5340-01-196-2547, right hand, or NSN 5340-01-235-6907, left hand). Active access doors to the material access area will be secured with two high-security padlocks mounted on high-security shrouded hasps. All other doors which are not ordinarily used for access to the nuclear reactor facility building and the material access area will be secured from the inside with locking bars, dead bolts, low-security padlocks (NSN 5340-00-158-3807, with chain, or NSN 5340-00-158-3805, without chain), or panic hardware (when required for rapid exit in emergencies). Panic hardware, when used, will be installed so as to prevent opening the door by fish-wire operation of the bolt from outside the door. A serial numbered seal will be affixed to the panic hardware and checked periodically to verify that unauthorized exit from the structure has not been attempted.

b. Physical barriers will 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. The fenced area surrounding nuclear reactor facilities will have the minimum number of pedestrian and vehicular gates consistent with operational requirements. Gates will be designed so that traffic through them will be under the positive control of the security force. Entry and exit control facilities housing security forces will be protected against small arms fire. Except in emergencies and operational necessities, entry and exit will always be made through the main pedestrian and vehicular gates. Gates will be closed and secured when not in use. Semi-active gates will be locked with low-security padlocks (described in para 4-4a above). The bottom of the gate

will be close enough to firm ground to prevent an intruder from crawling under the gate.

c. Physical barriers will be used to define the perimeter of the limited area surrounding the nuclear reactor facility. The exclusion areas and material access areas will be located within the limited area so that access to vital equipment and SNM stored within these areas requires passage through at least two physical barriers. The first physical barrier will consist of at least one perimeter fence which will enclose the limited area surrounding the nuclear reactor facility. The second physical barrier will be the walls and doors of the nuclear reactor building which contains the material access area(s) where the nuclear reactor and SNM are stored or used. The perimeter fence will meet the standards and specifications described in U.S. Army Corps of Engineers (USACE) Standard Design Drawing (STD) 872-90-04 for non-sensored fence and or 872-90-05 for sensed fence, and will be constructed of seven feet high fabric plus outriggers. Existing fences that do not meet the new fence standards in this regulation may continue to be used until replacement is necessary at which time the new fence standards will apply.

d. An illuminated clear zone will be maintained adjacent to the physical barrier at the perimeter of the limited area and will be large enough to permit unobstructed observation on either side of the barrier to detect activities and any penetration. Clear zones will extend 30 feet on both side of the perimeter fence when a single fence is used. When two fences are used, clear zones will extend 30 feet outside the outer fence, the entire area between fences, and 30 feet inside the inner fence. Clear zones will be clear of all objects that could conceal or shield an individual.

e. A warning system, consisting of warning signs and a loud-speaker to warn intruders of the consequences of unauthorized entry, will be established as an integral part of the physical barrier system. Restricted areas will be designated according to AR 190-13. Restricted area warning signs will be posted along the entire perimeter fence and at each entry point so they can be seen readily and understood by persons approaching the perimeter. Restricted area warning sign shown in USACE Drawing DEF 872-90-01 will be used to meet this requirement. Warning signs will contain the local foreign language, if any, in addition to English.

f. Guidance on construction techniques and materials for an effective barrier system is contained in MIL-HDBK-1013/1, *Design Guidelines for Physical Security of Fixed Land-based Facilities*. The *Security Engineering Manual* prepared by the Corps of Engineers Protective Design Mandatory Center of Expertise, or appropriate technical manuals, when published, may also be used as guidance.

4-5. Access controls

a. Limited areas, material access, and exclusion areas will be designed to positively identify and control all authorized individuals granted unescorted or escorted access to the nuclear reactor and SNM. The commander concerned, or designated representative (who will be appointed in writing by the commander), may grant unescorted or escorted access to authorized personnel who have a need for access to such areas. An entry control roster (ECR), or individual entry control cards, will be prepared that will contain pertinent identifying data of all personnel authorized access to the limited area. (The ECR is not required for personnel authorized unescorted access to the limited area providing such personnel have been issued a numbered picture badge containing the pertinent identifying data. If so, a list of such badges will be maintained at the limited area entry and exit control point.) The ECR and changes thereto will be signed by the commander concerned or designated representative. ECRs and changes will include an expiration date. Only Personnel Reliability Program (PRP)-certified personnel may be granted unescorted access to material access areas and exclusion areas under the two-person concept. Personnel who are not PRP-certified must have a need for access to material access areas and exclusion areas and will be escorted by PRP-certified personnel. Unescorted access to the limited area may be authorized for personnel who have, as a minimum, an Entrance National Agency Check, a National Agency Check, or National Agency Check with written inquiries. Uncleared

personnel (those without the requisite personnel security investigation or security clearance) will be escorted by personnel authorized unescorted access. Escorted personnel will be kept under continual control and surveillance to prevent unauthorized disclosure of, or access to, security interests. A system will be established by which personnel who control access, vouch for, or escort personnel into a limited area, material access area, or exclusion area can covertly communicate a situation of duress to other operating or security personnel. The duress code will be changed as often as needed to ensure integrity or when compromise is suspected. The duress code will also be changed when an individual who was allowed access to the code is no longer authorized access to the code. Duress codes will be classified CONFIDENTIAL and declassified when changed. All personnel without access authorization (visitors and those personnel who require escort) and their vehicles, packages, and material to be taken in or out of the limited area will be identified, controlled, and searched. All personnel authorized access (those personnel who do not require escort) and their hand-carried packages will be searched on at least a random basis. The access control system will be designed to ensure prompt ingress and egress during emergency conditions and ensure access to vital equipment. Entry and exit procedures may be modified for emergencies and exercises, but the procedures will not compromise the safety and security of nuclear reactors and SNM. As a minimum, the emergency entry and exit procedures will provide for a system to verify the identity of the senior member of the emergency force. Such procedures will require the senior member to verify the number of personnel involved in the emergency force (opportunity to indicate duress will be provided). Access control procedures will be specified in the site security plan.

b. Verification of identity will be conducted by security personnel at area entrances using a numbered picture badge identification system for all personnel authorized access to the limited and or exclusion/material access areas without escort. Personnel not authorized entry to the limited and or exclusion/material access areas without escort will be escorted and will be badged to indicate that an escort is required. A controlled security badge system will be established to meet this requirement. Detailed procedures for control, accountability, and storage of security badges (and blank badges) will be established according to requirements in this chapter and policy and standards in AR 600-8-14 and AR 190-13. A custodian will be appointed in writing to control the receipt, issue, turn-in, recovery, expiration, and destruction of controlled badges. The custodian's duties will include inventory and accountability of the badge system and investigation of stolen, lost, or unaccounted for badges. To preserve integrity of the badge system, an accurate written record will be maintained to ensure a documented audit trail from receipt or fabrication of blank badges at the installation to receipt and disposition of badges by the badge custodian. Shipping or receipt documents will be retained until the badge system is changed. All badges received or fabricated will be listed by serial number. Computer generated badge systems will ensure system integrity to preclude compromise of the badge system. The record will reflect the serial number of badges on hand, the serial number of badges issued and to whom issued, the disposition of badges turned in, and badges that have been lost, stolen, unaccounted for, or invalidated. An unannounced inspection and inventory of records, logs, and badges will be made at least quarterly. The quarterly inspection and inventory will be conducted by a person (appointed in writing by the commander concerned, or designated representative) who does not have a vested interest in the outcome of the inventory. The badge custodian is specifically excluded from conducting such inspections and inventories. A current list of valid and invalid badges (for example, badges lost, unaccounted for, or withdrawn for any reason) will be maintained at the entry and exit control point. Badge racks or containers will be positioned at the entry and exit control point to ensure the badges are accessible only to individuals assigned to control them. For those sites where the entry and exit control point is not manned during reactor operations due to a safety hazard (for example, radiological), the badge container or rack may be moved to a location that will meet safety

requirements. Badges will be inventoried by serial number at each change of guard shift. Additional levels of identification using other human, mechanical, or electronic means will be used when dictated by an increased threat. Personnel controlling access to the limited area must be able to determine promptly and accurately the number and identity of personnel within the area at any given time. Additionally, security personnel in guard towers and roving patrols will be notified when—

(1) Activities are being conducted within their areas of responsibility.

(2) Personnel enter and exit the limited area during non-duty hours.

