

~~SECRET//REL TO USA AND NATO~~

①



DoD MANUAL S-5210.41, VOLUME 1

(U) NUCLEAR WEAPON SECURITY MANUAL: THE DoD NUCLEAR WEAPON SECURITY PROGRAM

Originating Component: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics

Effective: August 11, 2016

Change 1 Effective: October 25, 2016

Releasability: Not cleared for public release. Available to authorized users from the DoD Issuances Website on the ~~SECRET~~ Internet Protocol Router Network at <https://www.dtic.smil.mil/whs/directives>.

Reissues and Cancels DoD Manual S-5210.41, Volume 1, "Nuclear Weapon Security Manual: The DoD Nuclear Weapon Security Program," July 13, 2009

Approved by: Arthur T. Hopkins, Principal Deputy Performing the Duties of Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs

Change 1 Approved by: Arthur T. Hopkins, Principal Deputy Performing the Duties of Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs

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

- (U) Implements policy, assigns responsibilities, and prescribes mandatory procedures for the security of nuclear weapons.

~~SECRET//REL TO USA AND NATO~~

Classified by: Vahid Majidi DASD (NM)
Reason: 1.4.0-1.4.0
Declassify On: 20401231

~~SECRET//REL TO USA AND NATO~~

DoDM S-5210.41-V1, August 11, 2016

Change 1, October 25, 2016

- (U) Describes DoD security policy, objectives, and concepts, and prescribes minimum security criteria for protecting nuclear weapons on alert, in storage, in maintenance facilities, in-transit, and in regeneration situations.
- (U) Implements the Nuclear Security Threat Capabilities Assessment (NSTCA), including subsequent updates or replacement threat capabilities assessments (TCAs) as endorsed by the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs (ASD(NCB)); provides security planning guidance; and describe security requirements for selected weapon configurations.
- (U) This volume assigns responsibilities and prescribes procedures for the implementation of the DoD Nuclear Weapon Security Program.

~~SECRET//REL TO USA AND NATO~~

TABLE OF CONTENTS

SECTION 1: (U) GENERAL ISSUANCE INFORMATION.....	6
1.1. (U) Applicability.....	6
1.2. (U) Policy.....	6
1.3. (U) Clarifying Information.....	7
a. (U) Warning Statements.....	7
b. (U) Descriptive Words.....	7
SECTION 2: (U) RESPONSIBILITIES.....	8
2.1. (U) ASD(NCB).....	8
2.2. (U) Director, Defense Threat Reduction Agency (DTRA).....	8
2.3. (U) Director, Defense Intelligence Agency (DIA).....	8
2.4. (U) General Counsel of the Department of Defense.....	8
2.5. (U) Secretaries of the Military Departments.....	8
2.6. (U) CJCS.....	10
2.7. (U) Combatant Commanders With Nuclear Responsibilities.....	10
2.8. (U) Commander, United States Special Operations Command (USSOCOM).....	11
SECTION 3: (U) DoD NUCLEAR WEAPON SECURITY PROGRAM.....	12
3.1. (U//DCNI) Nuclear Weapon Security Standard (NWSS).....	12
3.2. (S//REL TO USA, NATO) Denial Concept.....	12
3.3. (U) Nuclear Weapon Security Principles.....	13
a. (U) Nuclear Weapon Protection.....	13
b. (U) Custody and Control.....	15
c. (U) Personnel.....	15
d. (U) Assessments, Evaluations, and Inspections.....	15
e. (U) Areas Containing Nuclear Weapons.....	15
f. (U//DCNI) Structure and Building Security.....	16
3.4. (U) The DoD Nuclear Weapon Security Program.....	17
a. (U) Security Objectives.....	17
b. (U) Security Concept.....	18
c. (U) Implementing the Nuclear Weapon Security Concept.....	19
3.5. (U) Relationship of Nuclear Security, Safety, Survivability, Use Control, And Effectiveness.....	21
a. (U) Joint DoD and Department of Energy (DOE) Nuclear Surety Policy.....	21
b. (U) DoD Nuclear Weapon System Safety.....	22
c. (U) Survivability.....	22
d. (U) Use Control.....	22
e. (U) Operational Security (OPSEC) and Camouflage, Concealment, and Deception (CCD).....	22
SECTION 4: (U) NUCLEAR WEAPON SECURITY THREAT.....	24
4.1. (U) General.....	24
4.2. (U) Threats.....	24
4.3. (U) Localization of the Threat Capabilities Assessment.....	25

APPENDIX 4A: (U) VULNERABILITY ASSESSMENT (VA) GUIDE.....	26
4A.1. (U) General.....	26
4A.2. (U) Threat and Risks.....	26
a. (U) Assessed Threats.....	26
b. (U) Inherent Risk and Associated Threats.....	26
c. (U) Vulnerability Classification.....	26
4A.3. (U) Procedures for the Conduct of Vulnerability Assessment.....	26
APPENDIX 4B: (U) LOCALIZED THREAT CAPABILITY ASSESSMENT FORMAT.....	31
4B.1. (U) General.....	31
4B.2. (U) Composition.....	31
a. (U) Title.....	31
b. (U) Purpose.....	31
c. (U) Assessment.....	31
d. (U) Findings.....	31
e. (U) Other Considerations From the Assessment.....	32
f. (U) Plausible Attack Scenario Matrix.....	32
g. (U) Overall Risk Assessment.....	32
4B.3. (U) Approval.....	33
SECTION 5: (U) NUCLEAR WEAPON SECURITY PLANNING.....	34
5.1. (U) Site Planning.....	34
a. (U) General.....	34
b. (U) Responsibilities.....	34
c. (U) Planning Considerations.....	34
d. (U) Vulnerability Assessments (VAs).....	35
e. (U) Conduct of Risk Assessments.....	35
f. (U) Risk Management.....	36
g. (U) Systems Approach.....	36
h. (U) National Environmental Policy Act.....	37
i. (U) Safety.....	37
j. (U) Land Requirements.....	37
k. (U//DCNF) Electromagnetic Radiation (EMR) Surveys.....	37
l. (U) Considerations During Research, Development, and Acquisition.....	38
m. (U) Mandatory Implementation.....	38
n. (U) User or Host-Nation and NATO Agreements.....	39
o. (U) Planning Assistance.....	39
5.2. (U) Security Planning.....	39
a. (U) General.....	39
b. (U) Physical Security Plan.....	40
c. (U) Coordination.....	40
d. (U) Integration of Security Methods.....	40
e. (U) Standoff Attack Protective Measures.....	40
f. (C//REL TO USA, NATO) Vulnerability to Small Arms Fire.....	41
g. (U) Airborne and Air Attack Protective Measures.....	41
h. (U) Storage of Nuclear Weapons Components.....	41

i. (U) Control of Training Weapons and Empty Containers.....	41
j. (U) Separation of Nuclear From Non-Nuclear Activities.....	41
k. (U) Construction Activity.....	42
l. (U) Facility and Equipment Maintenance.....	42
m. (U) Site Plans, Drawings, and Documents.....	43
5.3. (U) Security System Design Standards.....	43
SECTION 6: (U) NUCLEAR WEAPON DENIAL	44
6.1. (U) General.....	44
6.2. (U) Concept.....	44
6.3. (U) Denial Systems.....	44
SECTION 7: (U) NUCLEAR WEAPON SECURITY FORCES, EQUIPMENT, AND TRAINING.....	46
7.1. (U) Security Forces.....	46
a. (U) Designated Forces.....	46
b. (U//DCND) Reaction Times.....	49
c. (U//DCND) Area Checks and Patrols.....	50
d. (U) Use of Force.....	50
e. (U) Exercises.....	50
7.2. (U) Security Force Weapons And Equipment.....	51
a. (U) Weapons.....	51
b. (U) Equipment.....	52
c. (U) Vehicles.....	52
7.3. (U) Security Force Training.....	53
a. (U) General.....	53
b. (U) Scope.....	53
c. (U) Specialized Training.....	55
d. (U) Continuing Education.....	56
e. (U) Force-on-Force Training.....	56
f. (U) Additional Training.....	57
(U) GLOSSARY	58
G.1. (U) Acronyms.....	58
G.2. (U) Definitions.....	59
(U) REFERENCES	65

TABLES

Table 1. (U) Plausible Attack Scenario Matrix (Format Example)	32
--	----

SECTION 1: (U) GENERAL ISSUANCE INFORMATION

1.1. (U) APPLICABILITY. This volume:

- a. (U) Applies to the OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the "DoD Components").
- b. (U) Does not abolish or abridge the authority or responsibility of a commander to apply different but equal (or more stringent) criteria and standards during emergencies. Such a change in standards does not abolish the requirement for maintaining U.S. control of nuclear weapons and components. Improvements to storage facilities requiring construction effort or procurement should be accomplished in accordance with Section 5 of Volume 1 and Section 3 of Volume 2 of this manual.
- c. (U) Does not provide protection standards for nuclear command and control (NC2) facilities or special nuclear materials (SNM). Protection standards for NC2 facilities and SNM are provided by DoD Manual (DoDM) S-5210.92 and DoD Instruction (DoDI) O-5210.63, respectively.
- d. (U) Pertains to all nuclear weapons, nuclear weapon systems, and nuclear components for which DoD Components have operational, maintenance, or custodial responsibility.

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

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

(b)(3):10 USC §128

- c. (U) The standards and criteria in this volume are the absolute minimums required to be implemented. Additional security measures may be required as dictated by threat, site configuration, topography, or operational considerations. Combatant Commands and Military Departments are expected to increase security protection as necessary and ensure continuity of efforts between nuclear weapon security and operational missions.

1.3. (U) CLARIFYING INFORMATION.

a. (U) Warning Statements.

(1) (U) This volume is releasable to the North Atlantic Treaty Organization (NATO) as ~~NATO SECRET~~. Disclosure of this volume outside NATO to foreign governments, international organizations, or their official representatives must follow the policy in accordance with DoDD 5230.11.

(2) (U) Certain paragraphs in this volume are classified ~~SECRET//REL TO USA, NATO~~ and ~~CONFIDENTIAL//REL TO USA, NATO~~, and are so marked to protect the information in accordance with the Joint DoD and Department of Energy (DOE) Classification Policy Guide and the original classification authority of the Deputy Assistant Secretary of Defense for Nuclear Matters (DASD(NM)).

(3) (U) The remaining paragraphs of this volume contain UNCLASSIFIED information, some of which is protected as ~~DoD Unclassified Controlled Nuclear Information (DCNI)~~ in accordance with DoDI 5210.83.

(a) (U) The decision to protect this information as ~~DCNI~~ is based on the determination that the unauthorized dissemination of such information could reasonably be expected to have an adverse effect on the health and safety of the public and the security of DoD nuclear weapons, components, and facilities.

(b) (U) Accordingly, users of this volume are prohibited from the unauthorized dissemination of ~~DCNI~~ contained herein regarding U.S. nuclear weapons security policy.

(c) (U) Guidance concerning the authorized release of ~~DCNI~~ information is found in DoDD 5230.11 and DoDD 5230.20.

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

(1) (U) Mandatory guidance that is directive in nature (i.e., use of the words "will" or "must") and provides standards, measures, or actions that are required, and subject to inspection. An inability to meet the requirement in this manual necessitates a request for a deviation as provided for in Section 6 of Volume 2 of this manual.

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

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

SECTION 2: (U) RESPONSIBILITIES

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

- a. (U) Provides management oversight of the DoD nuclear weapons security program.
- b. (U) Maintains and monitors prescribed nuclear security management processes.
- c. (U) Reviews the DoD Component implementation guidance for consistency and compliance with policy stated within in this manual.
- d. (U) Conducts programmatic reviews and management audits of nuclear weapons security processes.

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

- a. (U) Executes the DoD-sponsored nuclear security policy evaluations and activities, including the force-on-force exercise program (MIGHTY GUARDIAN).
- b. (U) Conducts Defense Nuclear Surety Inspection Oversight on behalf of the CJCS in accordance with CJCS Instruction (CJCSI) 3263.05B.
- c. (U) Conducts an annual DoD nuclear weapons security deviation analysis and provides a report of the analysis to the DASD(NM).

2.3. (U) DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA). Under the authority, direction, and control of the Under Secretary of Defense for Intelligence and in accordance with DoDD 5105.21, the Director, DIA, annually reviews and updates relevant TCAs, as necessary.

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

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

- a. (U) Implement this volume and make it part of their normal assurance and assessment process, including DoD Component Inspector General assessments as specified in Section 5 of Volume 2 of this manual.
- b. (U) Use this manual with DoDD O-5210.41 and the NSTCA as the primary nuclear weapon security planning references.
- c. (U) Plan and program for the resources needed to properly execute the nuclear weapon security standard at all nuclear weapon locations and operating environments, in accordance with Section 3 of this volume. Size, organize, train, arm, and equip location specific response forces (RFs) and initial and subsequent backup forces (BFs) to maneuver as tactical elements in a combined force, capable of defeating an adversary force in those situations that threaten or affect the security of nuclear weapons.

(b)(1)

- (1) (U) Weapons location.
- (2) (U) The configuration in which the weapons are maintained (e.g., storage, transport, maintenance, on alert).
- (3) (U) The nature and capabilities of potentially hostile forces.
- (4) (U) The reliability and capabilities of personnel responsible for working with or protecting nuclear weapons.