(3) Unauthorized access or other potential compromise situations occur.

c. The access control system will be designed to prevent unauthorized entry of prohibited items, such as firearms, explosives, or incendiary devices, into areas containing SNM or a nuclear reactor. Sealed packages that cannot be inspected will require a signed DA Form 1818 (Individual Property Pass). The bearer of the sealed package will not be allowed to sign the DA Form 1818. The form will be signed by another authorized individual. Persons authorized to sign DA Form 1818 will be designated by the commander concerned or authorized representatives (who will be appointed in writing). Samples of signatures of personnel authorized to sign DA Form 1818 will be maintained at the entry and exit control point. Changes will be updated as necessary. Other sealed packages and material not covered by DA Form 1818 will be opened and inspected for unauthorized items. Commanders concerned may designate additional items that must be controlled by DA Form 1818 when necessary. If so, DA Form 1818 will be controlled as described above. The system will also prevent the unauthorized exit of SNM from areas containing SNM.

d. Vehicle access to limited areas will be restricted and controlled. Only essential vehicles and materials handling equipment will be permitted access to limited areas. Privately owned vehicles will not be permitted in limited areas. Vehicles and materials handling equipment remaining in limited areas or material access areas after duty hours will be secured or disabled to ensure they are not readily usable by a hostile force. Vehicles and material handling equipment will not be parked within the inner or outer clear zone. Signs requiring removal of ignition keys and locking of all vehicles will be placed in all authorized vehicle parking areas adjacent to the site. Separate standards may be established for the security, parking, and removal of ignition keys and immobilization of official security force vehicles used for readiness operations. Such standards will ensure the vehicles cannot be readily used by a hostile force. All vehicles, except under emergency conditions, will be searched for prohibited items (and unauthorized personnel) before entry (and exit) to the limited area. As a minimum, each vehicle will be given a visual inspection of the passenger, cargo, and engine compartments, and underneath the vehicle. Emergency vehicles will be kept under positive control by security forces while in the limited area and will be searched before departing the area upon termination of the emergency.

e. All installed keys, locks, combinations, and related equipment used to provide access to limited areas (including intrusion detection systems (IDS), perimeter gates, and manhole covers), material access areas, vital areas, vaults, vault-type rooms, and other restricted access areas will be controlled at all times to reduce probability of compromise. The following procedures will apply—

(1) Keys will not be left unattended or unsecured at any time. Keys will be maintained separately from other keys and will be accessible only to those individuals whose official duties require access to them. Keys will not be removed from the installation.

(2) The two-person concept applies to keys and combinations to locks allowing access to SNM; and to keys or combinations to locks securing exclusion areas, material access areas, vaults, vault-type rooms, and storage rooms containing SNM.

(3) Access or possession of keys or combinations to both locks securing the active entrance doors to buildings containing nuclear reactors and SNM by only one person is prohibited. A dual control

system will be established to access such buildings so that security personnel control the keys to the "A" locks and operating personnel control the keys to the "B" locks.

(4) Keys required for maintenance and repair of IDS, including keys to the control unit and monitor cabinet, will be accessible only to authorized maintenance personnel. A list of authorized maintenance personnel will be kept current and accessible to personnel who control and issue such keys. Procedures will be established to ensure security personnel verify the IDS locations accessed by maintenance personnel. Testing of IDS by security personnel is required immediately after maintenance, repairs, or modifications of IDS.

(5) A roster of personnel authorized access to receive keys will be kept current by the responsible organization. The roster will be protected from public view. The roster will be signed by the designated official and contain the names of those individuals authorized to receive keys.

(6) The number of keys will be held to a minimum. Master key and keyed-alike systems are prohibited. Keys will not be duplicated unless authorized in writing by the key control officer.

(7) When not attended, or used, keys will be stored in a lockable key container. Any GSA-approved security container, or equivalent container, or key container constructed of at least 22 gauge steel, is acceptable for storing such keys. The key container will be located in a room where it is kept under surveillance or in a room that can be locked during non-duty hours. Procedures will be established to preclude access of the stored keys by one person in contradiction of two-person control requirements.

(8) In the event of lost, misplaced, or stolen keys, the affected locks or cylinders will be replaced immediately. Compromised lock combinations will also be changed immediately.

(9) Replacement of lock cylinders and broken keys to high-security locks will be requested by the key control officer through normal supply channels.

(10) MACOMs are designated as approval authority for any deviation in key procurement procedures, to include requests for procurement of extra keys for high-security locks (such keys will be accounted for at all times).

(11) Combinations to locks, when used, will be changed—

(a) When placed in use.

(b) When an individual knowing the combination no longer requires it.

(c) When the combination has been subject to compromise.

(d) At least annually.

(12) Lock combinations will be recorded, sealed in an envelope, and stored in a security container. No other written record of the combination will be kept. Standard Form (SF) 700 (Security Container Information), may be used to record the lock combinations. Controls will be established to ensure envelopes containing lock combinations are not made available to unauthorized personnel in contradiction of control procedures in this chapter.

(13) Padlocks will be locked to the hasp when the door or area is open to preclude theft, loss, or substitution of the lock.

(14) Reserve locks and keys will be secured at all times to preclude access by unauthorized personnel.

(15) Key registers will be established to identify keys for each installed lock, their current location, and custody.

(16) Completed key registers will be retained in the unit files for at least 90 days. The following information will be included in the key control register:

(a) Locks and or keys which do not have a serial number will be given one. This number will be inscribed on the lock or key as appropriate.

(b) Printed name and signature of the individual receiving the key.

(c) Printed name and signature of the person issuing the key.

(d) Date and time of issuance; and date and time returned.

(e) Printed name and signature of the individual receiving the returned key.

(17) DA Form 5513-R (Key Control Register) may be used to

meet the above key register requirement. If used, DA Form 5513-R will be reproduced locally on appropriate size paper. A copy for reproduction purposes is located in the back of AR 190-11, which is part of the *Physical Security UPDATE Handbook*.

(18) Key registers and lock location rosters of installed locks will be protected from unauthorized persons. Locksmiths and key control officers will not be authorized access to information concerning the specific locations of installed locks at the site.

(19) Keys will be inventoried jointly with each change of custody and recorded. Keys in two-person controlled containers will be inventoried only when the containers have been opened.

(20) Keys and locks will be inventoried by serial number every month. The inventory will be conducted by a person (appointed in writing by the commander concerned, or designated representative) who does not have a vested interest in the outcome of the inventory. The locksmith will not be assigned to conduct the inventory. The inventory will be reported in writing to the key control officer. Records of inventories will be kept in unit files for 1 year.

(21) Locks will receive preventative maintenance as required, but as a minimum, semi-annually.

(22) Locks described in paragraph 4-5e will be rotated randomly to different locations, or have cylinders changed, at least annually. Rotation of locks or changing of cylinders is not required when an "A" and "B" lock system has been established. Personnel will be identified and authorized access only to either "A" or "B" lock keys (or combinations), but not both. The system will preclude an individual from changing access to the "A" and "B" keys.

(23) A key control officer (who will be subject to PRP requirements in AR 50-5) will be appointed in writing by the commander concerned or designated representative to manage the lock and key control system. The locksmith will not be designated as the key control officer.

(24) The key control officer's duties will include—

(a) Procurement and initial receipt of locks and keys through supply channels.

(b) Maintenance of records (accountability from receipt to disposal) to identify each lock and key used by the nuclear reactor facility.

(c) Issuance of locks and keys to key custodians at the nuclear reactor facility. Two-person control locks and keys will be placed in use at the nuclear reactor facility by the respective key custodians and not by the key control officer.

(d) Storage of a sufficient quantity of spare locks as back up for the lock system. Such locks and keys will be stored and accounted for at all times.

(e) Establishment of a current lock and key control standing operating procedures (SOP) for the effective management and implementation of the lock and key control system prescribed in this chapter.

(25) The locksmith will not be designated as the key control officer or lock custodian.

f. The access controls for the limited area, materiel access, exclusion, and vital areas will be specified in the site security plan.

4-6. Intrusion detection systems

a. An IDS will 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. Two continuous lines of IDS sensors that utilize a different sensing phenomenon will be installed around the site perimeter to detect unauthorized penetration of the perimeter security system. Each line of IDS sensors will have line supervision. Sensors covering personnel and vehicle portals and entrapment areas may be placed in the access mode during high traffic periods provided appropriate compensatory measures are authorized in the site security plan. The IDS will provide the capability of early detection and near real-time assessment of any penetration into a nuclear reactor or SNM facility. Near real-time assessment may be satisfied when assessment of the actual cause of activation of the sensor alarm is either by direct visual assessment or electro-optical equipment (imaging system). Imaging systems provide a remote visual image of

activity in an area under surveillance. Closed circuit television, low light-level television, infrared, and radar are types of systems that may be used to meet the near real-time assessment requirement.

(1) Rooms, buildings, or portions of a building within a material access area or controlled and alarmed process area containing unattended SNM will be equipped with an IDS.

(2) Doors to vaults and vault-type rooms used to store SNM will be protected with an IDS.

(3) Vault-type rooms used to store SNM will be equipped with an interior IDS sufficient to detect unauthorized intrusion.

(4) All unmanned exits from the material access area, exclusion area, or vital area will be equipped with an IDS.

b. All IDS alarms will annunciate in a continuously manned alarm monitoring facility located within the limited area and in at least one other independent continuously manned station (not necessarily within the limited area) so that a single action could not interfere with the capability of calling for assistance or responding to the alarm. When the requirement to continuously man the alarm monitoring station within the limited area cannot be met due to safety considerations (for example, radiological hazards), all monitoring functions will be conducted at the other alarm monitoring station until the safety hazards no longer exist. The alarm monitoring facilities will be located within a building so that its interior is not visible from the perimeter of the limited area. Entry to alarm monitoring facilities will be controlled to prevent unauthorized access.

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

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

e. IDS sensors on moveable openings will consist of a balanced magnetic switch that meets or exceeds Switch, Balanced Magnetic SA-1955/FSS-9 (V) MIL-S-52867A (ME), 15 March 1977. This switch will be placed on the protected side (inside) of all moveable openings that exceed 96 square inches with a smaller dimension greater than 6.4 inches; for example, doors, windows, and hatches.

f. IDS will consist of sensors integrated by data transmission links into a monitor console. The data transmission link will include—

(1) Line supervision to detect and signal attempts of cutting, shorting, splicing, or substituting the transmission link. Supervision must initiate an alarm when a variance of 5 percent in the normal line supervision parameter is detected.

(2) Cable terminal boxes which group interior or exterior sensor inputs, and which are not within the structures being protected by the interior IDS, will be locked and alarmed. This requirement also applies to cable terminal boxes for perimeter IDS.

g. Alarm activations will be displayed at the alarm monitoring console. The following provisions will be included—

(1) Audio and visual indicators of alarm status will be displayed on a map or video display terminal. The display selected will graphically present the facility configuration as well as the zones being monitored. Monitoring console systems installed prior to publication of this regulation need not be replaced solely for the purpose of meeting the map or video display requirement; however, as the systems deteriorate and replacement becomes necessary, appropriate upgrades will be accomplished to conform to the standards set forth herein.

(2) Audio and visual indicators will also display line supervision status and access and secure status.

h. Backup battery power supply, independent of primary and standby power sources, will be capable of operating the equipment for 4 hours.

i. Capability will be provided to conduct remote self-test of IDS circuit continuity.

j. IDS will be active (in secure status) at all times except when the area containing SNM is occupied by authorized personnel.

k. Appropriate compensatory measures will be taken when the IDS is not installed or inoperable.

l. Procedures will ensure that persons monitoring the IDS maintain record of alarms. The records will be used to evaluate IDS effectiveness (reliability, sensitivity, required adjustments or maintenance, and other data intended to maintain or increase security). Records will be retained in unit files for 1 year. Records will include the nature of the alarm, the date and time the alarm was received, the location, and actions taken in response to the alarm. Records will be reviewed by supervisory personnel to ensure proper actions were taken, and to identify and correct IDS reliability problems. DA Form 4930-R (Alarm/Intrusion Detection Record) may be used to record alarms received. If used, DA Form 4930-R will be reproduced locally on appropriate size paper. A copy for reproduction purposes is located in the back of AR 190-11, which is part of the *Physical Security UPDATE Handbook*. A computer-generated printout of alarms may also be used, provided all required information has been included or supplemental information is included in a log.

m. IDS technical manuals and operating instructions for installed IDS will be available for reference to ensure sensor sensitivity setting criteria and testing methods are properly applied. When such manuals and operating instructions are not available for any reason, supporting engineer personnel will be contacted for assistance and technical advice.

n. The purpose of testing the IDS is to ensure reliability and to preclude undetected tampering and neutralization of the system. Written instructions will be provided for testing sensors. Instructions will be facility specific and include procedures which verify sensor sensitivity and simulate actions an intruder could be expected to use. The following testing requirements will apply—

(1) Interior sensors will be tested at least monthly by causing an actual alarm. Testing will be conducted by security personnel or by maintenance personnel under the supervision of and in the presence of security personnel. Depending on the type sensor, such alarm activations could include opening doors and windows, loosening antitamper devices, deliberate movement within the structure, or vibrating the walls and floors. Where advanced sensor systems which provide the capability to remotely stimulate individual sensors via an electronically activated sensor phenomenology device are installed, this capability may be used to fulfill the testing requirement.

(2) Randomly selected sections (zones) of the perimeter (exterior) IDS will be tested daily (when permitted by radiation safety requirements) by causing an actual alarm. Depending on the type sensor, such alarm activations could include touching, tapping, pulling or climbing the fence, crawling, rolling, walking or running over "protected" ground, or passing through a sensor beam. The IDS sections to be tested will be selected in such a manner that the entire perimeter IDS is tested at least monthly.

o. A record of all sensor tests will be maintained for 1 year. The record will reflect the date of the test, name of person conducting the test, results of the test, and any required corrective action resulting from the test.

p. Each change of guard and security shift will conduct a remote self-test of IDS circuit continuity from the annunciator and display equipment.

q. Routine IDS maintenance will be conducted at least twice a year, unless recommended more frequently by the equipment manufacturer. Documentation will be available to validate the manufacturer's recommended maintenance program. Maintenance personnel must be qualified to repair or replace worn or failing components, and to detect evidence or possible indications of tampering with the IDS. Immediately after IDS maintenance, repairs, or modifications, an actual test of the IDS of the affected area will be performed by security personnel and recorded in the daily guard/security log.

r. A record of IDS maintenance, repairs, and replacement of component parts will be maintained for 1 year. The record may be

maintained on DA Form 2404 (Equipment Inspection and Maintenance Worksheet) according to instructions in DA Pam 738-750.

s. A monthly check will be made of the IDS backup batteries and included in the record of alarm checks. The monthly check of backup batteries will require that the batteries assume the full load to ensure the capability exists to support the sensor complement. Voltage and amperage checks are in addition to systems loading.

4-7. Communications equipment

a. Nuclear reactor and SNM facilities will 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 local law enforcement agencies. A capability will also be provided for communications between alarm monitoring personnel and personnel who remain inside the nuclear reactor building during reactor operations.

b. There will be at least two systems of communications between fixed and mobile security force locations, such as entry control facilities, and the central alarm monitoring facility (to include alarm monitoring facility located off-site). One of these systems will be radio. Radios will have a multiple channel capability and be secured or securable by an approved crypto- system (see AR 380-19 for guidance). The second system will be a direct line type of telephone network. Each system of communications will have an auxiliary power source.

c. Strict communications discipline will be enforced for all radio and telephone transmissions on the security force communications net. Security personnel, both mobile and fixed, will have access to a duress alarm or duress code system, as appropriate.

d. Communications equipment will be tested daily and maintained on a regular schedule. When operationally feasible, all communication checks will be conducted on a random basis. Test schedules and procedures will be specified in the site security plan.

4-8. Lighting

Adequate lighting will be provided in clear zones (para 4-4d) and around controlled access areas to discourage unauthorized entry, facilitate the detection of intruders, and assist in the identification of authorized personnel at entry and exit control points during hours of darkness or reduced visibility. Perimeter lights will provide full lighting output within 3 minutes after primary or standby generator power is applied. The lighting controls will be protected against tampering or unauthorized use. Perimeter lighting controls will be installed to enable activation by security personnel. Switches for exterior lights will be installed so they are not accessible to unauthorized persons. If power is lost to perimeter lighting, a thorough security sweep of the site area will be conducted after power is restored. All security lighting will have an auxiliary power source.

4-9. Power sources

a. *Primary electric power* . Sites will have primary electric power (for example, commercial power) to provide sufficient capacity to carry the connected load with the least voltage fluctuation.

b. *Standby generator power* . Sites will have standby generator power to provide emergency electrical power for all on-site security functions. The following criteria applies—

(1) The line distribution grid, which transmits the emergency power within the site, will be underground, when possible.

(2) Fuel tanks for standby generators will be located underground, when possible.

(3) An automatic or remote start capability will be able to assume the full essential on-site load within 60 seconds of primary power interruption.

(4) Operating instructions will be mounted on a wall near each standby generator. The instructions will detail the steps to start, run, load, unload, and shut down the generator under both exercise and emergency conditions. It will also include instructions for manual operations if the automatic equipment fails to function properly (appropriate security personnel will be trained in this operation).

(5) Testing will be conducted under full load to ensure the generator will be operable when needed. Testing standards, maintenance and records requirements are contained in AR 420-43.

c. *Battery power* .

(1) *Automatic switchover* . In case of failure of the primary electric power, sensor alarms and communications systems will be automatically switched over to battery power. Audible and visual indications that primary electric power has failed or has been restored must be provided at the sensor data display monitor system.

(2) *Battery charging system* . Batteries must be capable of operating sensor, alarm, and communication components for at least 4 hours when operating in a reasonable maximum demand situation. This requirement does not apply to perimeter lighting and CCTV systems. The battery charging system, using primary electric power, must fully charge the batteries from “no charge” to “fully charged” within 12 hours. The batteries will “float” during primary power operations and be maintained at “full charge.”

(3) *Battery locations* . The batteries and primary electric power charger system will be located within a building inside the limited area and either placed under continual surveillance or contained in a locked enclosure with an IDS installed to protect against tampering.

d. *Protection of power sources* . The generator (including fuel tanks), transformers, and transmission lines for standby power will be protected against the effects of small arms fire.

4-10. Security force

a. A security force will be established to perform the physical security requirements outlined in this regulation, in the security plan, and in applicable regulations. Security guards sufficient to control entry and to prevent unauthorized access to nuclear reactors and SNM will be provided at each nuclear reactor facility 24 hours a day (para 3-1d). The actual number of guards will be specified in the site security plan. In addition, each facility will have continuously on-site at least one full-time member of the security force with the authority and capability to direct physical security protection activities and security forces under emergency situations. Facilities housing the security force will be protected against small arms fire.

b. Members of the security force will be trained, equipped, and qualified to perform each assigned security duty and to meet emergency situations. Training requirements are prescribed in chapter 7. Only the most physically fit, trained, capable, reliable, and trustworthy personnel will be assigned to protect nuclear reactors and SNM. Provisions in AR 190-56 apply to civilian guards assigned to nuclear reactor facilities.

c. Sufficient security force members will be readily available to react and respond to security alarms and incidents. (See DoD C-5210.41-M, implemented by AR 50-5-1, regarding force on force training exercises (chapter 7) associated with security of SNM.)