(b)(1)

- f. (U) Provide a security concept of operations for new or modernized security systems (e.g., electronic security system (ESS) or subsystem, entry control and circulation control system or subsystem, area protection system or subsystem, facility protection system or subsystem, weapon movement protection system or subsystem, security force composition, or response times) to the ASD(NCB) for review.
- g. (U) Adhere to the minimum security criteria and standards for denying unauthorized access to nuclear weapons prescribed in this volume.
- h. (U) Comply with the concepts and procedures, described in detail in this manual, for denying unauthorized access to nuclear weapons and implement procedural requirements immediately.

SECTION 2: (U) RESPONSIBILITIES

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

j. (U) Develop and distribute supplementary instructions, when necessary, to provide for Military Department-specific requirements within their respective Military Departments. Two copies of any additional guidance issued by the Military Departments will be forwarded to the DASD(NM), under the ASD(NCB), through the CJCS, within 30 days of publication and after each subsequent change.

k. (U) Direct and ascertain compliance that improvements to storage facilities requiring construction or procurement are accomplished in accordance with Section 5 of this volume and Section 3 of Volume 2 of this manual.

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

2.6. (U) CJCS. The CJCS:

a. (U) Prescribes procedures for the conduct of the nuclear surety inspections as described in CJCSI 3263.05B.

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

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

d. (U) Supports the EMBER IMMUNE and MIGHTY GUARDIAN programs.

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

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

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

c. (U) Coordinate the development of plans and procedures to recover lost, stolen, or missing nuclear weapons or nuclear weapon components.

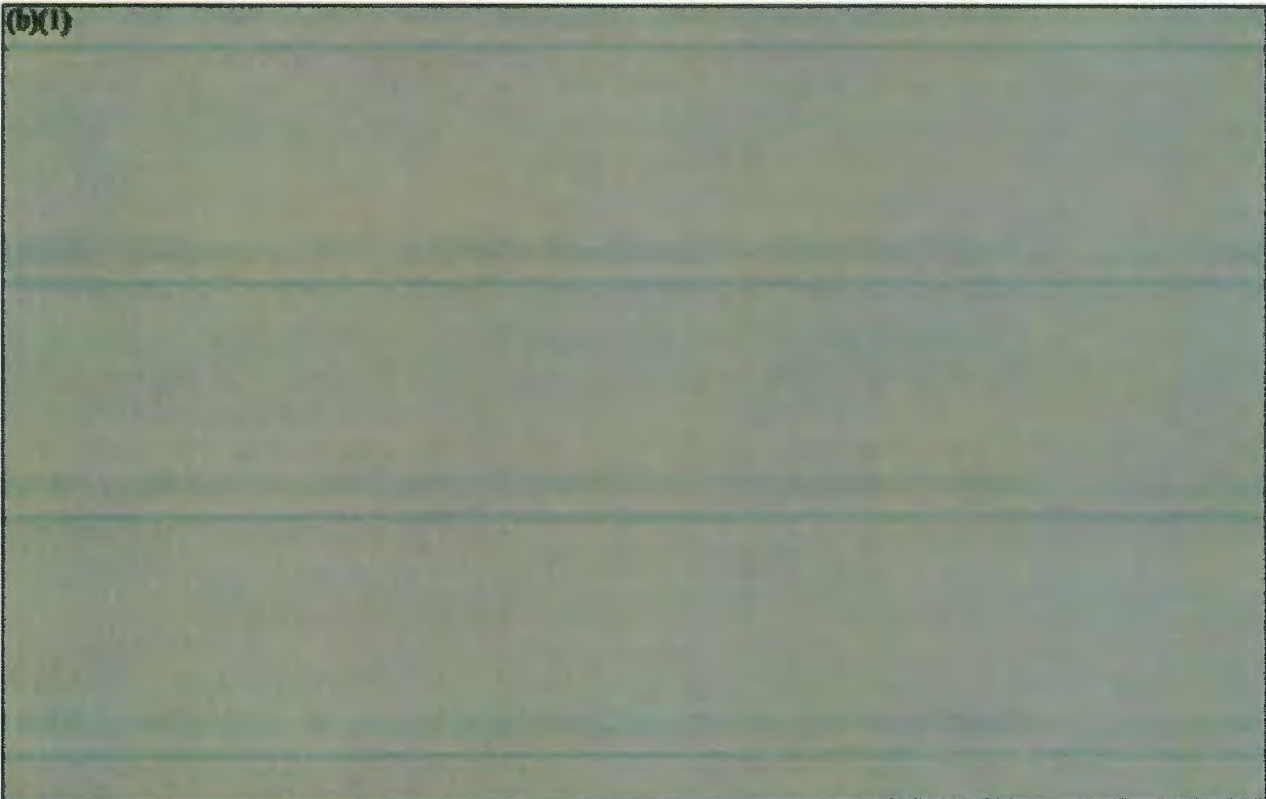
d. (U) Advocate for emerging nuclear security requirements submitted by DoD organizations by giving due analysis and consideration including these requirements in the integrated priority lists.

SECTION 2: (U) RESPONSIBILITIES

e. (U) May issue supplementary instructions, when necessary, to provide for unique requirements within their commands. Any supplemental instructions issued by the Combatant Commanders will be forwarded to the DASD(NM), through the CJCS, within 30 days of publication and after each subsequent change.

f. (U) Support the EMBER IMMUNE and MIGHTY GUARDIAN programs.

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



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

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

h. (U) In coordination with the USD(AT&L), specifies the capacity in which contractors may be used before each MIGHTY GUARDIAN exercise.

SECTION 2: (U) RESPONSIBILITIES

SECTION 3: (U) DOD NUCLEAR WEAPON SECURITY PROGRAM

(b)(3):10 USC §128



(b)(1)



(b)(3):10 USC §128



c. (U) Delay and denial systems should be designed to integrate with and support the overall security system while contributing to the security concepts of deterrence, detection, delay, denial, and defeat of potential adversaries.

(1) (U) Denial systems must be developed, tested, evaluated, and fielded to meet the provisions outlined in Section 6 of this volume. When considering which denial systems to implement, national laws that impact selective denial system implementation must be accounted for, as described in Paragraph 5.1.n. of this volume.

(2) (U) Delay systems must be developed, tested, evaluated, and fielded to increase adversary task time for achieving unauthorized access to nuclear weapons to the greatest extent possible.

(3) (U) The collective incapacitating, non-lethal, or lethal effects (as applicable) of denial systems and the impeding effects of delay systems will be assessed through formalized certification testing and must consider MIGHTY GUARDIAN or other DoD-sponsored nuclear security force-on-force exercise data (where available), modeling and simulations, and engineering studies.

(a) (U) Such assessments are necessary to support recommendations for the consideration of policy changes in security forces size and response times.

(b) (U) DASD(NM) will review formal certification test data for these systems and issue changes as appropriate. All major changes to the security system must be coordinated with DASD(NM).

3.3. (U) NUCLEAR WEAPON SECURITY PRINCIPLES.

a. (U) Nuclear Weapon Protection.

(b)(1),(b)(3):10 USC §128



(b)(3):10 USC §128



(4) (U) Commanders responsible for the implementation of the NWSS will prevent unauthorized access, damage or sabotage, unauthorized destruction, loss of control, capture or theft, and unauthorized use of nuclear weapons, nuclear weapon systems, and Military Department- or Nuclear Weapon System Safety Group-designated critical components during all phases of their life cycles.

(5) (U) Whenever there is indication of an increased threat in an area where nuclear weapons are located, Commanders will take additional security measures appropriate to the threat to ensure adequate protection and coordinate these additional measures with applicable headquarters and commands. While considering operations security (OPSEC), Commanders will coordinate applicable additional measures with local law enforcement officials, as necessary.

(b)(3):10 USC §128



(7) (U) Facilities containing nuclear weapons must be opened only when necessary for operations (including alarm system testing), required maintenance, inventory, weapon movement, inspections and, in some instances, training.

(8) (U) Safety and survivability of nuclear weapons must be significant considerations in the design of security systems.

(9) (U) Site-specific plans must be developed and exercised to fulfill the NWSS. These plans must describe the means for preventing unauthorized penetration of limited and exclusion areas containing nuclear weapons and methods to ensure the recapture or recovery of the weapon

in the event of capture or removal by unauthorized persons. Plans will be coordinated following Military Department and Joint Staff procedures.

b. (U) Custody and Control. Commanders will maintain complete and positive physical U.S. custody and control of nuclear weapons at all times unless transfer is authorized by a competent authority.

c. (U) Personnel. Personnel who are selected to perform nuclear weapon duties must demonstrate the highest levels of integrity and dependability. These personnel will be assigned to designated DoD Reliability Assurance Program (RAP) positions, or a host-nation equivalent, and will be evaluated for adherence to RAP standards, as described in DoDM 5210.42. The RAP aids in mitigating certain threats, as discussed in Section 4 of this volume and the NSTCA.

d. (U) Assessments, Evaluations, and Inspections.

(1) (U) Commanders having responsibility for the protection of nuclear weapons must periodically (at a minimum, annually) assess the possible threats to nuclear weapons, whether in storage, maintenance, in transit, or on operational launch platforms. These assessments will be used to upgrade security plans, procedures, tactics, and OPSEC measures. Whenever risks become evident, they must be elevated to senior leaders, so that effective decision making and resource allocation can be accomplished in accordance with Section 6 of Volume 2 of this manual.

(2) (U) Security measures for the protection of nuclear weapons, including security forces, facilities, equipment, systems, plans, and procedures, must be thoroughly examined during appropriate inspections and staff visits by representatives of the Combatant Commands, the Military Departments, and DTRA.

(a) (U) Inspections and visits will focus primarily on whether the security program can meet the NWSS under the scenarios represented by the DIA, localized TCA, and local threat assessments (i.e., "performance-based standards").

(b) (U) Inspections and visits also will assess the security program's ability to meet the technical requirements of this volume (i.e., "criteria-based standards"). When this manual's criteria based security standards cannot be met and a deviation is required, aggressive compensatory measures will be implemented to meet the NWSS.

(3) (U) Once developed, local security plans should be validated through modeling and simulation technologies provided by the managing Military Department.

e. (U) Areas Containing Nuclear Weapons.

(1) (U) Nuclear weapons must be secured in exclusion areas within limited areas.

(2) (U) Limited and exclusion areas must encompass the smallest practicable amount of geographical space consistent with operational and explosives safety requirements in order to eliminate requirements for securing and maintaining unnecessary terrain. When reducing the

size of these areas, ensure sufficient distance between the perimeter barriers and the weapons to aid the RF in interception and neutralization of intruders prior to their gaining unauthorized access to a nuclear weapon.

(3) (U) The most secure modes available must be used for the storage, maintenance, and transportation of nuclear weapons. Nuclear weapons must not be stored routinely in above-ground maintenance and inspection (M&I) facilities.

(a) (U) Temporary storage is permitted when a weapon is in a normal maintenance processing flow; however, this will only be done when absolutely necessary.

(b) (U) Effective compensatory measures are required to ensure access denial is provided in these temporary facilities, which normally do not have access denial features.

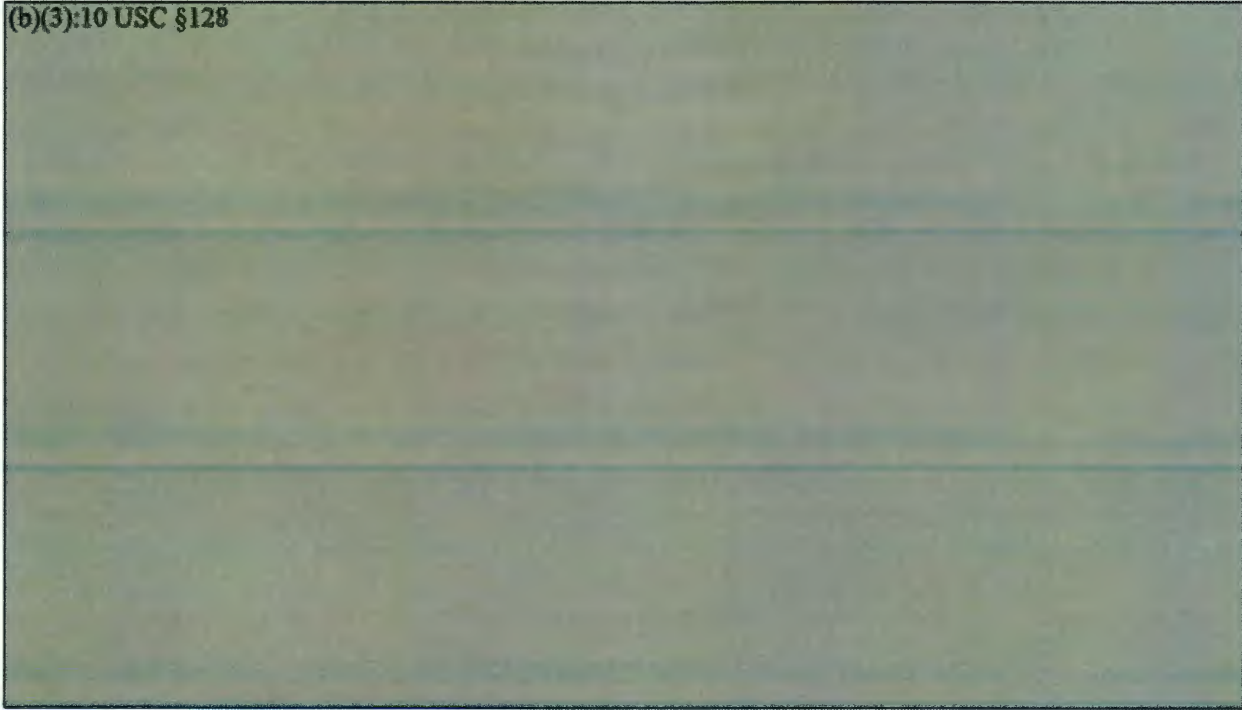
(c) (U) Wing and Strategic Weapons Facility commanders responsible for the protection of nuclear weapons who exercise temporary storage options must state their policies regarding the acceptance of additional risk in these instances in writing.

(4) (U) Facilities and procedures must be established to ensure positive control of all personnel and vehicles authorized to enter and depart limited and exclusion areas. Additionally, security systems and procedures must be established to control the movement of persons and vehicles within the limited and exclusion areas and to detect unauthorized acts or procedures.

(b)(3):10 USC §128



(b)(3):10 USC §128



3.4. (U) THE DoD NUCLEAR WEAPON SECURITY PROGRAM. Nuclear weapon security is systems-based and employs an integrated collection of components or elements designed to achieve the final objective of preventing or defeating the overt and covert actions of an adversary. This is achieved through implementation of the DoD Nuclear Weapon Security Program.

a. (U) Security Objectives. The DoD Nuclear Weapon Security Program is designed to:

- (1) (U) Deny unauthorized access to nuclear weapons.
- (2) (U) Prevent damage or sabotage to nuclear weapons.
- (3) (U) Prevent loss of control of nuclear weapons.
- (4) (U) Prevent an unauthorized nuclear detonation.
- (5) (U) Prevent, to the maximum extent possible, radiological contamination caused by unauthorized acts or damage, emergency destruction actions, or security force actions. Security forces must not let the concern over possible contamination deter their actions to neutralize an adversary.
- (6) (U) Ensure weapons are operationally available to the President of the United States.

b. (U) **Security Concept.** The concept for protection of nuclear weapons mandates that the security system stops an intruder **before** they achieve unauthorized access to a weapon.

(1) (U) Stopping an intruder before unauthorized access is accomplished through an integrated defense-in-depth approach, which includes:

- (a) (U) Physical security technologies deployed from the weapon outward.
- (b) (U) Implementation of planned actions to disrupt adversary planning cycles.
- (c) (U) Immediate response and action by dedicated and well-trained security forces.
- (d) (U) Additional security measures deployed at and beyond the security site perimeter.

(2) (U) As an integral part of the security system, the security force must be sized, organized, armed, equipped, trained, and tactically employed to meet the NWSS.

(3) (U) The security concept is implemented through interrelated, interlocking and supporting capabilities, principles and practices designed to protect nuclear weapons from unauthorized access, theft, damage or destruction, sabotage, or unauthorized use. This concept must contribute to a defense-in-depth approach that supports the capabilities of detection, delay, denial, and defeat of an adversary, thereby providing a deterrent capability. Correct design of a security system will **deter** a potential adversary by projecting an image of a robust, capable system that includes **detection** and immediate assessment of any attempted breach of a protected area, **delay** of an adversary's progress toward a nuclear weapon while **denying** unauthorized access to the weapon and **defeating** the adversary force in the tactical engagement. This is achieved through a defense in-depth strategy that starts at each and every nuclear weapon and builds outward in an expanding series of security checks, detection capabilities, physical security barriers of delay and denial; and a mix of static and mobile lethal response forces to engage threats and overwhelmingly defeat an adversary while maintaining an effective capability to recapture and recover any nuclear weapon which is lost.

(a) (U) **Detection.** Detection is achieved through effective entry control, vigilant patrolling, and observation supported by a suite of sensors and assessment devices specifically engineered and designed for the nuclear weapon security environment supported. It involves sensing the action as far away from the nuclear weapon as possible, assessing it, and reporting it to a control center or tactical control element. The ability to counter an attack is predicated upon detecting it in time to react. Once a threat is detected, it must be delayed and denied so the security force has enough time to respond, engage, and defeat it.

(b) (U) **Delay.** The adversary's path to a nuclear weapon is a function of time and is affected by the speed, distance, barriers, and mission tasks necessary to achieve unauthorized access. Effective barriers and security force employment effectively impede and delay a threat's ability to progress toward the nuclear weapon upon detection. Delay features slow and impede threats, thereby increasing the time it takes the threats to reach a nuclear weapon. This capability

should penalize a threat's task time by causing the threat more time to reach a weapon than the time it takes the security force to respond, interdict, and defeat the threat. Delay features employed before a threat is detected don't effectively contribute to delay as they provide no additional time for a response force to react.

(c) (U) Denial. Denial is achieved through the employment of cumulative layers of delay features employed before reaching a protected area and designed to ensure an adversary is slowed, fixed in place, limited in maneuver and ultimately engaged and defeated by responsive security forces.

(d) (U) Defeat. The security force must be sized, equipped, armed, designed, and organized to survive and prevail while tactically maneuvering to decisively engage and defeat or remove any threats from areas containing nuclear weapons. Effective defeat is necessary should deterrence fail. Effective defeat ensures an adversary will fail and the NWSS will be met in all circumstances.

(e) (U) Deterrence. Proper design, execution, and employment of an effective security system employs detection, delay, denial, and defeat capabilities, resulting in a robust defense against threats. This in turn influences an adversary's decision to forgo actions they may otherwise attempt based on perceived benefits when compared with likely costs or consequences. Activities normally taken by a security force and visible to a potential threat actor help to discourage adverse actions. Deterrence is an overarching capability applicable across all nuclear weapon environments and configurations. Deterrence is achieved through the robust application of the capabilities of detection, delay, denial, and defeat.

c. (U) Implementing the Nuclear Weapon Security Concept. Applying successively more aggressive security measures requires maximum reliance on physical security systems to achieve the stated security objectives. Strong security measures include the area protection system, the facility or weapon system protection system, the entry and circulation control system, and the transportation protection system. Security forces also form an integral part of these security measures. The entire security system must protect the weapons for a period of time longer than the minimum adversary access time (as determined by validated force-on-force evaluations, engineering studies, and modeling and simulation). This protection also must be longer than the designated security force response times to prevent unauthorized entry access, or sabotage perpetrated by personal acts; bulk demolitions; hand, power and thermal tools; and forced entry explosive devices, including standoff attacks, identified as plausible attack scenarios.

(1) (U) Area Protection System. This system protects the limited area, a designated area immediately surrounding one or more nuclear weapon exclusion areas. Components of the area protection system are:

(a) (U) Perimeter Boundary Barrier Subsystem. Boundary barriers prevent inadvertent entry into the limited area, preclude or provide initial delay against unauthorized entry, and facilitate detection and assessment.

(b) (U) Perimeter Boundary Detection Subsystem. The boundary detection subsystem is designed to detect and warn of the presence of possible threats or intruders and attempts at unauthorized entry at or shortly after the time of occurrence. It must include an intrusion detection system (IDS) and clear zones.

(c) (U) Perimeter Boundary Assessment Subsystem. The assessment subsystem is designed to permit near-real-time determination of whether an alarm event is hostile or non-hostile and to assist in localizing and identifying an unauthorized intrusion or activity before the boundary is breached.

(d) (U) Perimeter Area Lighting Subsystem. The area lighting subsystem is designed to provide adequate illumination of the area perimeter, entry control points, the outer clear zone, the area between the fences, and the inner clear zone during darkness and periods of reduced visibility.

(e) (U) Area Command and Control Subsystem. Command and control, through diverse, redundant, and encoded communications, ensure that all countermeasures (electronic and human) are operational, coordinated, informed, and contribute to assessing, preventing, and delaying or containing attempted penetrations or other hostile acts. The Site Security Control Center (SSCC) is the center for command, control, and communications.

(b)(1)



(a) (U) Facility Barrier Subsystem. The facility barrier subsystem, such as doors and locks, in conjunction with other site and facility barrier and delay and denial systems, is intended to prevent unauthorized entry, access, or damage to any weapons for the assessed time based on available data (see Paragraph 4A.3.d.(7) of Appendix 4A of this volume) and the threat as identified in the local TCA.

(b) (U) Facility Detection Subsystem. The facility detection subsystem (e.g., IDS) is intended to detect and provide warning of unauthorized attempts to penetrate the boundary of an internal nuclear weapon facility or group of facilities.

(c) (U) Facility Delay Subsystem. Delay subsystems, such as concrete blocks of sufficient weight to require material handling equipment for their movement, together with the facility barriers and active security measures, impede intruder efforts to gain unauthorized access to or cause damage to weapons.

(d) (U) Facility Denial Subsystem. Denial subsystems may be either lethal or nonlethal and based upon technologies such as laser, microwave, sound, remotely operated weapons, various projectile launching munitions, or other technologies that will stop or incapacitate intruders before they achieve unauthorized access.

(e) (U) Facility Assessment Subsystem. The objective of external facility assessment subsystems, such as closed circuit television or sentries, is to be able to determine, in near-real time, the activities of intruders should they reach the storage facility.

(3) (U) Entry and Circulation Control System. The entry control system provides for identification and control of all personnel and vehicles authorized entry into the limited and exclusion areas. In addition to entry control, control and monitoring of personnel movements and action within the limited and exclusion areas is essential. The limited area entry control facility, part of the area boundary barrier subsystem, may consist of a gate house, personnel entry gate, entry control portals, which may be automated with equipment approved by the Military Department, and a vehicle entrapment area with gates and crash barriers.

(b)(3):10 USC §128

(5) (U) Security Forces. As an integral element of all weapon security systems, security forces assigned nuclear weapon security responsibility will be composed of an RF (which includes the security response team (SRT)); an initial BF; and subsequent BFs, as needed.

(a) (U) The minimum size and composition of security forces for various weapons and weapon configurations is described in Volume 3 of this manual.

(b) (U) To reflect the mission, enemy, terrain and weather, troop availability, time availability, and civil considerations (METT-TC) variations at each location, the force size and composition requirements include the statement "or more" to reflect that local circumstances may require additional security forces to properly support the currently deployed physical security technologies in order to deny unauthorized access to a weapon.

(c) (U) RFs and BFs will be sized, organized, trained, armed, and equipped to maneuver as tactical elements, and as a combined force and be capable of defeating an adversary force in those situations that threaten or effect the security of nuclear weapons.

3.5. (U) RELATIONSHIP OF NUCLEAR SECURITY, SAFETY, SURVIVABILITY, USE CONTROL, AND EFFECTIVENESS. Nuclear weapons physical security (NWPS) is closely intertwined with the concepts for nuclear safety, survivability, use control, and effectiveness.

a. (U) Joint DoD and DOE Nuclear Surety Policy. Nuclear surety includes nuclear weapon system safety, security, control, and effectiveness. In developing and maintaining a nuclear deterrent, the DoD, with the DOE, protects the security of the United States in a manner consistent with health, safety, and environmental needs in accordance with the DoD and DOE "Joint Policy Statement on Nuclear Weapons Surety." Accordingly, nuclear surety will be evaluated throughout the entirety of each nuclear weapon system's life cycle.

b. (U) **DoD Nuclear Weapon System Safety.** Nuclear weapon system safety provides for the protection of nuclear weapon systems against risks inherent in the environment and is achieved through the DoD Nuclear Weapon System Surety Program, as set forth in DoDD 3150.02.

c. (U) **Survivability.** Nuclear forces need to survive in order to be available, if called upon, to execute their nuclear mission. In many instances security measures enhance survivability and vice versa. In other instances, security measures tend to increase the vulnerability of the force to detection and attack. During transition to war and wartime, commanders should weigh the alternatives and tradeoffs between survivability and security (S2) when determining the security posture and measures for nuclear weapons and forces. The Chemical, Biological, Radiological, and Nuclear Survivability Policy is described in DoDI 3150.09.

d. (U) **Use Control.** Use control is applied through a combination of design features, procedures, and safety rules.

e. (U) **OPSEC and Camouflage, Concealment, and Deception (CCD).** The attainment of surprise and security is essential for military effectiveness, and it requires concealment of capabilities and intentions. OPSEC is the primary means of achieving this goal.

(1) (U) Commanders must ensure that unclassified but sensitive information related to nuclear operations and security (e.g., weapons movements, weapons maintenance schedules) is kept from open source mediums such as the Internet. They must also ensure any such information already posted or disseminated is removed and kept from open source mediums. This information must be marked and protected as DCNI, where appropriate.

(2) (U) Information about weapons maintenance and other activities must be limited and restricted to those having a need to know in order to perform their official duties.

(3) (U) CCD is a supporting technique for achieving OPSEC and for enhancing S2. Commanders will conduct site security and operations involving nuclear weapons in such a manner as to reduce or eliminate, as much as possible, a potential adversary's ability to collect audio or visual intelligence data.

(4) (U) Methods for reducing foreign intelligence service, terrorist, and domestic agitator group intelligence gathering include:

(b)(1)



(b)(1)



SECTION 4: (U) NUCLEAR WEAPON SECURITY THREAT

4.1. (U) GENERAL.

(b)(1)

b. (U) Senior officials must ensure that security keeps pace with changing security environments, especially the threats posed by foreign intelligence services, transnational groups, national groups, and terrorists, as well as opportunities afforded by new technologies. Commanders at all levels are responsible for meeting the NWSS. The NSTCA, which outlines potential adversary capabilities, is the strategic planning tool used to develop and modify security systems to counter plausible threats. Upon release of updates to the NSTCA or new intelligence community assessments, the DASD(NM) will forward planning implementation instructions to the Military Departments for inclusion in the localized TCA referenced in Paragraph 4.3.

c. (U) Security efforts must be concentrated to counter adversary capabilities. Because adversary intent is unpredictable and dependent on possessing the capability to execute a particular function, adversary intent is not the driving factor. Similarly, the opportunity for an adversary to complete an attack successfully is countered by the sum total of the effectiveness of the entire security system, including force protection, installation information, personnel, communications, cyber, and other security functions. Countering assessed and projected adversary capabilities is the cornerstone of an effective NWPS program. Units with a nuclear weapon security responsibility will use Appendix 4A of this volume to conduct vulnerability assessments in their effort to counter adversary capabilities.