(1) A response force (RF) will be organized and trained to respond to those situations that threaten or affect the security of nuclear reactors and SNM (para 3-1d). The size, composition, and response time of the RF at each nuclear reactor facility will be set by the major subordinate commander concerned and approved by CG, AMC. The postulated threat, in conjunction with the site vulnerability assessment (para 2-2), will be used as the criteria for determining the minimum RF requirements at each nuclear reactor facility. The posted guards (for example, entry and or access control and tower guards) will not be a part of the RF, and will continue their assigned tasks when the RF is deployed. Elements of the RF may be deployed to patrol the nuclear reactor facility, assess alarms which cannot be otherwise assessed, act as the initial contingent of the RF until the total RF arrives (if necessary), or perform other security functions providing they do not degrade the primary functional capability of the total RF. In addition to the RF, all available installation security forces will be used to protect the nuclear reactor facility as needed.

(2) An augmentation force (AF) will be organized and trained to reinforce the RF during emergencies, to include increased threat

conditions or receipt of advance notice of likely terrorist acts, involving the security of nuclear reactors and SNM. CG, Forces Command will provide the AF to meet this requirement. The number of personnel required and response time for the AF will be set by CG, AMC, in coordination with CG, FORSCOM. The response time for the AF will be based on the actual or anticipated threat and geographical location of the AF. The AF, its location, and method of contacting the AF when needed, will be included in the site security or contingency defense plan. Cost of the AF deployment will be borne by the supported organization. (See para 7-7 for training exercise requirements.)

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

e. Security force personnel will not be tasked to perform non-security functions while on duty.

f. Commanders will monitor and evaluate overtime hours and take appropriate action to preclude excessive overtime by guards. (Extensive use of overtime could affect the guard's effectiveness and readiness to respond in an emergency situation.) Use of overtime hours will be reviewed and evaluated during physical security inspections.

g. Information concerning security force weapons includes the following:

(1) Weapons which provide the maximum practical firepower will be provided for security forces, either as the weapon assigned or as one that is immediately available. Sidearms have little value as protection from dedicated adversaries except in confined quarters. Where it is determined to be necessary or advisable to issue sidearms to personnel responsible for protection of nuclear reactors and SNM, weapons providing greater firepower will be immediately available to them, where appropriate.

(2) The security force will be equipped and armed for combat type operations and terrorist incidents. The physical security and vulnerability assessment and local surrounding environment will be considered in authorizing the types of weapons to be employed. The weapons listed below or comparable types will be considered for use—

- (a) M16 rifle.
- (b) M14 rifle.
- (c) M60 machine gun.
- (d) M2 .50 caliber machine gun.
- (e) M203 or M79 40mm grenade launcher.
- (f) M249 squad automatic weapon.
- (g) M1911A1 .45 caliber pistol.
- (h) M9 9mm pistol.
- (i) .38 caliber revolver.
- (j) Shotgun.

h. Equipment required by the security force includes the following:

(1) Security forces will be provided the maximum feasible protection. As a minimum, protective masks, protective body armor, and helmets will be available for use in the immediate vicinity of all personnel assigned to security functions.

(2) In areas of difficult terrain or subject to adverse weather, a capability for cross-country travel over this terrain or snow will be available to security forces.

(3) All vehicles used by the security force will meet the highest standards of reliability and, in order to minimize the probability of breakdown, will not exceed the established maintenance criteria for replacement. Commanders will conduct a continuing, objective, analysis of the condition and readiness of the security force motor vehicle fleet's reliability and take appropriate action to ensure vehicle readiness.

(4) Where response is normally on foot, vehicles (surface and or air) will be designated for use by security forces in the event of operational necessity.

(5) The RF normally stationed outside the limited area will have wire or bolt cutters issued as part of their equipment in order to cut

through the fences should the normal entry gates not be available for use.

i. To ensure security of weapons and ammunition have not been tampered with and made unserviceable when needed, the following precautions will be taken—

(1) Security force weapons will be randomly checked for serviceability. Checks will include pertinent weapon parts such as firing pins, extractors, and so forth.

(2) Ammunition magazines or clips will be randomly unloaded and the rounds inspected. Ammunition, both loose and bulk, will also be randomly checked.

(3) The random checks of weapons and ammunition will be performed by personnel other than those who maintain or routinely issue such weapons and ammunition to security forces (for example, armorers or arms room personnel).

Chapter 5 Recovery Operations

5-1. General

a. The commander having custody of SNM will immediately alert, activate, and deploy all resources capable of recovering or locating and maintaining surveillance of lost, seized, or stolen SNM.

b. Recovery operations will have the highest priority, taking precedence over all other missions.

c. Radiation safety and nuclear criticality of SNM must be determined in recovery operations. Proper handling of SNM is vital.

5-2. Planning

a. HQ, AMC will develop and publish command SNM recovery plans. Plans will include forces to be used and rules of engagement. Information copies of plans will be forwarded to HQDA (DAMO-ODL), Deputy Chief of Staff for Operations and Plans, 400 Army Pentagon, Washington DC 20310-0400, and HQDA (DAMO-SSN), Deputy Chief of Staff for Operations and Plans, 400 Army Pentagon, Washington DC 20310-0400.

b. Nuclear reactor facilities storing or having custody of SNM will practice recovery operations plans according to AMC command guidance.

5-3. Communications

Secure communications (see AR 380-19 for guidance) will be provided security forces responsible for initiating recovery operations. However, recovery operations will not be delayed by lack of secure communications equipment.

Chapter 6 Security Criteria Deviation Program

6-1. General

The purpose of the nuclear reactor and SNM security criteria deviation program is to—

a. Ensure that the prescribed security standards are properly observed and implemented at all activities where nuclear reactors and SNM are used, processed, or stored.

b. Be used as a management tool to monitor corrective actions taken to ensure established security standards are maintained.

c. Ensure deviations from established criteria are systematically and uniformly identified by the proper level of command so that compensatory measures will be taken where necessary.

6-2. Deviation categories

Deviations from established security criteria will be categorized as either a waiver or exception, and may be applicable to physical security, facilities, plans, procedures, equipment, and monitoring standards established in this regulation.

a. 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 will normally be approved for a period not to exceed 12 months and will be extended only by the authority who granted the waiver and only after a review of the circumstances necessitating the extension. Each extension will state "first extension," "second extension," and so forth.

b. 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 will be granted only when correction of the nonstandard condition is adjudged to be not feasible or cost-effective. Exceptions will be granted only after a most careful and critical evaluation. All exceptions will be formally reviewed by the approval 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 will be cancelled unless it is found, by the approval authority, that the exception continues to be required and is justified.

6-3. Review and approval of requests

a. Waivers and exceptions will be evaluated and approved by a general officer, or member of the Senior Executive Service, assigned to HQ, AMC, having assigned staff cognizance for physical security matters for the command. This waiver and exception approval authority may not be delegated. Information copies of approved waivers and exceptions, and renewal of such waivers and exceptions, will be sent to HQDA (DAMO-ODL), Deputy Chief of Staff for Operations and Plans, 400 Army Pentagon, Washington DC 20310-0400. When considering a deviation request for a particular facility or site, the approval authority will 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 will 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, and so forth, is permitted; therefore, such deviation does not require the submission and or approval of a waiver or exception request.

b. Requests for security deviations will be coordinated with the provost marshal (or security manager) and surety and safety officials on the installation or activity concerned. For structural deviations, requests also will be coordinated with the supporting engineer office. Requests will include—

(1) A statement of the problems or deficiencies that constitute standards below those cited in this regulation.

(2) Compensatory measures in effect at the activity to make up for noncompliance with required standards cited in this regulation.

(3) A statement that adequacy of the compensatory measures has been considered in light of the vulnerabilities identified in the last site physical security and vulnerability assessment (para 2-2).

(4) Reasons the unit, facility, or installation cannot comply with the requirements of this regulation.

(5) The commander's statement of the action taken or planned to correct the deficiencies.

(6) Each successive command's recommendations on such requests.

c. Exceptions and waivers will not be used to reduce or eliminate the minimum security standards required by this regulation.

6-4. Compensatory measures

a. A compensatory measure will be instituted for each waiver or exception in effect. If appropriate, one compensatory measure may suffice for more than one waiver or exception.

b. The approval authority will 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, barricades, and so forth, which provide a level of security comparable to the required security standard. The criteria for accepting compensatory measures will involve an assessment of the threat or vulnerability that has resulted from the condition that necessitates a waiver or exception. 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 do not provide a comparable level of security.

6-5. Security force considerations

a. Security force supervisors will ensure that prescribed compensatory measures are implemented as required.

b. Security forces will be made aware of the deviations and required compensatory measures currently in effect in the area where they are assigned security duties.

c. Prescribed compensatory measures for individual deficiencies must not, when considered in total, unrealistically task the security forces in the area where they are assigned security duties.