4.2. (U) THREATS.

(b)(1)

b. (U) An adversary force attempting to seize, destroy, or detonate a nuclear weapon will size itself according to its objective and an assessment of the target's vulnerabilities and defenses.

(b)(1)

(b)(1)

4.3. (U) LOCALIZATION OF THE THREAT CAPABILITIES ASSESSMENT.

a. (U) Threat capabilities and actors evolve and change. For nuclear weapon security planning purposes, the NSTCA provides a baseline assessment based on adversary-assessed capabilities. It is not an exhaustive list of ways an adversary can attack a nuclear weapon environment or attempt to gain unauthorized access to a weapon. Therefore, the base document must be tailored by Military Department, Combatant Command, and unit security and intelligence planners including local factors of METT-TC. The capabilities, tactics, and courses of action assessed in the NSTCA will be included in the localized TCA. Upon release of updates to the NSTCA or upon release of new intelligence community assessments, the DASD(NM) will forward planning implementation instructions to the Military Departments.

(b)(3):10 USC §128

d. (U) The local threat assessment team should attempt to identify additional plausible attack scenarios based on their local METT-TC factors. These additional scenarios should become a component of the localized TCA.

e. (U) Military Departments must develop threat assessment review and approval procedures as part of the localization of the NSTCA. At a minimum, the flag officer responsible for approving deviations to security criteria, as defined in Section 6 of Volume 2 of this manual, will review the threat assessments. The Supported Commander in accordance with the Unified Command Plan and the geographic Combatant Commanders where nuclear forces operate within their areas of responsibility will receive copies of the review.

Appendix 4A: (U) VULNERABILITY ASSESSMENT (VA) GUIDE

4A.1. (U) GENERAL. Commanders will ensure VAs are conducted at nuclear weapon operating locations and maintenance and storage facilities, as well as of associated weapon and logistics movement routes, to:

a. (U) Determine the facility's vulnerability to sabotage, stand-off attack, theft, loss, seizure, or unauthorized access by external and internal threats. Vulnerability testing of IDS that support nuclear weapon environments is a necessary part of any VA. Procedures for conducting IDS vulnerability testing are contained in Section 3 of Volume 2 of this manual.

b. (U) Identify vulnerabilities.

4A.2. (U) THREAT AND RISKS.

a. (U) **Assessed Threats.** The NSTCA, as well as the localized TCA, will be used as the basis for determining the facility's vulnerability to threats from external and internal sources.

b. (U) **Inherent Risk and Associated Threats.** The associated threats to and inherent risks for nuclear weapons will be considered in establishing priorities for countering identified vulnerabilities.

c. (U) **Vulnerability Classification.** Vulnerabilities associated with a specific nuclear site are classified. Follow the appropriate classification guidance as provided by the applicable Military Department or Combatant Command responsible for the nuclear weapon.

4A.3. (U) PROCEDURES FOR THE CONDUCT OF VULNERABILITY ASSESSMENT.

a. (U) Conduct the VAs annually, or more frequently as new vulnerabilities become apparent. Use the annual force protection vulnerability assessment to assist in completing the nuclear mission specific analysis. Military Departments should consider scheduling a DTRA-conducted, balanced survivability assessment to assist in identifying vulnerabilities. Document specific actions taken to eliminate or mitigate identified vulnerabilities.

b. (U) DoD Components should ensure timely completion and submission of VAs, updates, and reviews, in accordance with component guidance. Military Departments will establish a higher headquarters review process for nuclear VAs. At a minimum, the flag officer responsible for approving deviations as defined in Section 6 of Volume 2 of this manual must review the VA for each nuclear location in his or her command.

c. (U) VA team composition:

(1) (U) The Military Department responsible for the nuclear weapon defines the process by which the VA team is formed. The VA should be accomplished by a team consisting of members with expertise in the following areas:

- (a) (U) Installation security forces, operations functions, and maintenance functions.
- (b) (U) Safety and health physics.
- (c) (U) Security and intelligence.
- (d) (U) Special operations forces.
- (e) (U) Protective design.
- (f) (U) Cyber threat.

(2) (U) The commander concerned will designate the team leader, and all members of the team will coordinate documentation.

d. (U) Conducting the VAs.

(1) (U) The VA team leader should brief the VA team on the purpose and scope of the VA and threats to nuclear weapons at the operating location or facility.

(2) (U) Detailed briefings should be provided on the nuclear weapon operating location, maintenance or storage facility, or weapon movement routes (i.e., the target(s) being assessed) and results of applicable force-on-force exercises.

(3) (U) The VA team should review all applicable defense plans and pertinent standard operating procedures.

(4) (U) The VA team should review maps, functional schematics, and engineering drawings of facility equipment, communications, and structures.

(5) (U) The VA team should conduct a tour of the target location and surrounding area to become knowledgeable of the configuration, terrain, supporting security systems, security forces, and technical operational activities. During the tour, the team should identify specific vulnerabilities from external and internal threats. The team should:

- (a) (U) Observe day and night operations.
- (b) (U) Interview personnel, as appropriate.
- (c) (U) Observe demonstrations of equipment and procedures.
- (d) (U) Note how the security systems are utilized, including security forces

and BFs.

(e) (U) Ask "what if" questions with reference to the possibility of covert or overt acts by insiders (e.g., "What if an entry controller allows an unauthorized person or device to bypass the entry control system or an alarm monitor fails to acknowledge a valid alarm?"). Concentrate on means to bypass, subvert, overwhelm, or interrupt elements in the security systems, or the two-person rule system.

(f) (U) As part of the terrain walk around the target location, note most likely avenues of approach, areas providing concealment, fields of fire into the location, and probable strong points for attackers.

(6) (U) After the physical and operational layout of the target location is well known, team personnel should assume the role of the overt and covert attacker and conduct war-game attacks against the security system.

(7) (U) The VA team should develop and document plausible attack scenarios for each target by considering the vulnerabilities noted and the stated threats. The chance of adversary success is evaluated by identifying critical pathways to the target. More than one scenario may be applicable. Each scenario should be developed by utilizing two-party, adversary, and defender gaming approaches. Together, the two parties choose credible paths and actions for the adversaries as well as plausible responses by the security system. Following documentation, the team should review each scenario, conduct a physical walk through, and possibly develop additional scenarios or refine those already developed.

(8) (U) The VA team should develop and document conclusions and recommendations while following appropriate security classification guidance. The documentation should identify the vulnerabilities found and recommend specific actions or identify required capabilities necessary to eliminate or reduce the vulnerabilities.

(a) (U) Conclusions should express results that follow logically from the VA.

(b) (U) Recommendations must support conclusions.

(c) (U) The commander concerned should make a formal risk decision based on the conclusions and recommendations made by the VA team. Each identified vulnerability and recommended corrective action will be addressed.

e. (U) Sample VA format (This format is a guide only. VA teams may modify the format as appropriate.):

(1) (U) Introduction.

(a) (U) Purpose. Describe what the VA is being used for and how it is being applied.

(b) (U) Scope. Describe what facilities are included in the VA.

(c) (U) Site Description. Give a brief description of the site and include maps of the site and surrounding area.

(d) (U) Site Mission. Give a brief description of the site mission.

(e) (U) Security Interests. Identify specific areas that contain security interests. Address any security interests that were not considered and why they were not considered.

(2) (U) Identification and Description of Potential Threats. Address what specific threats apply to the site according to the requirements. Be specific; do not just reference existing guidance. Specify likely threat objectives, threat tactics, and tools, explosives, and weapons that the threat could use in the attack execution. Describe what threats were considered and eliminated and why they were eliminated. Cover:

(a) (U) Insider adversaries.

(b) (U) Outsider (external) adversaries.

(c) (U) Insider or outsider collusion.

(d) (U) Airborne threats.

(e) (U) Cyber threats.

(3) (U) Characterization of Security Systems. Describe the physical protection, access controls, and multi-element protection measures in place to protect target locations from the threat spectrum. Characterization should be specific to all protection in place relative to facility targets, exclusion, and limited areas.

(4) (U) Target Identification. Identify target items in each area. Describe potential adversary acts for each target (i.e., sabotage, theft, loss, seizure, unauthorized access or use).

(5) (U) Identified Vulnerabilities. Describe the specific vulnerabilities for each target identified during the VA.

(6) (U) Scenarios Developed.

(a) (U) Describe in detail the plausible scenarios that were developed for each target for the specific threat spectrums.

(b) (U) Describe what performance tests were conducted to evaluate the facility or site security systems.

(c) (U) Provide a recapitulation of security systems probabilities, barrier delay times, adversary target task times, security force response times, and security force neutralization times.

(7) (U) Conclusions and Recommendations. Set forth the conclusions and recommendations developed during the VA. Conclusions should express results that follow logically from the VA. Recommendations should support conclusions, and should be designed to reduce scenario likelihood of success for each identified vulnerability.

(8) (U) Commander's Decisions on Conclusions and Recommendations. Each identified vulnerability and recommended corrective actions should be addressed.

(9) (U) Team Composition. Include the names and position titles of the members of the VA team who conducted the assessment, along with their unit of assignment and area of expertise.

(10) (U) Signature. Commander's signature and forwarding for higher headquarters review and action, as appropriate.

Appendix 4B: (U) LOCALIZED THREAT CAPABILITY ASSESSMENT FORMAT

4B.1. (U) GENERAL. The NSTCA must be localized to each nuclear weapon environment at each storage or operational location. The localized TCA must be formatted as set forth in this appendix. Local variations to reflect uniquely local environments or situations are expected and encouraged. Individual elements of information as well as overall classification markings will be necessary and should be included. Tailoring the NSTCA should be done by the Force Protection Threat Working Group (including civil agencies) and modified as necessary for the nuclear mission. Outside the continental United States (OCONUS) units must involve host-nation counterparts. Limitations due to restrictions on classified information distribution to host nations will be raised to the respective Military Department and Combatant Commands for resolution in accordance with Volumes 1-4 of DoDM 5200.01. Limitations that the Military Departments cannot resolve will be raised to DASD(NM) through the Joint Staff for resolution.

4B.2. (U) COMPOSITION.

a. (U) Title. "(Installation Name) Nuclear Security Threat Capability Assessment"

b. (U) Purpose. Include the requirement of the NSTCA to be localized and include a reminder that the localized product must be used in conjunction with the NSTCA or other TCA product, as directed by DASD(NM).

c. (U) Assessment. Reflect the NSTCA assessment of the overall threat to the DoD Nuclear Weapons Program, the date(s) during which the localized TCA assessment was conducted, the locally assessed level of the threat to the local Nuclear Weapons Program, and the overall approach implemented to conduct the local assessment. Include the local assessment of the most likely overall threat size and, if applicable, a minimum and a maximum assessed threat group size.

(1) (U) Threat Assessment Core Group Membership. Include the names and position titles of the members of the threat assessment team core group assigned by the Force Protection Threat Working Group, who conducted the assessment, along with their unit of assignment and area of expertise. At least one member of the core group should have experience in intelligence warning, indications, and threat analysis and one member have experience in cyber security.

(2) (U) Threat Assessment Core Group Threat Groups. List the threat groups identified by the NSTCA and any others identified by local authorities. This list represents the threat groups that the local assessment team reviewed to determine the threat capabilities considered in their assessment.

d. (U) Findings. List the team's findings and assessments by individual threat group (as identified in Paragraph 4B.2.c.(2) of this appendix). This should include a rating and validation process that rates each terrorist group outlined in the NSTCA and any others identified by the

local core group. It also should include a determination of which group(s) is most likely to attempt to gain unauthorized access to a nuclear weapon in each environment specific to the local environment(s). The team should rate each threat group using the categories: Composition, Presence, Targeting, Intentions, and History. The team should attempt to identify additional plausible attack scenarios based on local METT-TC factors. These additional scenarios should be combined with those from the NSTCA into a master attack scenario matrix and become a component of the localized TCA.

e. (U) **Other Considerations From the Assessment.** Include additional information the core group decided was important to consider in planning. Add the statement that the local assessment is valid only if used in conjunction with the NSTCA and any planning being conducted using the local TCA must also include the NSTCA.

f. (U) **Plausible Attack Scenario Matrix.** The matrix should be designed in concert with the development of the local TCA and should follow the format provided in the Table. Each environment the core group assesses should be addressed.

Table 1. (U) Plausible Attack Scenario Matrix (Format Example)

UNCLASSIFIED					
Legend:					
Threat Group Intent: D = To disable the weapon or create embarrassment for the Department of Defense or the United States					
I = In-place detonation					
T = Theft of the weapon					
Insider Estimation: M = More likely					
L = Less likely					
Environment (Above Ground, Below Ground, Waterside Restricted Area, WS3, etc.)					
#	Scenario	Team Composition	Threat Group	Intent	Insider
Number each scenario separately using a local numbering system	Provide a synopsis of the adversary scenario and course of action	List the adversary team size and composition as well as special equipment and weapons	Name the threat group(s) from which this scenario was selected	D, I, T as applicable	M, L as applicable to signify probability as to whether an insider will be used for the scenario

g. (U) **Overall Risk Assessment.** An overall assessment of the risk to nuclear weapons at the installation as determined by the core group should be provided (low, low-medium, medium, medium-high, high). Restate the lowest, overall, and largest threat group sizes as assessed by the

~~SECRET//REL TO USA AND NATO~~

DoDM S-5210.41-V1, August 11, 2016

Change 1, October 25, 2016

teams and which group or groups is most likely to attempt to gain unauthorized access to a weapon.