Chapter 7 Training

7-1. General

a. Personnel assigned to nuclear reactor and SNM security duties will receive basic and continuing training to ensure they are adequately trained and qualified to perform assigned duties.

b. Training will be comprehensive and consist of both formal classroom training and practical exercises, to include force-on-force training exercises.

c. In addition to the training specified in this appendix, minimum training requirements in AR 190-56 are applicable to civilian security guards assigned to security duties at nuclear reactor facilities.

7-2. Training program

Commanders will establish an adequate training program to meet the requirements of this regulation. The program will include at least the following training subjects:

a. *General training* .

(1) Personnel identification.

(2) Circulation control (how personnel within the site area are identified and controlled, to include escort requirements and procedures for duress situation; and rapid entry and exit procedures for emergencies).

(3) Apprehension.

(4) Operation and use of IDS equipment.

(5) Search and seizure: individuals, packages, and vehicles.

(6) Operation and use of primary and alternate security communications systems and equipment.

(7) Operation and procedures for starting emergency generators when automatic system fails.

(8) Adversary threat (for example, terrorism, sabotage, theft, loss or diversion, demonstrations, civil disturbances).

(a) Adversary groups (to include insiders).

(b) Motivation and objectives.

(c) Tactics.

(d) Recognition of sabotage related devices and equipment.

(9) Security vehicle operations.

(10) Duress system.

(11) Security awareness and vigilance.

(12) Record-keeping.

(13) Type and location of hazardous and vulnerable equipment and material.

(14) Location and use of fire protection equipment, utility switches, and first aid facilities.

(15) Protective measures against chemical attack, self-aid and first-aid measures.

(16) Physical form of SNM (recognition of such items in case of attempted unauthorized removal from the facility).

(17) Basic radiation safety.

b. Security skills training .

(1) Small unit combat tactics (day and night).

(2) Anti-terrorism tactics.

(3) Specialized equipment (for example, protective masks, body armor, night vision devices, radio communications, contraband electronic detectors, and so forth).

(4) Use of force (including deadly force).

(5) Contingency defense plans.

(6) Weapons qualification with assigned weapons to include familiarization fire for weapons without formal courses of fire.

c. Transportation security (when applicable) .

(1) Convoy techniques.

(2) Escort vehicle procedures.

(3) General tactics for responding to threats.

(4) Continuous surveillance of shipment procedures.

(5) Emergency transfer of shipment procedures.

(6) Isolation of shipment (load) vehicle.

d. Security supervisory personnel training .

(1) *Contingency defense plan .*

(a) Bomb threats.

(b) Civil disturbances and demonstrations.

(c) Hostage situations.

(d) Motivation of security personnel.

(e) Evaluation and uses of intelligence services.

(2) Recovery operations .

(a) Recovery plan.

(b) Interaction with other military or civilian recovery forces.

(3) Emergency reporting requirements .

7-3. Specialized training

Security force personnel will also will receive specialized training pertaining to their specific duties and duty location. This training will be certified by a supervisory level individual designated by the commander for this purpose, indicating that the individual is proficient for duty.

7-4. Continuing training

Commanders will also establish a continuing training program to promote the education and motivation of security force personnel. The program will include—

a. Firing of assigned weapons (para 7-9).

b. Briefings on security incidents of interest which have occurred at nuclear reactor or other sensitive facilities (use as lessons learned).

c. Current and potential exterior and insider threats.

d. Intelligence and counterintelligence procedures and capabilities.

e. Postulated actions by intruders and insiders and the planned security force reactions.

f. Practical exercises in defensive techniques to counter the threats.

7-5. Training records

Training records will be maintained on each individual assigned to site security duties. These records will be of sufficient depth, as determined by the commander, to ensure that the individual is qualified for certification and has maintained that qualification.

7-6. Response force (RF) training

The RF will deploy on training exercises at least once a week to maintain proficiency. Deployment of the RF in response to incidents may be counted as the weekly training exercise. All such training exercises must be scheduled in coordination with the reactor facility operating personnel and approved by the responsible safety officer to ensure radiation safety considerations are met. A record of the RF training exercises will be maintained in unit files for 3 months.

7-7. Augmentation force (AF)

The AF will be exercised at least annually at the supported nuclear reactor facility. CG, AMC may deviate from the requirement to conduct such exercises at the supported nuclear reactor facility when determined necessary. In such cases, the commander and key operations staff personnel of organizations providing the AF support will be required to visit the supported nuclear reactor facility as a group at least annually. They will visit pertinent areas and review the support plan. The cost of the exercises and staff visits will be borne by the supported unit or organization. A record of the current and previous annual training exercise or staff visit will be maintained by the supported commander.

7-8. Force-on-force training

Force-on-force training exercises are required at least every 18 months for security forces assigned at nuclear reactor facilities. The training will be tailored to each location based on the vulnerability assessment and postulated threat. The training may be conducted on-site or off-site as determined by security, safety, and radiation considerations. The training will include realistic force-on-force exercises using an engagement simulation system and employing an aggressor force. Feedback from such training exercises will be provided to all site personnel so lessons learned can be developed. A record of the last two training exercises (current and prior) will be maintained in unit files for review during physical security inspections.

7-9. Weapons training

a. Security personnel will receive training so they will thoroughly know the weapons with which they are armed, to include the proper care, maintenance, safety features, and corrective actions in the event of malfunction.

b. HQ, AMC will prescribe the frequency of training in live fire of weapons (following guidance in DA Pam 350-38 for military personnel and AR 190-56 for civilian security guards). Every effort should be made to conduct night firing as part of the live fire weapons training.

c. The security force should be cross-trained and familiar with all weapons available to the security force.

7-10. Training evaluation

Commanders will determine the adequacy of the security training program through periodic evaluation of security force proficiency during response and training exercises and while on duty at fixed posts and mobile patrols. Adjustments to the training program will be made accordingly.

Appendix A References

Section I Required Publications

AR 25-55

The Department of the Army Freedom of Information Act Program. (Cited in para 2-1g.)

AR 50-5

Nuclear Surety. (Cited in para 2-1i.)

AR 190-11

Physical Security of Arms, Ammunition and Explosives. (Cited in paras 4-5e(17) and 4-10c.)

AR 190-13

The Army Physical Security Program. (Cited in paras 2-4a, c, 4-4e, and 4-5b.)

AR 190-14

Carrying of Firearms and Use of Force for Law Enforcement and Security Duties. (Cited in para 2-4a, b.)

AR 190-40

Serious Incident Report. (Cited in para 1-4g(5).)

AR 190-56

The Army Civilian Police and Security Guard Program. (Cited in paras 1-4g (5), 4-10b, 7-1c, and 7-9b.)

DoDD 5210.83

Department of Defense Unclassified Controlled Nuclear Information. (DoD UCNI) (Cited in paras 2-1f and 3-4.)

DoDI 5210.67

Special Nuclear Material Information, Security Classification Guidance. (Cited in para 3-4.)

Section II Related Publications

A related publication is merely a source of additional information. The user does not have to read it to understand this publication.

AR 15-6

Procedures for Investigating Officers and Board of Officers

AR 360-5

Public Information

AR 380-5

Department of the Army Information Security Program

AR 380-13

Acquisition and Storage of Information Concerning Nonaffiliated Persons and Organizations

AR 380-19

Information Systems Security

AR 381-10

U.S. Army Intelligence Activities

AR 420-43

Electrical Services

AR 600-8-14

Identification Cards, Tags, and Badges

CFR 10, Part 73 (10 CFR 73)

Physical Protection of Plants and Materials

DA Pam 350-38

Standards in Weapons Training

DoDD 3224.3

Physical Security Equipment (PSE): Assignment of Responsibility for Research, Development, Testing, Evaluation, Production, Procurement, Deployment, and Support

DoDD 5210.56

Use of Deadly Force and the Carrying of Firearms by DoD Personnel Engaged in Law Enforcement and Security Duties

DoDD 5210.63

Security of Nuclear Reactors and Special Nuclear Materials

DOE Order 5632.1A

Protection Program Operations

Note: DOE orders may be obtained from Director, Office of Safeguards and Security, ATTN: SA-10, Germantown, MD 20874; commercial (301) 903-4244

Department of Energy (DOE) Order 5632.2A

Physical Protection of Special Nuclear Material and Vital Equipment

FM 101-5

Staff Organization and Operations

MIL-H-2981

Hasp, High-security, Shrouded, for High- and Medium-security Padlock. Note: Military Specifications may be obtained from Commanding Officer, Code 156, Naval Construction Battalion Center, Fort Hueneme, CA 93043-5000.

MIL-P-4307

Padlock, Key-operated, High-security, Shrouded Shackle

Security Engineering Manual

Note: May be obtained from Corps of Engineers, Omaha District, ATTN: CEMRO-ED-ST, 215 North 17th Street, Omaha, NE 68102.

USACE Drawing DEF 872

Restricted Area Perimeter Warning Signs

Note: USACE drawings may be obtained from USA Engineer Division, Huntsville, ATTN: HN-DED-ES, (Svc Sec), Box 1600, Huntsville, AL 35807-4301.

USACE Standard (STD) Drawing 872-90-04

FE7 Chain-Link Security Fence Details for Non-sensored Fence.

USACE Standard (STD) Drawing 872-90-05

FE7 Chain-Link Security Fence Details for Sensored Fence

Section III

Prescribed Forms

This section contains no entries.

Section IV

Referenced Forms

DA Form 1818

Individual Property Pass

DA Form 2404

Equipment Inspection and Maintenance Worksheet

DA Form 4930-R

Alarm/Intrusion Detection Record

Appendix B Physical Security and Vulnerability Assessment

B-1. General

a. A physical security and vulnerability assessment is a detailed analysis of the entire nuclear reactor site (as well as the reactor operational environment within the site (para B-3)), and the environment surrounding the site. The vulnerability assessment determines the nuclear reactor facility's vulnerability to sabotage, theft, loss, diversion, unauthorized access, or seizure of SNM from an external and internal threat perspective.

b. The vulnerability assessment is similar to an estimate of the situation (that is, a study of the mission, enemy terrain, security forces available, and time). In conjunction with the postulated threat (para 2-2b), which includes both an external and internal threat, the assessment forms the basis for preparation of the site security and defense planning. From the assessment, the commander plans a defense and organizes security forces accordingly.

c. The vulnerability assessment is accomplished by a team consisting of the facility director or activity commander (commander's participation is encouraged, but is not required), security officer, knowledgeable members of the security force, and security experts from outside the span of control of the facility director and activity commander.

B-2. Conduct of site vulnerability assessment

a. *Enemy*. Update the enemy situation and threat to the site by coordinating with supporting law enforcement and intelligence agencies. Determine the known, potential, or perceived threat to the site (para 2-2b).

b. *Mission*. Consider the mission of security forces. It is to—

(1) Deny unauthorized access to SNM. The defense of the site's terrain and preventing penetration of the site perimeter are secondary to defending or preventing unauthorized access to SNM. Identify storage areas that contain SNM. This knowledge and information learned during terrain analysis will help to identify SNM storage areas most likely to be targets.

(2) Contain the enemy. If access to the site is gained, prevent the enemy from exiting the site with the SNM.

(3) Recover the material (radiological aspects must be considered). Ensure plans to recover SNM includes measures for on-post and off-post scenarios.

c. *Terrain*. Determine how to use terrain to the advantage of security forces and how the enemy will try to use terrain to the enemy's advantage. These determinations are made by gathering information from studying the site, conducting terrain walks, and studying site models, maps, or sketches of the area.

(1) During the terrain walk inside the site, note the vulnerability of the SNM storage areas.

(2) During the terrain walk through the area around the site, note the logical avenues of approach, areas providing concealment, fields of fire into the site, and probable strong points for attackers.

d. *Observation and fields of fire*. Analyze where security forces will have the best fields of fire to cover entrances and approaches to SNM storage areas. Observation is needed to gain information on the enemy, to adjust fire, and to accurately shoot direct fire. Ensure entrances can be observed and defended with direct fire. Consider the following:

(1) The positions outside the site that provide the enemy with observation of site activities.

(2) The positions that provide the enemy with clear fields of fire on the SNM storage or reactor operating areas.

(3) The locations from which the enemy may observe and fire on the SNM storage or reactor operating areas.

(4) Locations from which the enemy can observe and fire on exit points of the entry control facility and security deployment routes.

(5) How motorized vehicles will be deployed. Consider the following:

(a) The advantage of an offense and defense using rapid changes in location and by rapid changes from mounted fighting to dismounted fighting.

(b) How the security forces should be divided between mounted and dismounted forces, and how the mounted and dismounted forces should work as a team.

e. *Cover and concealment*. Identify cover and concealment to protect or hide security forces. Identify covered and concealed positions from which the enemy can fire at site security forces.

f. *Obstacles*. Analyze natural and artificial obstacles in and around the site. Some obstacles will stop, delay, or divert personnel, while other obstacles are required to block vehicles. Analyze the approximate delay time provided by artificial obstacles when planning maneuvers and security force deployment. Security forces must be in position to defend entrances to storage areas containing SNM before the enemy can bypass all obstacles and get inside a storage area. Backup forces must be in position to reinforce the on-site force and prevent the enemy's escape; and must also be in position before the enemy exits the storage area with SNM.

g. *Key terrain*. Identify key terrain that, if occupied, gives an advantage to the forces occupying it. Key terrain for site defense provides cover, concealment, good observation, and field of fire. Examples of key terrain, inside and outside the site, that may help attackers, include hills, roads, and buildings. Security forces must frequently reconnoiter these positions and be able to occupy or cover them with fire.

h. *Avenues of approach*. Analyze avenues of approach to the site for the deployment of security forces, weapons, and obstacles. Identify approaches that may be hard to travel, but may be used by the enemy to gain surprise.

i. *Weather*. Determine how weather conditions may be used advantageously and how to keep the enemy from taking advantage of those conditions. Review the effect weather conditions will have on the terrain (that is, observation, key terrain, and avenues of approach).

j. *Time*. Consider the time and space over which forces will be deployed. The time provided by obstacles and physical security delay systems will help to determine deployment routes, location of fighting positions, and maneuvers.

k. *Security forces*. Available security forces affect the selection of defensive positions, fire planning, and deployment. Determine how the mission can be accomplished with available security forces, considering the mission, enemy, terrain, and weather.

l. *War-game*. War-game the attack of the site after the physical layout of the area is well known and site vulnerabilities have been identified. Personnel conducting the vulnerability assessment should mentally place themselves in the role of both the overt and covert attacker. Develop the various scenarios (e.g., ground and aerial attack, containment, and recovery). Walk through the various scenarios and develop new scenarios as necessary. The scenarios then become the basis for writing the contingency plan for the defense of the site.

m. *Prepare plan*. Prepare the site contingency defense plan after the vulnerability assessment is completed.

n. *Evaluate plan*.

(1) Walk security forces through the planned deployment. This provides an opportunity to analyze alternatives and to plan for enemy reactions.

(2) Use a game-board (or a sand table) to apply attack scenarios to identify shortcomings in the site contingency defense plan.

(3) Use force-on-force exercises. These exercises are probably the most realistic method of evaluating the site contingency defense plan. The Multiple Integrated Laser Engagement System, or similar

system, adds realism to the evaluation. Force-on-force exercises allow observation of the performance of defense forces.

B-3. Internal threat

The goal is to prevent an insider from having an opportunity to sabotage (see also para B-1a) the nuclear reactor and SNM. Review and observe internal control procedures, including the two-person concept and how it is applied under different situations. Observe reactor operations. Pay particular attention to the operation of the reactor by remote means. Ask "what if" questions with reference to the possibility of sabotage by an insider during the reactor operations. Determine if the two-person control is effective. Identify the vulnerabilities and recommend corrective actions. Document the results and include the security measures in the reactor operating procedures and site security plan.

B-4. After action results

See paragraph 2-2h for specific requirements for documenting the results of the vulnerability assessment.

Appendix C Physical Security Plan Outline

(See para 2-3 for basic guidance and requirements).

C-1. Classification and authority

Cite the overall security classification of the plan and the authority for such classification (para 2-3e).

C-2. Name and location of the facility

Self-explanatory.

C-3. Mission of the facility

Self-explanatory.

C-4. Purpose of plan

A brief statement of the purpose of the plan. In general, the plan should ensure that good planning has integrated all forces, procedures, devices and equipment into an effective security system.

C-5. Objectives

Cite the objectives of the plan (for example, protection of the nuclear reactor and SNM from sabotage, theft, loss, diversion, or unauthorized access (paras 2-1 and 4-2).

C-6. Threat analysis (external/internal)

Review the postulated threat (para 2-2) and overall threat considerations (para 4-3). Review threat information from the supporting counterintelligence and law enforcement activities which are responsible for the geographical area of the site concerned. Analyze the threat from terrorism, sabotage, theft, vandalism, and so forth, and identify any known individuals or organizations which pose these threats. Update the threat analysis at least annually, or more frequently if warranted by changing conditions.

C-7. Vulnerability

Identify critical and other structures, buildings, and work areas (to include vital areas) that require protection. Consider their location, size, function, and contents (to include vital equipment) even if used only occasionally.

C-8. Priorities

Establish priorities for protecting the various facilities and or areas within the nuclear reactor facility.

C-9. Limited, exclusion, material access, and vital areas

Delineate these areas.

C-10. Equipment and devices to detect or delay intrusion

a. Perimeter boundary .