4B.3. (U) APPROVAL. The final product representing the localized TCA must include a letter of approval from the senior local commanders responsible for the assigned weapons covered in the localized assessment. At dual or multiple command locations, all commanders must approve.

SECTION 5: (U) NUCLEAR WEAPON SECURITY PLANNING

5.1. (U) SITE PLANNING.

a. (U) **General.** This section delineates command responsibilities to conduct necessary risk assessments. Additionally, this section provides security considerations for the selection, construction, or major modification of storage and alert areas. Safety requirements and efficiency must be considered in conjunction with security when conducting nuclear weapon security planning.

b. (U) **Responsibilities.**

(1) (U) **Commanders.** Commanders will ensure threat assessments are conducted as the basis for conducting VAs of weapons, weapon storage locations and operating environments, identifying the risks facing these weapons, locations, and environments, and identifying the need for changes or improvements to fully protect U.S. nuclear weapons at all times.

(2) (U) **Supporting Units.** Supporting military intelligence, counterintelligence, and law enforcement units will assist nuclear sites by providing spot reports of potential or actual threats or incidents that may affect the security of a site and investigating incidents or suspected security violations reported by nuclear units. Established force protection threat indications and warning systems will be used in this mission.

(3) (U) **Operating Commands and Site Specific Commanders.** Operating commands and site specific commanders must review intelligence data at least 24 hours prior to all logistics movements outside permanent limited areas.

c. (U) **Planning Considerations.**

(1) (U) **Storage and maintenance facilities located underground provide the best security for nuclear weapons.** Underground facilities are more difficult to attack than above-ground facilities because they complicate adversary surveillance operations and hinder attack planning and execution while providing better protection from the airborne threat. Underground facilities provide an indigenous and significant advantage in delay and denial against an adversary force and are easier to defend because adversaries can be engaged before they get to the entrance. They offer fewer entries and exits to defend and less ground for defenders to observe and dominate, and lessen the standoff weapons threat. Military Departments should consider moving current storage facilities underground while keeping operational considerations in mind. Construction of future storage and maintenance facilities will be underground unless uniquely localized soil or water table constraints prohibit such construction or unless specifically prohibited by national laws or agreements.

(2) (U) **Site planning will consider the adversary's current and future capabilities, the system vulnerabilities produced by those adversary capabilities, and inherent risks associated with nuclear weapons in all environments.** An initial threat and risk vulnerability assessment

will be made in accordance with Sections 4 and 5 of this volume, and subsequently must be updated at least on an annual basis. Each site must be evaluated separately and its security planned and implemented accordingly.

(3) (U) Nuclear security threat and vulnerability information is often classified at the Top Secret level. Military Departments must ensure nuclear security planners and commanders are granted Top Secret clearances as necessary to evaluate and manage the threats to the local operating environments effectively.

d. (U) VAs. Commanders will conduct tests and evaluations to determine the effectiveness of in-place protection systems against the DIA and localized TCA analyses and to identify vulnerabilities in the protection systems. The results of these tests will form the basis for commanders and Military Departments to identify and implement corrective actions, determine and construct risk management strategies, and quantify the degree of risk to nuclear weapons while implementing strategies to reduce the identified risks. The commanders tasked to establish the level of acceptable or unacceptable risk are the same as those assigned deviation approval authority, as identified in Section 6 of Volume 2 of this manual. Identified risk must be communicated to these commanders and their decisions implemented.

(1) (U) Vulnerabilities in protection systems that raise the risk to nuclear weapons above the commander's acceptable level must be mitigated. Improvements to any portion of the security system in technology, tactics, techniques, and procedures must be identified and tested to see what reduction in risk is achievable and a strategy implemented to choose and implement cost effective mitigation strategies.

(2) (U) The risk to nuclear weapons must be continuously assessed and reevaluated as threats evolve, environments change, and protection systems age. This process is accomplished by a combination of VAs, capabilities-based evaluations and tasks, computer modeling and simulation, and force-on-force exercises.

(b)(1),(b)(3):10 USC §128

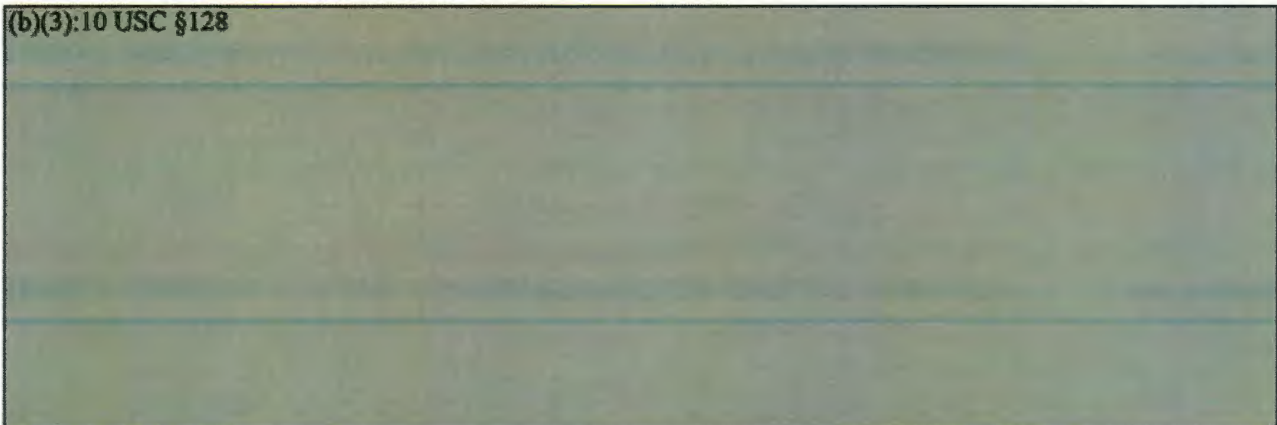


e. (U) **Conduct of Risk Assessments.** Military Departments, Combatant Commands, and commanders must conduct formal risk assessments of the nuclear weapons in their custody. At a minimum, a formal VA is required before nuclear weapons are introduced for the first time to a

nuclear weapon storage or permanent alert area. VAs must be updated at least annually, but more frequently if threat assessments dictate and must contain recommendations on how best to reduce or mitigate identified vulnerabilities.

(1) (U) **Security System Effectiveness.** Military Departments, Combatant Commands, and commanders will review the security plans and measures for all phases of operations and for all potential environments concerning the weapons. Such reviews include integrated force protection and defense plans, physical security measures (including barriers, obstacles, clear zones, lights, detection systems, alarms, communications, delay systems, and security forces personnel), training, and equipment to determine if the security system is balanced, in-depth, and sufficient to protect against the potential threat.

(b)(3):10 USC §128



f. (U) **Risk Management.** Commanders will use the formal assessments process to validate increases or decreases in security force requirements and security equipment or system upgrades needed to reduce risk. These assessments and the commander's decision on each recommendation will be documented and retained using a format similar to that in Appendix 4B of this volume.

g. (U) **Systems Approach.** Denial systems and security forces should mutually support one another and offer a synergistic effect that achieves the NWSS. When properly employed elements are integrated in a systems approach, the overall effect on the security systems' ability to deter, detect, delay, deny, and ultimately defeat an adversary is increased. The systems approach must:

(1) (U) Prevent penetration of limited and exclusion areas by an adversary.

(2) (U) Ensure a capability for positive deterrence, detection, delay, assessment, denial, and defeat of any attempt to gain unauthorized access to nuclear weapons. Physical delay must be longer than the maximum security force response time to permit interdictions prior to adversary access. The intent is to design physical security that delays unauthorized access long enough to allow the security force to detect, react to, and defeat the adversary before they can reach the nuclear weapon.

(3) (U) Provide complete, positive, and efficient entry to and surveillance of the site and of access to nuclear weapons.

(4) (U) Ensure expeditious and secure entry of emergency forces such as fire department, explosives ordnance disposal (EOD) personnel, security, and other RFs. Positive measures must be implemented to preclude an adversary from using modified emergency entry procedures to circumvent procedural security.

(5) (U) Ensure that the first priority for allocating applicable resources is to increase the overall effectiveness of security operations for nuclear weapons. This includes intelligence estimates and plans, availability of security forces, transportation means and routes, and availability of logistic support facilities (helipads and airfields) to enhance the security of the nuclear weapons. Pertinent consideration should be given to the efficiency of nuclear weapon facilities within an existing military installation so as to facilitate administrative support, logistical support, and augmentation of security forces, and to minimize the need for movement of weapons off of military installations.

(6) (U) Locate nuclear storage, custodial, and maintenance facilities within the same limited area, where feasible.

h. (U) National Environmental Policy Act. The National Environmental Policy Act requires an environmental assessment of the effect of construction or modification of sites on the environment. Site planning must consider local and national environmental standards and conservation of the natural resources of the area.

i. (U) Safety. Safety aspects enhance overall security. Site planning must account for certain factors from the DTRA Technical Publication 20-7, including: explosive safety quantity-distance criteria, plutonium storage limitations, ground transport considerations, potential external hazards, and availability and adequacy of supporting emergency forces. Industrial, ground, explosive, and radiation safety requirements specified in pertinent directives and references also must be considered during the planning phase. However, explosive safety quantity-distance criteria intended to enhance personnel safety must not be the determining factor in positioning of facilities intended for the use of security forces. These facilities will be considered operational structures, not subject to restrictions appropriate to habitations, and located to optimize response to threats.

j. (U) Land Requirements. Land area requirements for nuclear weapon storage and alert areas must not deviate from the explosives quantity-distance requirements found in DoDM 6055.09. Site planning will ensure that land requirements include permanent easements or ownership to accommodate present and anticipated requirements and limit civilian encroachment. When possible, nuclear weapon areas should be located as far as possible from main or frequently traveled roads, and the surrounding terrain out to at least 300 meters should be off limits to personnel not associated with the nuclear mission.

(b)(3):10 USC §128

(b)(3):10 USC §128

1. (U) Considerations During Research, Development, and Acquisition. Nuclear weapon systems security considerations and the modernization and updating of existing systems must be integrated into the systems engineering process, consistent with mission requirements and cost-effectiveness, in accordance with DoDD 5000.01 and DoDI 5000.02.

(1) (U) The DoD Components participating in the Defense Acquisition Process will develop a system security engineering management program.

(2) (U) The criteria for the selection and implementation of nuclear physical security systems should include a cost-benefit analysis.

(3) (U) Each nuclear weapon system must be evaluated for known or potential system vulnerabilities for its entire life cycle, and significant vulnerabilities and associated risks must be identified to the DASD(NM) and the Military Departments prior to Milestone B, "Engineering and Manufacturing Development Phase," Decision.

(4) (U) Vulnerabilities in systems must be eliminated or controlled before Milestone C, "Production and Deployment."

(5) (U) System security programs must be applied to off-the-shelf procurement and in-house research, development, production, modification, and test programs.

m. (U) Mandatory Implementation.

(1) (U) The provisions of this volume are mandatory for the new construction of permanent land-based installations for nuclear weapons storage and alert areas. Modifications to existing facilities must be accomplished in accordance with the criteria set forth herein. However, the tearing down and rebuilding of facilities should not be undertaken unless the required physical security protection cannot be attained with existing facilities. The deviation requirements in Section 6 of Volume 2 of this manual must be applied if system replacement is deemed to be cost prohibitive or a replacement system is technically similar to the requirement.

(2) (U) The DoD Components will develop NWPS roadmaps that evaluate current nuclear weapons security capabilities against assessed threats derived from the DIA's TCA. The roadmap should:

(a) (U) Identify and prioritize capability gaps and determine potential solutions within doctrine, organization, training, materiel, leadership, personnel, and facilities capabilities.

(b) (U) Include a priority list by site for meeting the security requirements set forth herein and program and budget for necessary improvements or changes.

(3) (U) The Military Department's NWPS roadmaps must be provided to the DASD(NM) triennially. Military Departments must establish a priority system for the required improvements at each site, setting forth the order for achieving the required upgrading actions and the projected fiscal year in which these requirements are to be programmed.

n. (U) **User or Host-Nation and NATO Agreements.** Where facilities are provided by a user or host nation of NATO, the standards and criteria specified in this manual will be used in negotiations to improve existing facilities and systems. The standards and criteria may be modified to meet user or host-nation or NATO requirements, provided that the changes provide equivalent security and the DASD(NM) reviews them in advance. The DASD(NM) will review every DoD Component nuclear security policy document prior to final approval and publication. The purpose of this review is to ensure compliance with U.S. nuclear security policy.

o. (U) **Planning Assistance.** Upon request, DTRA will help plan, design, and construct storage and alert areas. Such assistance does not relieve the DoD Component from the provisions of DoDM 6055.09, which require that all general site plans for construction or modification of fixed or movable ammunition and explosives facilities and sites, or facilities in proximity to or affected by such facilities and sites, be submitted to the DoD Explosives Safety Board for review.

5.2. (U) SECURITY PLANNING.

a. (U) General.

(1) (U) This section specifies criteria and security standards that must be applied to all physical security plans for nuclear weapon environments. Each environment is unique; therefore, specific nuclear weapon security requirements must be tailored to the characteristics and individual facilities of each environment.