- (1) Type and construction.
- (2) Clear zones.
 - (a) Widths.
 - (b) Surface undulations, depressions, and ditches.
 - (c) Obstacles (for example, poles, trees, boulders, structures, and so forth) that could not be removed.
 - (d) Culverts, utility or escape tunnels, and other structures.
- (3) Gates.
 - (a) Type and construction (personnel, vehicle, or both).
 - (b) Locations.
 - (c) Hours of operation.
 - (d) Locking means and procedures.
 - (4) Signs.
 - (a) Types — no trespassing, persons and or vehicles subject to search, use of deadly force, and bilingual wording when appropriate.
 - (b) Location.
 - (5) Inspection and maintenance. Inspection should be scheduled frequently enough to ensure the barriers are accomplishing their purpose. Provide information for mowing of grass, removal of debris, repair of eroded ground, and trimming or pruning of trees and shrubs.
 - b. Security lighting .*
 - (1) Types — area, glare projection, controlled (width of lighted strip), and portable.
 - (2) Type of light source (low-pressure sodium vapor, high-pressure sodium vapor, mercury vapor, incandescent).
 - (3) Use, control, and standards.
 - (a) Perimeter.
 - (b) Gates.
 - (c) Interior areas and structures.
 - (4) Inspections and maintenance.
 - (5) Emergency actions for power failure— who does what and when.
 - (6) Emergency generator— type, location, fuel supply, operating instructions, testing procedures, and maintenance requirements.
 - (7) Emergency backup lighting— operating instructions.
 - c. Protective alarms.*
 - (1) Types— ensure application of proper device(s) to protect the limited, exclusion, and material access areas.
 - (2) Locations.
 - (3) Procedures for operation, monitoring, and activation or deactivation.
 - (4) Tests and antitamper procedures.
 - (5) Inspections and maintenance— who does what and when.
 - (6) Sensitivity settings (obtain information as appropriate from the system operating instructions or technical manual).
 - (7) Records and logs.
 - (8) Actions by security force when alarms occur or when the system, or any part of the system, becomes inoperative.
 - (9) Duress system.
 - d. Communications system .*
 - (1) Types.
 - (2) Locations.
 - (3) Use.
 - (4) Tests.
 - (5) Inspection and maintenance.
 - (6) Records and logs.
 - (7) Emergency and or backup power sources.
 - e. Locks and keys .*
 - (1) Types.
 - (2) Use.
 - (3) Locations.
 - (4) Maintenance and rotation.
 - (5) Controls, logs, and accountability.
 - (6) Two-person key controls.
 - f. Delay systems .*
 - (1) Types.
 - (2) Locations.
 - (3) Controls and operating instructions.
 - (4) Total delay time provided.
 - (5) Inspections and maintenance.

g. Security procedures during construction, renovation, or extensive maintenance .

h. Security procedures during nuclear reactor operations with special consideration to the internal threat .

C-11. Measures to control personnel, vehicles, and material.

Determine what restrictions on access and movement are required for each critical area or structure (for example, limited area, exclusion area, material access area, vital area).

- a. Personnel access controls.*
- b. Assigned personnel— PRP.*
- c. Visitors— cleared and uncleared.*
- d. Maintenance personnel (Government and contractor).*
- e. Escort requirements.*
- f. Search and seizure procedures.*
- g. Duress system.*

C-12. Personnel identification system

Personnel recognition and identification cards or badges for assigned personnel, visitors, and maintenance personnel.

- a. Identification cards.*
- b. Badges.*
- c. Entry control rosters.*

C-13. Vehicle control

a. Search and seizure procedures.
b. Parking locations during duty and non-duty hours (include security requirements).

- c. Restrictions and control of:*
- (1) Privately-owned vehicles.
 - (2) Government vehicles.
 - (3) Contractor vehicles.
 - (4) Maintenance vehicles.
 - (5) Commercial vehicles.
 - (6) Emergency vehicles (for example, security, fire, and medical).
 - d. Registration, if applicable.*

C-14. Material control

- a. Incoming.*
- (1) Requirements for admission, to include restrictions.
 - (2) Inspection, search, and seizure.
 - (3) Sealed packages and containers.
- b. Outgoing.*
- (1) Documentation required.
 - (2) Inspections, search, and seizure.
 - (3) Classified documents or materials, controls, and procedures for incoming and outgoing, including emergency destruction.

C-15. Emergency entrance and or exit procedures

Means of rapid entry and or exit should be provided for EOD, fire, security, and medical personnel.

C-16. Security forces

- a. Type— military, civilian.*
- b. Composition and organization.*
- c. Authority and jurisdiction.*
- d. Weapons, ammunition, and equipment.*
- e. Rules of engagement and use of deadly force.*
- f. Training.*
- g. Actions to be taken under adverse weather and limited visibility conditions.*
- h. Posts.*
 - (1) Locations.
 - (2) Areas of responsibility.
 - (3) Hours.
 - (4) Duties and functions, including general patrol routes (require that routes and times be varied and that stationary posts be rotated to combat boredom).
 - (5) Reporting procedures.
- i. Response force.*

- (1) Purpose and mission.
- (2) Size, composition, and organization.
- (3) Weapons, ammunition, and equipment.
- (4) Location and call-out procedures.
- (5) Reaction time.
- (6) Protection of response vehicles from sabotage.
- (7) Protected response means and alternate routes.
- (8) Training, including frequency of testing.

C-17. Emergency actions of general nature

Indicate the actions which are required for serious emergencies. Attach detailed plans for natural or man-made disasters, fire, serious injuries, emergency entrance and exit procedures, bomb threats, demonstration control and civil disturbance, recovery operations, and so forth.

C-18. Movements of SNM

Procedures to ensure security compliance. (When applicable.)

C-19. Coordination

- a. Integration of this plan with supporting forces.*
- b. Liaison and coordination with nearby military units, including combat, police, intelligence, and counterintelligence units, and with cognizant civil agencies (including civil police and FBI, as appropriate).*

C-20. Appendixes

- a. Guard orders.*
- b. Communications plan.*
- c. Recapture/recovery plan.*
- d. Rules of engagement and use of deadly force (include rules for air or helicopter assault).*
- e. Threat analysis.*
- f. Site vulnerability assessment documentation.*
- g. Contingency defense plan.*
- h. Disaster control plan.*
- i. Demonstration control plan.*
- j. Civil disturbance plan.*

Glossary

Section I Abbreviations

AF

augmentation force

AMC

U.S. Army Materiel Command

AOC

U.S. Army Operations Center

ASA (I,L&E)

Assistant Secretary of the Army (Installations, Logistics, and Environment)

CCTV

closed-circuit television

CFR

Code of Federal Regulations

CG

commanding general

DA

Department of the Army

DIA

Defense Intelligence Agency

DCSINT

Deputy Chief of Staff for Intelligence

DCSOPS

Deputy Chief of Staff for Operations and Plans

DoD

Department of Defense

DoDD

DoD Directive

DoDI

DoD Instruction

DOE

Department of Energy

DSN

Defense Switch Network

ECR

entry control roster

EOD

explosive ordnance disposal

FBI

Federal Bureau of Investigation

FORSCOM

Forces Command

FOIA

Freedom of Information Act

GSA

General Services Administration

HQDA

Headquarters, Department of the Army

IDS

intrusion detection system

PRP

Personnel Reliability Program

RF

Response force

ROI

Report of Investigation

SIR

serious incident report

SNM

special nuclear material

UCNI

unclassified controlled nuclear information

USACE

U.S. Army Corps of Engineers

USACIDC

U.S. Army Criminal Investigation Command

Section II Terms

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.

Armed

Equipped with a loaded weapon. (DoD 5210.56)

Augmentation force

Additional personnel (or units) organized, trained, equipped, and capable of augmenting site security forces as required.

Auxiliary power source

See emergency power source.

Clear zone

An area adjacent to a physical barrier (for example, perimeter fences), clear of all objects that could conceal or shield an individual. Clear zones will extend 30 feet on both sides of the perimeter fence when a single fence is used. When two fences are used, clear zones will extend 30 feet outside of the outer fence, the entire area between fences, and 30 feet inside the inner fence.

Custody

Responsibility for the control, transfer, and movement of, and access to, special nuclear

material. Custody may or may not include accountability.

Deadly force

Force that a person uses causing, or that a person knows or should know would create a substantial risk of causing, death or serious bodily harm. (DoDD 5210.56)

Delay

The effort achieved by physical features, technical devices, or security measures and forces that impedes an adversary from gaining access to a nuclear reactor or SNM. Normally expressed as a function of time, it is a major consideration in the design and development of nuclear reactor and SNM security systems.

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.

Emergency power source

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

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.

Exception

An approved permanent deviation from the provisions of this regulation that creates a security vulnerability and requires compensatory measures.

Facility

See site.

Insider

An insider is any individual who has authorized access to a nuclear reactor facility and or SNM.

Intrusion detection system

An alarm system consisting of a sensor(s) capable of detecting one or more types of phenomena, signal media, annunciator(s), and energy source, for signaling the entry or attempted entry of a person or other target into the area protected by the system.

Key control officer

A person, other than a locksmith or key custodian, appointed in writing by the commander to manage the lock and key program for the installation or facility.

Key custodian

A person, other than a locksmith or key control officer, who has custody of the keys in use at a particular site or facility. A documented chain of custody for such keys is required at all times.

Keyed alike system

A system that allows a number of locks to be operated by the same key.

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 (perimeter fences).

Material access area

An area containing SNM specifically defined by physical barriers, located within a protected area, and subject to specific access controls.

Material surveillance procedures

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

Near-real time assessment

Instantaneous assessment of the actual cause for the activation of the sensor alarm by either direct visual assessment, or with the aid of electro-optical imaging equipment such as closed circuit television.

Nuclear reactor

A reactor in which fissile material is used in a self-supporting chain reaction (nuclear fission) to produce heat and or radiation for both practical and research development.

Nuclear reactor facility

See site.

Postulated threat

An estimate of potential adversary types, acts, capabilities, and combinations thereto 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.

Primary electric power source

The source of power, either external (commercial) or internal, that provides power to the site facilities on a day-to-day basis.