(2) (U) Plans must incorporate the capability concepts of detection, delay, denial, and defeat to prevent unauthorized access to a nuclear weapon.

(3) (U) Plans must initiate immediate recapture and recovery efforts in the event that U.S. control of nuclear weapons is lost. Nuclear weapon recapture and recovery guidance is provided in Section 4 of Volume 2 of this manual and must be considered in security planning. Recapture and recovery planning is integral to the NWSS.

(4) (U) The task of maintaining security at a nuclear weapon storage or alert area is facilitated by proper site location, facility layout, and design. Security personnel must participate in the site selection, site layout, and development of appropriate security plans. Physical security features necessary for effective protection must be incorporated into the design and construction of the site. However, since most facilities are located in already existing sites, effective planning must consider all elements of the METT-TC template.

(5) (U) Planning is based on adversary capabilities, as articulated in the DIA TCA and localized TCA. Plausible attack scenarios are developed in conjunction with those included, by environment, in the NSTCA.


b. (U) **Physical Security Plan.** A physical security plan must be prepared for each location having a storage area and each location where nuclear weapons are mated to operational platforms. Field units charged with the security of multiple sites (e.g., land-based Intercontinental Ballistic Missile (ICBM) Launch Facility wings; European WS3 sites) may consolidate their planning into one physical security plan; however, each individual site must be specifically addressed. The security plan should be updated as required, but must be formally reviewed by the local security force commander at least annually and appropriate changes made.

c. (U) **Coordination.** Defense, protection, recapture, and recovery plans for nuclear weapons must be coordinated to ensure that protection of nuclear weapons receives adequate coverage. Such plans will include provisions for mutual support of collocated forces. The tenant or custodial nuclear weapon organization will be a participant in host base planning. Combatant Commands having nuclear weapons security responsibilities will receive copies of the plans through Military Department higher headquarters. Recapture and recovery plans, specifically local integrated response plans, must be coordinated with the Federal Bureau of Investigation Field Office responsible for the mission within the continental United States.

d. (U) **Integration of Security Methods.** The security plans will be formulated and implemented from a systems approach. All elements, systems, and subsystems of the plan will be integrated and will complement each other. Authority, jurisdiction, and responsibilities of security forces will be defined and coordinated in situations involving the protection and security of nuclear weapons.

e. (U) **Standoff Attack Protective Measures.**

(b)(3):10 USC §128



(2) (U) Protective measures to mitigate the risk of standoff attack may include:

(b)(3):10 USC §128



(b)(3):10 USC §128



(d) (U) The use of underground storage facilities.

(e) (U) The use of OPSEC and CCD techniques, particularly during loading and movements.

(b)(3):10 USC §128



g. (U) Airborne and Air Attack Protective Measures. As national policy allows, provisions must be instituted in all nuclear environments to defend against plausible airborne threats, as described in the DIA and local threat assessment. See Paragraph 3.2.b.(7) of Volume 2 of this manual for specific measures to be taken against airborne assault threats.

h. (U) Storage of Nuclear Weapons Components. Nuclear components, including nuclear limited-life components, critical components, and radioactive materials, may be stored in any structure suitable for storage of nuclear weapons or in any facility that meets or exceeds Military Department-directed safety, security, and explosive requirements for the components. SNM security requirements are found in DoDI O-5210.63.

i. (U) Control of Training Weapons and Empty Containers.

(1) (U) Military Departments and Combatant Commands must ensure strict accountability, including secure storage, is exercised over training weapons designed by the DOE. Under no circumstances may a war reserve nuclear weapon or its container be marked with the identification of a training weapon or vice versa.

(2) (U) Military Departments and Combatant Commands must institute provisions to ensure visual confirmation that nuclear weapon or nuclear weapon component containers are empty and marked according to Military Department directives prior to moving empty containers from a site.

j. (U) Separation of Nuclear From Non-Nuclear Activities. In order to maximize nuclear surety, nuclear weapon storage, maintenance, and inspection activities should remain separate from unrelated activities such as storage, maintenance, and inspection of conventional munitions.

k. (U) **Construction Activity.** Where substantial construction is underway at nuclear weapon storage or alert areas, the construction site may be physically separated from the areas containing nuclear weapons. If this option is deemed suitable for the scale of the activity, the area thus formed is designated a "free zone."

(1) (U) A combination of additional security measures, including sentries, entry controls, and physical barriers, must be established to ensure that the capability to detect and prevent unauthorized entry at the "free zone" barrier is equal to that provided by the area's permanent barrier system.

(2) (U) *Any construction activity that may impact the security requirements of this manual, whether a free zone or other large-scaled activity unsuitable for the establishment of a "free zone," requires a formal deviation with appropriate compensatory measures. Free zone plans must be approved by the deviation approval authority as defined in Section 6 of Volume 2 of this manual.*

~~(3) (U) Large-scaled activities involving substantial areas or portions of the storage or alert area may not be suitable to the establishment of a "free zone." In such situations, a plan must be established and approved by the risk acceptance authority that compensates for the activity while maintaining the NWSS.~~

l. (U) Facility and Equipment Maintenance.

(1) (U) Nuclear weapon facilities and related security equipment must be maintained to ensure no degradation of safety or security. Priority maintenance will be given — but not limited — to perimeter fences, vegetation control, security lights, clear zones, IDS, delay and denial systems, communication systems, auxiliary power equipment, automated entry control system, vehicle barriers, locking devices, doors, gates, and structures.

(2) (U) Maintenance of security and storage facilities and equipment must be accomplished on a continuing basis. At least weekly, security forces must thoroughly check all exclusion and limited area fences, lights, clear zones, doors, and gates.

(a) (U) The check of the fence lines and clear zones must be conducted on foot so as to permit a complete check of the fence fabric.

(b) (U) At least once each day during daylight hours, the on-duty supervisor must make a physical inspection of the limited area.

(c) (U) These checks are designed to ascertain deficiencies or new vulnerabilities in the security system and identify evidence of potential attack preparations by an adversary.

(d) (U) Records of these checks must be maintained by the unit responsible for the security of the nuclear weapon. The supporting engineering or maintenance activity will be notified of deficiencies not corrected by site personnel. Any discrepancy that degrades security and is not corrected immediately must be mitigated.

(e) (U) The requirements of this paragraph do not apply to the WS3 or ICBM Launch Facility configurations.

m. (U) Site Plans, Drawings, and Documents.

(1) (U) Plans, drawings, and documents concerning nuclear weapon facilities that reveal the layout (showing buildings, parking areas, access roads, fences, emergency generators, outside storage areas, natural terrain, landscaped areas, tunnels, storm and waste sewers, water intake and discharge conduits, culverts, creeks, canals, and other physical characteristics, such as construction features of buildings, barriers, fences, guard stations, etc.) must be marked and controlled as DCNI, at a minimum. Local unit commanders must review such documents and determine if a classification of Confidential or higher is warranted based on unique local information and VAs.

(2) (U) Plans, drawings, and documents showing construction characteristics of buildings and associated fencing, electrical, and other utility system layouts or revealing information that identifies a facility or installation as a nuclear weapon storage site or nuclear alert area must be classified in accordance with the Department of Defense Nuclear Weapon Security Program Security Classification Guide.

5.3. (U) SECURITY SYSTEM DESIGN STANDARDS. Specific security design standards for nuclear weapons protection systems depend on the weapon configuration. For more information, see Section 3 of Volume 2 and Volume 3 of this manual.

SECTION 6: (U) NUCLEAR WEAPON DENIAL

6.1. (U) GENERAL. This section describes concepts and requirements for the denial of unauthorized access to nuclear weapons.

6.2. (U) CONCEPT.

a. (U) The concept of denying unauthorized access to nuclear weapons is a national responsibility. The accompanying recapture and recovery capability is not based in rules of evidence, but rather a military operation protecting or regaining control of vital national interests.

b. (U) All security system capabilities are designed to work together to achieve the NWSS.

(b)(3):10 USC §128



6.3. (U) DENIAL SYSTEMS.

a. (U) Area denial begins at the limited area boundary and can include boundary clear zones, fences, IDS, and security forces and their weapons.


(b)(3):10 USC §128



~~SECRET//REL TO USA AND NATO~~

DoDMS-5210.41-V1, August 11, 2016
Change 1, October 25, 2016

(b)(3):10 USC §128



c. (U) Incapacitating denial systems, at a minimum, must:

(b)(3):10 USC §128

~~SECRET//REL TO USA AND NATO~~

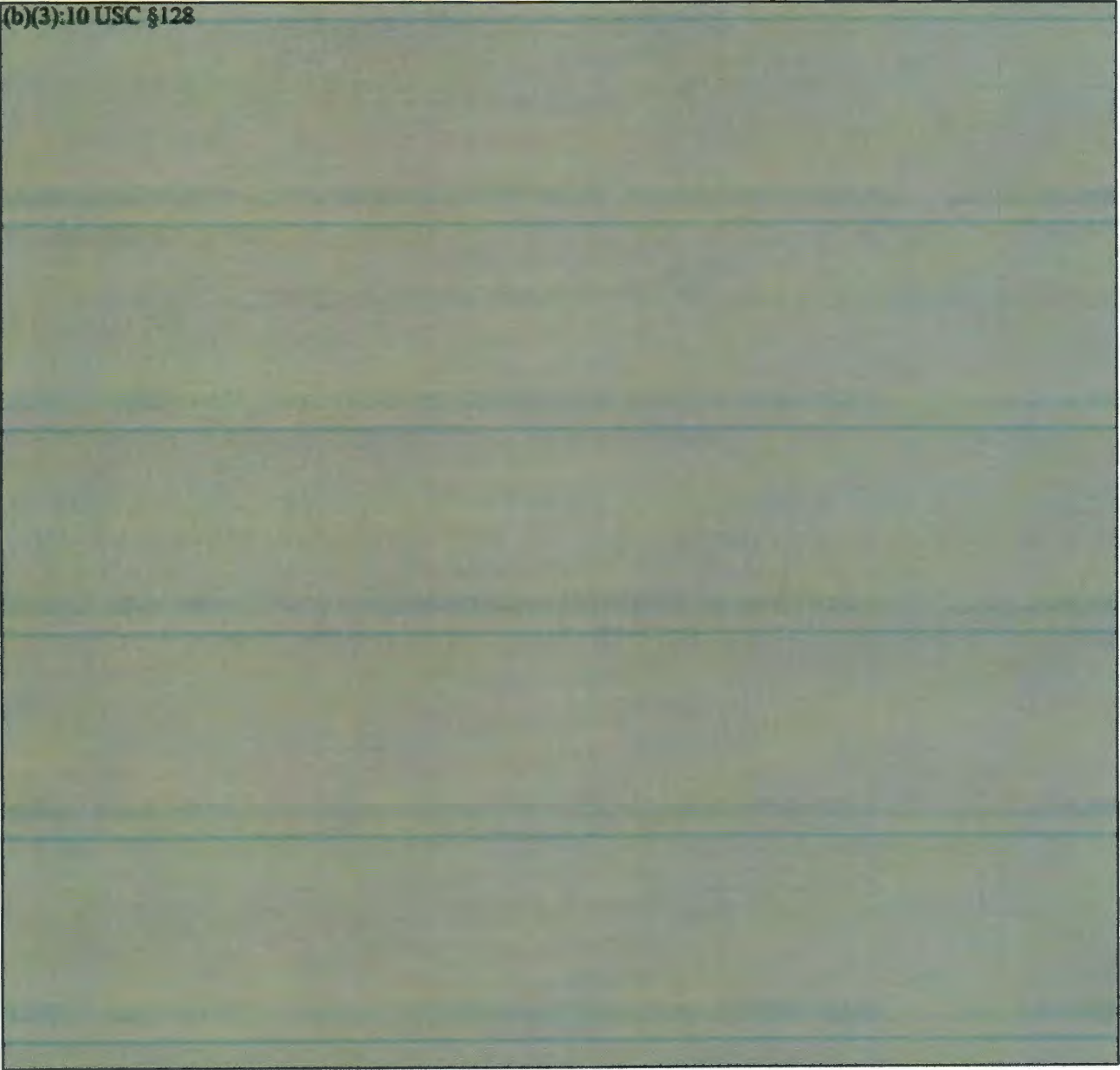
DoDM S-5210.41-V1, August 11, 2016
Change 1, October 25, 2016

SECTION 7: (U) NUCLEAR WEAPON SECURITY FORCES, EQUIPMENT, AND TRAINING

7.1. (U) SECURITY FORCES.

a. (U) Designated Forces.

(b)(3):10 USC §128



(c) (U) DoD Components ensure their post manning factor equations or task organized units are appropriate to ensure that the authorized strength of nuclear security force units are at sufficient levels to meet the NWSS. Post manning factor equations may include, but not be limited to:

1. (U) The unit's responsibilities to perform multiple tasks at the same time (e.g., security for weapon movements, weapons storage areas, contingency operations, force protection condition increases).

2. (U) Present-for-duty factors.

3. (U) Training requirements to maintain proficiency (e.g., weapons qualification, tactics).

4. (U) Other requirements of this volume (e.g., dedicated recapture and recovery teams, post rotation requirements).

(b)(3):10 USC §128



(4) (U) During peacetime, the minimum security force baseline must be U.S. military personnel in active status (in NATO, security forces must be user- or host-nation military), certified under a RAP, and must consist of:

(b)(3):10 USC §128

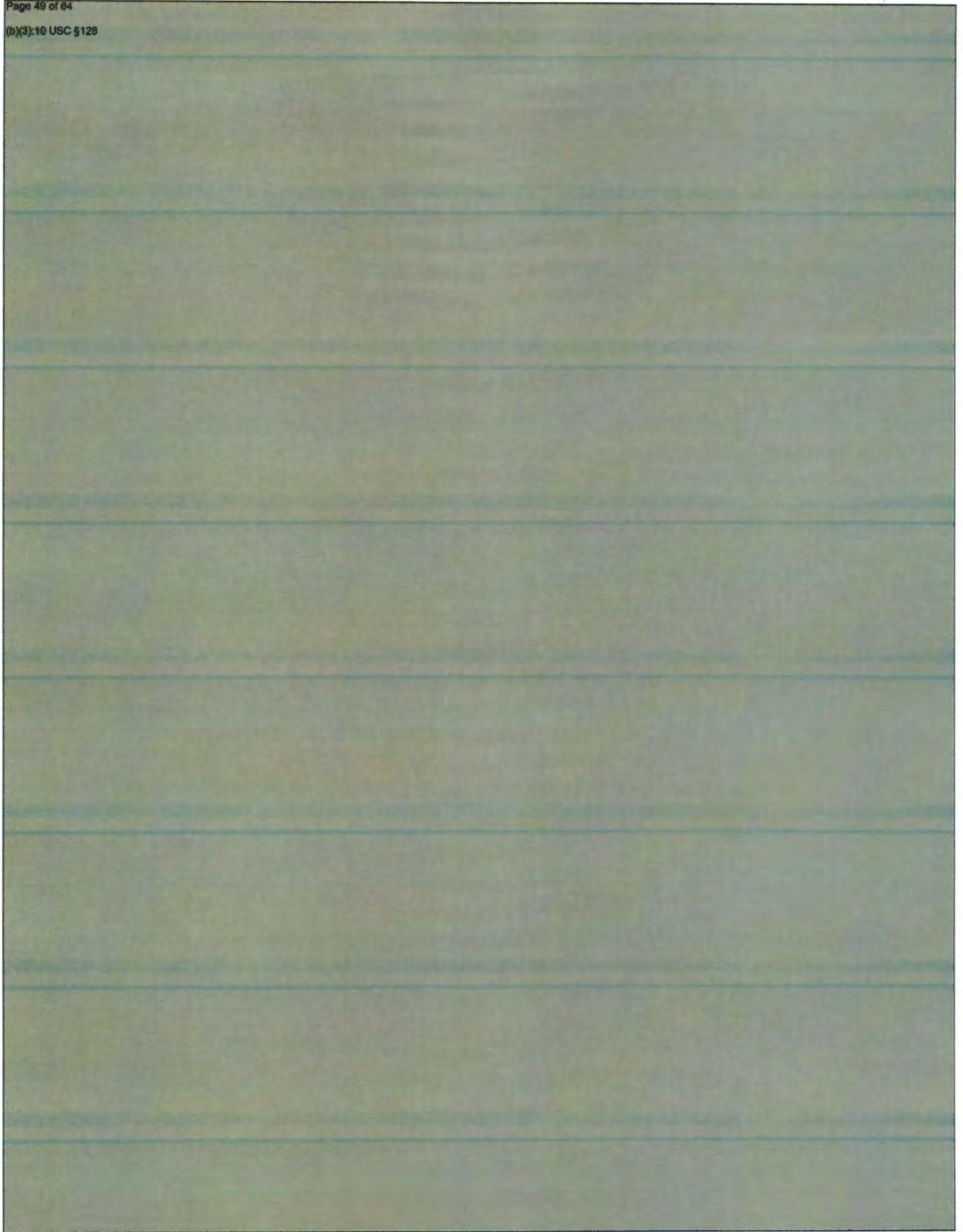


1. (U) An area or movement supervisor.
2. (U) Alarm monitors (ESS-equipped security system operating environment).
3. (U) Entry controllers, as required per environment.
4. (U) Boundary sentries, if necessary.

(b) (U) Sentries on post armed with a firearm. Types of weapons carried must be appropriate to counter the most likely attack scenarios, as defined in the NSTCA and local threat assessments.

(b)(3):10 USC §128





(b)(3):10 USC §128

d. (U) **Use of Force.** All security forces must act in accordance with CJCSI 3121.01B.

(b)(1),(b)(3):10 USC §128

(3) (U) At OCONUS locations, rules for the use of force must consider any restrictions contained in existing status of forces agreements and applicable host-nation laws pertaining to the use of deadly force.

(b)(3):10 USC §128

(5) (U) All security forces personnel will be trained on the use of force, including deadly force, and be knowledgeable of the most likely attack scenarios for their particular locations.

e. (U) **Exercises.** Exercises will be conducted for baseline security forces (RF, BF, and subsequent BFs) to maintain proficiency, as set forth in Paragraphs 7.1.e.(1) and 7.1.e.(2) .

(1) (U) RF. In order to maintain tactical proficiency, the complete RF will be tactically deployed at least once each week (unless otherwise authorized in this volume) in reaction to a sufficiently capable robust threat scenario. Maneuver, communications, and command and control elements should receive emphasis during this exercise. Actual deployment of the RF may be counted as the weekly exercise requirement, provided composition and time requirements were met.

(2) (U) BF. In order to maintain tactical proficiency, the complete initial BF will be tactically deployed at least monthly in reaction to a sufficiently robust threat scenario. Maneuver, communications, and command and control elements should receive emphasis during this exercise.

7.2. (U) SECURITY FORCE WEAPONS AND EQUIPMENT.

a. (U) Weapons.

(1) (U) Weapons that provide the maximum practical firepower must be provided for security forces, either as the weapon assigned or as one that is immediately available (issued and on post, not in storage at the arming point or other location).

(a) (U) Where it is determined necessary or advisable to issue side arms to personnel responsible for the protection of nuclear weapons, weapons providing greater firepower will be available to the individual for immediate use in the defense of the nuclear weapon in case of hostile attack. This requirement does not apply to WS3 alarm operators.

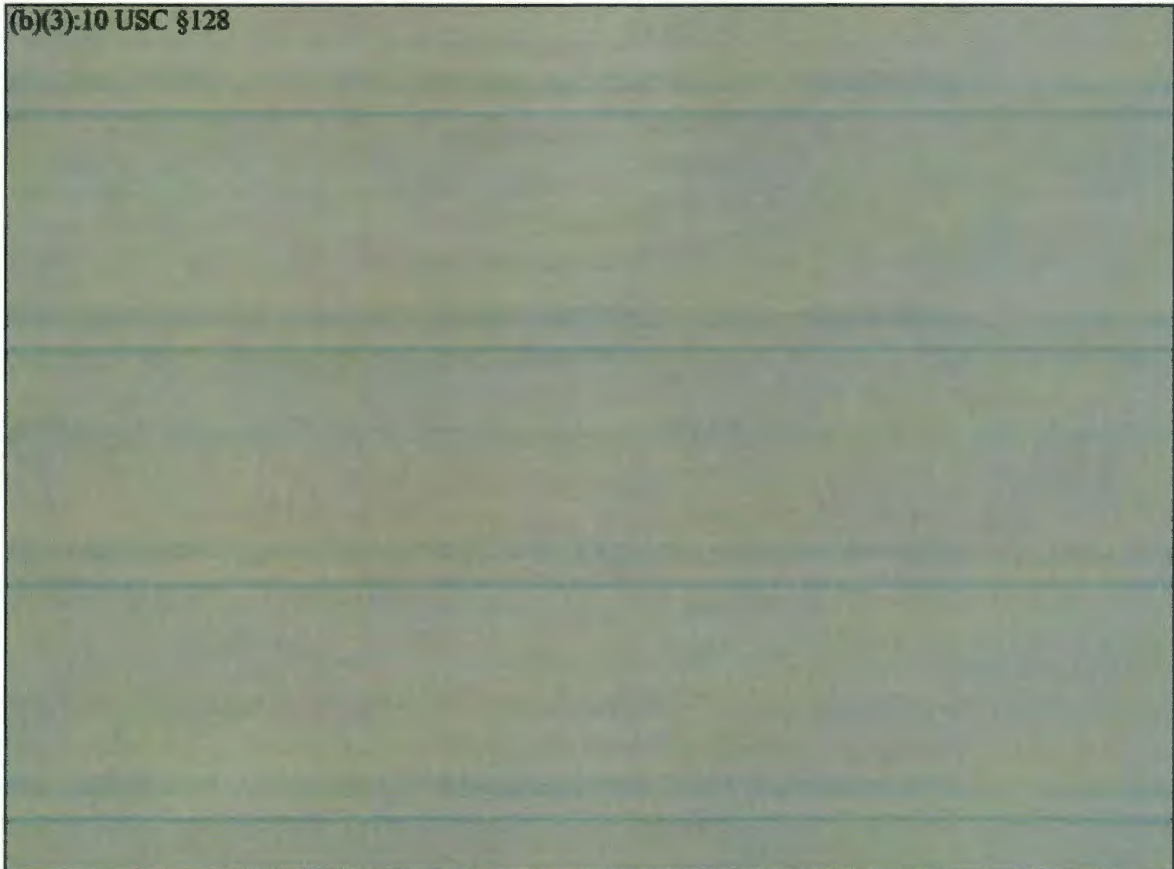
(b) (U) Although non-lethal weapons may be issued, personnel performing nuclear security duties must never be issued non-lethal weapons as the primary or sole duty weapon (submerged underway nuclear armed submarine roving security forces patrols are exempt from this requirement).

(b)(1)



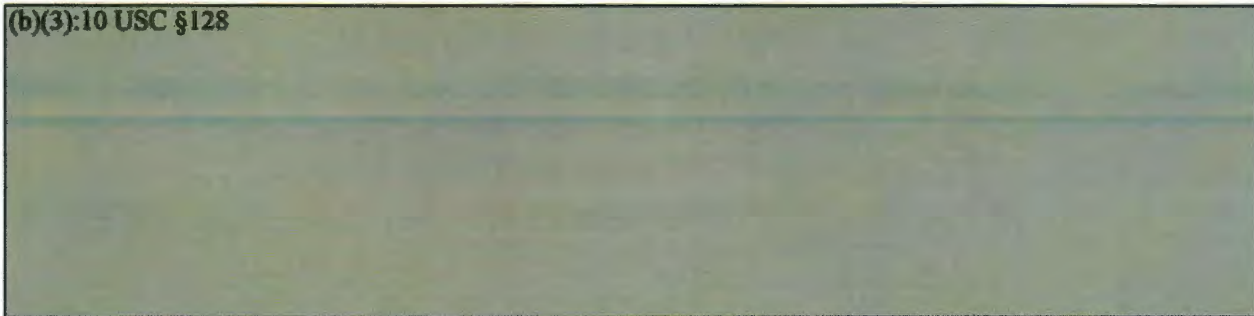
b. (U) Equipment.

(b)(3):10 USC §128



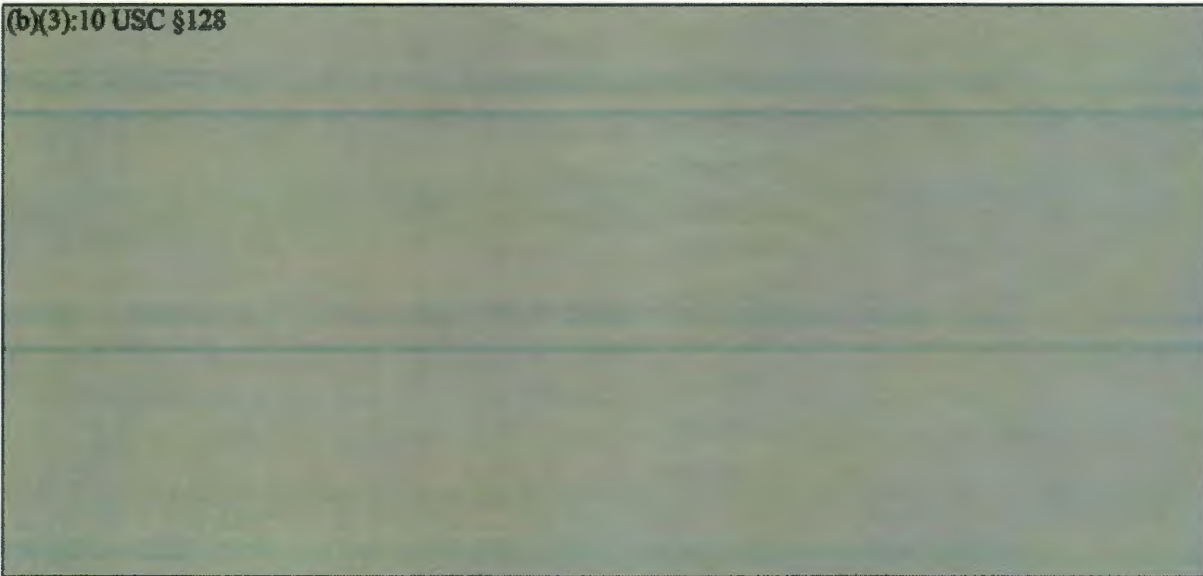
c. (U) Vehicles.

(b)(3):10 USC §128



(a) (U) Tires must have a run-flat capability and vehicles must be suitable for crew sustainment in varying weather conditions. Security force vehicles will be four wheel/all-wheel drive except in situations where specific tactics teams require vehicles of a size and weight that preclude their off-road use.