Protected area

An area encompassed by physical barriers and to which access is controlled.

Radiological sabotage

See sabotage.

Reactor facility

A building containing a nuclear reactor and or SNM.

Response force

The immediate, on-location security force organized, trained, armed, equipped, and capable of responding to any situation as required.

Responsible commander

Normally, the first commander in the chain of command who is responsible for the overall security of the nuclear reactor facility and or SNM. (Also referred to as site commander)

Restricted area

See AR 190-13.

Sabotage

a. National defense . An act or acts with intent to injure, interfere with, or obstruct the national defense of a country by willfully injuring or destroying, or attempting to injure or destroy, any national defense or war material, premises or utilities, to include human and natural resources (DoD Joint Pub 1-02).

b. Industrial . Any deliberate act which is directed against a facility, property, component, or procedure and intended to cause damage, obstruct productivity, or interrupt normal operating functions (DOE Order 5632.1A).

c. Radiological . Any deliberate act directed against an SNM facility, an SNM shipment, transport, or a component of such a facility or shipment or transport, which could directly or indirectly endanger the public health and safety (to include facility and or installation personnel) by exposure to radiation (DOE Order 5632.1A).

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.

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.

Site

A storage or nuclear reactor facility, activity, place, or location containing a nuclear reactor and or SNM.

Site commander

See responsible commander.

Small arms fire

Projectiles of the ball type with impact force up to that of a 7.62 mm bullet fired from an M14 rifle or equivalent at its highest velocity using service ammunition.

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 SNM (except source material), or any material enriched by any of the foregoing.

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 inch 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 part 101, title 41, Code of Federal Regulations. Double lock system is required in all cases. Lock system may consist of two built-in combination locks, or two high-security padlocks mounted on high-security shrouded hasps (para 4-4a), or one built-in combination lock and one high-security padlock mounted on high-security shrouded hasp.

Standby generator

See emergency power source.

Two-person concept (or two-person rule)

See AR 50-5 for definition. It is applicable to SNM. It is also applicable to the prevention of sabotage by an internal threat, to include by remote means during nuclear reactor operations.

Vault

A burglar-resistant, windowless enclosure that meets the definition of an SNM vault. Additionally, vaults will include an intrusion detection alarm activated by an opening of the door.

Vault-type room

A room having a combination-lock on its doors or doors protected by an intrusion detection system activated by the penetration of walls, floors, ceilings, openings, or motion within the room.

Vital area

A security area located within a protected area for the protection of vital equipment.

Vital equipment

Equipment, systems, or components whose failure, sabotage, or destruction would cause unacceptable interruption to a national security program or an unacceptable impact to the health and safety of the public. Remote controls for operation of nuclear reactor is considered vital equipment.

Waiver

An approved temporary deviation from the provisions of the regulation that creates a security vulnerability and requires compensatory measures.

Section III**Special Abbreviations and Terms**

This section contains no entries.

Index

This index is organized alphabetically by topic and by subtopic within topic. Topics and subtopics are identified by paragraph number.

Access

- Controls, 2-1, 4-5
- Entry control security procedures, 3-3, 4-5
- Limited, material, and exclusion areas, 4-5
- To keys and locks, 4-5
- To nuclear reactors and SNM, 2-1
- To vital areas, 3-3
- Two-person concept, 2-1, 4-5

Alarms

- Assessment of, 4-6
- Maintenance of, 4-6
- Recording of, 4-6
- Sensors, 4-6
- Status display, 4-6
- Monitoring, 4-6

Ammunition

- Security forces, 4-10

Area

- Clear zone, 4-4
- Limited, 4-4
- Material, 4-4
- Exclusion, 4-4
- Vital, 3-1
- Restricted, designation of, 4-4 Augmentation force
- Composition of, 4-10
- Exercises, 7-7
- Reaction time, 4-10

Batteries, 4-9

Classification

- Of plans, 2-1
- Of SNM, 3-4
- Public release, 2-8
- FOAI, 2-1

Clear zone, 4-4

Communications

- Requirements, 4-6
- Discipline, 4-6

Compensatory measures

- For deviations, 6-4

Construction

- Techniques and materials, 4-4
- Fences, 4-4

Control

- Access and controls to keys and locks, 4-5
- Entry, 4-5
- Entry control rosters, 4-5
- Visitors, 4-5

Deadly force

- Use of force, 2-4

Deviations

- Approval authority, 6-3
- Blanket, 6-3
- Categories of, 6-2
- Compensatory measures, 6-4
- Deviation requests, 6-3
- Purpose, 6-1
- Ten (10) percent, 6-3

Entry control

- Concept, 4-5
- Delay system concept, 4-2
- Facility, 4-4
- Identification badges, 4-5

- Personnel entry, 4-5
- Rosters, 4-5
- Searches and inspections, 4-5
- Security procedures, 4-5
- Vehicle entry, 4-5
- Visitor control procedures, 4-5

Entry control facilities, 4-4

Equipment

- Vehicle/material handling equipment, 4-5
- Vital, 3-1

Exceptions

- (See deviations)

Exclusion area

- Designation of, 4-5
- Entry control, 4-5
- Two-person concept, 4-5

Fences

- Standards and specifications, 4-4

Force on force

- Requirements for, 2-4
- Training, 7-8

FOIA, 2-1

Gates, 4-4

Hostages

- Duress system, 4-5
- Use of force, 2-4

Identification badges, 4-5

Intrusion detection system

- Alarm assessment detection system, 4-6
- Annunciator/display equipment, 4-6
- Automatic switchover to battery power, 4-6
- Test and records, 4-6

Keys

- (See also locks)
- Access and controls, 4-5
- Accountability, 4-5
- Key control officer, 4-5
- Lock rotation, 4-5

Lighting

- Requirements, 4-4, 4-8
- Clear zone, 4-4

Limited area

- Designation of, 4-5
- Entry control into, 4-5
- Vehicles, 4-5

Locks

- (See also keys)
- Combinations to, 4-5
- For perimeter gates, 4-4
- Key and lock controls, 4-4
- Key control officer, 4-4
- Lock rotation, 4-4
- Replacement of, 4-4
- Types of locks, 4-4

Loss of SNM

- (See recovery operations)
- Reporting loss, 2-5

Movement of SNM

- Domestic shipments, 3-2
- Limited area movement, 3-2

Perimeter

- Physical barriers, 4-4
- Clear zones, 4-4
- Entry control facility, 4-4
- Lighting systems, 4-4

- Warning signs, 4-4

Physical security plan

- Classification of, 2-3
- Coordination of, 2-3
- Preparation of, 2-3, app C
- Recovery operations, 5-1
- Requirements for, 2-3

Postulated threat

- Requirement, 2-2, 4-10
- Responsibility for development of, 2-2

Power sources

- Intrusion detection system, 4-9
- Battery, 4-9
- Electric, 4-9
- Generator, 4-9

Recovery operations, 5-1

- Communications, 5-3
- Planning, 5-2
- Practice, 5-2

Response force (RF)

- (See also security forces)
- Composition, 4-10
- Exercises, 7-6
- Training, 4-10, 7-6
- Reaction time, 4-10

Responsibilities

- AMC, 1-5
- FORSCOM, 1-5, 4-10
- Commanders, directors, and custodians, 1-5
- HQDA officials, 1-5
- Key control officer, 4-4
- Badge control officer, 4-4

Restricted areas

- Designation of, 4-4
- Loud speaker, 4-4
- Warning signs, 4-4

Security force

- (See also augmentation force, response force)
- Composition, 4-10,
- Considerations, 6-5
- Concept, 4-10
- Equipment, 4-10
- Training, 2-4, 4-10, 7-1, 7-2, 7-5, 7-6
- Exercises, 4-10
- Use of force, 2-4
- Weapons, 2-4, 4-10

Security planning

- (See also site vulnerability assessment, physical security plan, contingency plan)
- Requirements, 2-1, 4-2
- Threat, 2-1
- Vulnerability assessment, 2-2

Sensors

- Self-test capability, 4-6
- Exterior, 4-6
- Interior, 4-6
- Testing, 4-6 Signs, warning,

Site physical security plan

- Classification of, 2-1
- Plan outline, 2-2
- Requirement for, 2-3
- Threat considerations, 2-2

Site vulnerability assessment

- Conduct of, app B
- Format of, 2-2
- Requirement for, 1-5, 2-2
- Threat assessment, 2-2

Storage requirements

SNM, 3-1

Threat

Analysis, 2-2

Considerations, 2-2, 4-3

Postulated, 2-2

Training

(See security force training)

Two-person concept, 2-1**Use of force**

Requirements, 2-4

Training, 7-2

Vehicles

Control of, 4-4

Searches and inspections, 4-4

Waivers

(See deviations)

Warning signs, 4-4**Weapons**

Requirement for, 2-4

Types, 4-10

Security of, 4-10

Training on, 2-4, 7-9

Unclassified

PIN 047236-000

USAPA

ELECTRONIC PUBLISHING SYSTEM
TEXT FORMATTER ... Version 2.54

PIN: 047236-000

DATE: 08-31-98

TIME: 16:12:24

PAGES SET: 25

DATA FILE: ar190-54.fil

DOCUMENT: AR 190-54

DOC STATUS: NEW PUBLICATION