(b)(3):10 USC §128



7.3. (U) SECURITY FORCE TRAINING.

a. (U) **General.** Security training programs must prepare and train personnel to meet the NWSS. Security forces must attain and maintain training capabilities necessary to achieve the objectives of the DoD nuclear weapon security program stated in Section 3 of this volume. Military Department training programs must have an active process to exchange lessons learned regarding tactics, training, procedures, and security incidents with other units tasked with nuclear security missions.

b. (U) **Scope.** Security forces personnel assigned to duties involving the protection of nuclear weapons will be trained in the subjects in Paragraphs 7.3.b.(1) through 7.3.b.(4). Personnel designated to augment or reinforce security forces (support forces) in emergencies will be trained in these subjects commensurate with their planned participation in security force emergency operations.

(1) (U) **General Training.** Responsible commanders must ensure nuclear security force personnel are fully trained. The Military Department concerned determines training frequency, and gives priority to those training tasks that most directly relate to the security force member's ability to perform their duties. Training tasks include:

- (a) (U) Personnel identification.
- (b) (U) Circulation and internal control (how personnel within the area are identified and controlled).
- (c) (U) Apprehension.
- (d) (U) Overview and characteristics of ESS.

- (e) (U) Inspections (i.e., of individuals and packages for entry control).
- (f) (U) Vehicle inspections.
- (g) (U) Operation and use of security communication systems and equipment.
- (h) (U) Familiarity with the DIA and localized TCA (for their environments).
 - 1. (U) Adversary groups.
 - 2. (U) Motivation and objectives, and plausible scenarios.
 - 3. (U) Tactics (including standoff attack).
 - 4. (U) Recognition of sabotage-related devices and equipment.
 - 5. (U) Adversary threats, including the ability of an adversary to conduct internet-based virtual reconnaissance and the dangers and vulnerabilities of social network sites. Effective operational security and information security principals are necessary to deny an adversary critical information.
- (i) (U) Security vehicle operation.
- (j) (U) Duress system.
- (k) (U) Security awareness and vigilance.
- (2) (U) Security Skills Training.
 - (a) (U) Small unit combat tactics (day and night).
 - (b) (U) Antiterrorism tactics.
 - (c) (U) Defense against standoff attack.
 - (d) (U) Specialized personal equipment (e.g., night vision aids, range finders).
 - (e) (U) Use of force (including deadly force).
 - (f) (U) Applicable site defense plans.
 - (g) (U) Weapons qualification and familiarization fire for weapons without formal courses of fire.
 - (h) (U) Airborne threat engagement.
- (3) (U) Transportation Security Training.

- (a) (U) Weapon movement techniques.
- (b) (U) Escort vehicle procedures.
- (c) (U) General tactics for responding to threats.
- (d) (U) Continuous surveillance of shipment procedures.
- (e) (U) Emergency action procedures addressing local threat scenarios.
- (4) (U) Security Supervisory Personnel Training (Supervisory Personnel).
 - (a) (U) Applicable site defense plans.
 - 1. (U) Bomb threats.
 - 2. (U) Civil disturbances.
 - 3. (U) Hostage situations.
 - 4. (U) Motivation of security personnel.
 - 5. (U) Evaluation and use of intelligence services.
 - (b) (U) Recapture operations.
 - (c) (U) Recovery operations.
 - 1. (U) Recovery plan.
 - 2. (U) Interaction with other military or civilian recovery forces.
 - (d) (U) Emergency reporting requirements.
 - (e) (U) Operation and use of ESS.
 - (f) (U) The DIA and localized TCA, VAs, and likely adversary tactics.

c. (U) Specialized Training.

(1) (U) Security forces personnel will receive specialized training, as applicable (e.g., recapture and recovery team training, breach training, command disable training) pertaining to their specific duties and duty location. A supervisory level individual designated by the unit commander must certify this training.

(2) (U) Supporting security forces will receive detailed guidance and training in recognizing the difference between forceful or determined hostile site penetration and the assembly of demonstrators, inadvertent trespass, or comparable encroachments.

d. (U) **Continuing Education.** Security force commanders will ensure the establishment of a continuing program to promote the education of security forces personnel. The program must include briefings on nuclear weapon site security incidents, current and potential threats, OPSEC, intelligence and counterintelligence products, plausible actions by possible intruders and the planned security forces reactions, and practical exercises in defensive techniques to counter the threat. Additionally, it will cover the appropriate technical information regarding the types of weapons in storage and any special information the security forces need to consider when planning or executing recapture or recovery operations.

e. (U) **Force-on-Force Training.**

(1) (U) Required unit level force-on-force training exercises improve and maintain the proficiency of security forces. Unit level force-on-force training must not be used for personnel or unit evaluation or inspection by outside agencies.

(2) (U) Security forces commanders will ensure force-on-force training is conducted for all security forces members with enough frequency to maintain proficiency in their nuclear weapons security duties and reinforce the small unit tactics training provided during security skills training. The training should be tailored to each location based on localized TCA scenarios, local threat assessments, and assessments of local vulnerabilities. The training may be conducted at off-site locations when required by critical security and safety considerations.

(3) (U) The training must include realistic engagement exercises and an aggressor force trained and equipped to replicate the NSTCA as closely as possible. It is strongly suggested that this training be complemented with modeling and simulation programs and tabletop exercises. Engagement systems such as multiple integrated laser engagement systems, other electronic engagement systems requiring blank munitions, or simulated munitions engagement systems are examples of realistic engagement systems. The training should provide maneuver and response forces the opportunity to train realistically in a dynamic learning training environment.

(a) (U) Units should conduct training in as realistic an environment as possible. When developing the composition and strategy of the "opposing force," use the threat contained in the NSTCA and local or theater-wide threats.

(b) (U) Military Departments conducting training where armed security forces are posted must establish necessary policy guidelines. Never conduct force-on-force training in a manner that will allow armed security forces to come into contact with the personnel in training.

1. (U) Provide actual security forces with constant supervision to preclude involvement in exercise scenarios.

2. (U) Provide positive controls to prevent personnel from introducing or using live ammunition in the training exercise.

3. (U) Alert all personnel of whom is carrying live ammunition.

~~SECRET//REL TO USA AND NATO~~

DoDM S-5210.41-V1, August 11, 2016

Change 1, October 25, 2016

(4) (U) Submarine unit security personnel force-on-force training will be incorporated into coordinated submarine base and waterfront force-on-force training exercises.

f. (U) **Additional Training.** Consideration should be given to training selected supervisory security force personnel in incident management systems such as the National Incident Management System or similar Service incident management systems.

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

ASD(NCB)	Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs
BF	backup force
CCD	camouflage, concealment, and deception
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
DASD(NM)	Deputy Assistant Secretary of Defense for Nuclear Matters
DCNI	DoD Unclassified Controlled Nuclear Information
DIA	Defense Intelligence Agency
DoDD	DoD Directive
DoDI	DoD Instruction
DoDM	DoD Manual
DOE	Department of Energy
DTRA	Defense Threat Reduction Agency
EMR	electromagnetic radiation
EOD	explosive ordnance disposal
ESS	electronic security system
ICBM	intercontinental ballistic missile
IDS	intrusion detection system
JP	Joint Publication
METT-TC	mission, enemy, terrain and weather, troop availability, time availability, and civil considerations
M&I	maintenance and inspection
NATO	North Atlantic Treaty Organization
NC2	Nuclear Command and Control
NSTCA	nuclear security threat capabilities assessment
NWPS	nuclear weapons physical security
NWSS	nuclear weapon security standard
OCONUS	outside the continental United States
OPSEC	operations security

RAP	reliability assurance program
RF	response force
S2	survivability and security
SNM	special nuclear materials
SRT	security response team
SSCC	Site Security Control Center
TCA	threat capabilities assessment
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USSOCOM	U.S. Special Operations Command
VA	vulnerability assessment
WS3	Weapons Storage and Security System

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

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

a. authorized access. Close physical proximity within the nuclear weapon exclusion area, obtained through proper control measures, to accomplish a specific authorized mission(s).

b. unauthorized access. Close physical proximity to a nuclear weapon in such a manner as to allow the opportunity to tamper with or damage a nuclear weapon. In the absence of positive control and preventative measures, presence within the exclusion area constitutes unauthorized access. Possession or use of stand-off weapons or systems from outside the exclusion area does not constitute close physical proximity.

alert area. A designated land-based area where delivery systems containing nuclear weapons are located and are postured for immediate reaction.

armed. Equipped with a loaded firearm. A firearm is considered loaded when a magazine is inserted into the magazine well in bolt-operated weapons, or ammunition is physically attached to the weapon in a manner preparing the firearm for immediate use.

balanced survivability assessment. DTRA-conducted assessments of U.S. and allied systems designed to identify vulnerabilities and potential mitigation approaches for critical DoD facilities, including command, control, communication, and intelligence systems, infrastructure, hardened underground facilities, and mobile systems.

BF. A security force of 15 or more personnel (unless otherwise stated), appropriately armed and equipped, whose primary duty is to provide augmentation to the RF and on-duty security force

during those situations that threaten or affect the security of the nuclear weapons concerned. Security force personnel must comprise the initial BF. Subsequent BFs may include appropriately trained and equipped combat support specialists (e.g., RED HORSE combat engineers, EOD technicians, special operations forces). As a final resort, additional BFs may contain non-security force military personnel (support forces or units) that are trained, equipped, and capable of conducting emergency security operations.

CCD. A supporting technique for achieving OPSEC and enhancing S2.

clear zone. An area within the storage site perimeter and around the boundary of the storage site that is free of all obstacles, topographical features, and vegetation exceeding a specified height. The clear zone is designed to facilitate detection and observation of an intruder, to deny protection and concealment to the intruder, to maximize effectiveness of security force weapons, and to reduce the possibility of surprise attack. Clear zones must consist of an area 30 feet (9.1 meters) inside (inner clear zone) and outside (outer clear zone) the site perimeter fence. For areas using two fence systems, the clear zone must consist of 30 feet (9.1 meters) outside the outer fence, the entire area between the fences, and 30 feet (9.1 meters) inside the inner fence.

critical component. A component of a nuclear weapon, nuclear weapon system, or NC2 system that, if bypassed, activated, or tampered with, could result in or contribute to the unauthorized deliberate or inadvertent authorization, prearming, arming, launching, or releasing of a nuclear weapon; the delivery of a nuclear weapon; the unauthorized launching of a combat delivery vehicle carrying a nuclear weapon; or the delivery of a weapon to other than its planned target. These components are normally defined by the Military Departments or by a nuclear weapon system safety group.

custody. Defined in Joint Publication (JP) 1-02.

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

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

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

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

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

deterrence The prevention of action by fear of the consequences.

A state of mind brought about by the existence of a credible threat of unacceptable counteraction.

Includes those activities normally undertaken by security forces and visible to a potential adversary to help discourage any adverse action by making the adversary believe the consequences of the action are unpalatable and unacceptable.

The legal and visible means that serve to discourage hostile attempts to penetrate the perimeter of nuclear facilities. Deterrence is overarching and applies across all environments and configurations.

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

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

EMBER IMMUNE. USSOCOM team that provides physical security assessments to the DoD, the Nuclear Regulatory Commission, and the DOE.

emergency destruction. Destroying nuclear munitions, components, and associated classified material without nuclear yield to render a weapon tactically useless.

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

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

exposed nuclear weapon. A nuclear weapon, including containers or sections that do not provide ballistic protection, that is visible to unauthorized personnel.

facility. Any configuration where a nuclear weapon is located, such as a magazine, M&I facility, ICBM launch facility, or WS3 vault. In all other instances, as defined by JP 1-02.

free zone. The section of a limited area that is physically separated from the areas containing nuclear weapons to facilitate ongoing construction activities. A combination of additional security measures, including sentries, entry controls, and physical barriers, must be established to ensure that the capability to detect and prevent unauthorized entry at the "free zone" barrier is equal to that provided by the nuclear area's permanent barrier system.

hostile act. Defined in JP 1-02.

hostile intent. Defined in JP 1-02.

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

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

incapacitate. To render physically incapable of gaining unauthorized access to a nuclear weapon.

integrated defense. The integration of multidisciplinary active and passive, offensive and defensive capabilities employed to mitigate potential risks and defeat adversary threats to DoD operations.

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

M&I facilities. Those buildings or structures in which nuclear weapon inspections, checkouts, assembly, or maintenance operations are primarily performed.

MIGHTY GUARDIAN. DoD-sponsored nuclear security evaluations designed to evaluate the adequacy of nuclear security policy.

Military Department. Defined in JP 1-02.

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

NSTCA. A DIA-led intelligence community assessment of the capabilities and intentions of a variety of actors to gain unauthorized physical access to a U.S. nuclear weapon. The NSTCA forms the cornerstone of threat planning for nuclear security systems until updated or superseded. As the NSTCA is updated or superseded, implementing guidance for the new intelligence products will be provided by DASD(NM).

nuclear weapon system. One or more nuclear weapons that are on or physically attached to their delivery platform, in combination with all related equipment, materials, services, and personnel required for self-sufficiency. A nuclear weapon system is distinct and different from an NC2 system.

NWSS. The standard of nuclear weapons security that requires measures be taken to deny unauthorized access to nuclear weapons; prevent loss of control; and prevent, to the maximum

extent possible, radiological contamination caused by unauthorized acts. The fundamental tenets of nuclear security are to first deny unauthorized access to nuclear weapons and then, should unauthorized access be gained, take any and all actions necessary to regain control of nuclear weapons immediately.

OPSEC. Defined in JP 1-02.

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

post manning factor or security post validation. Service-distinctive manpower planning term used to develop and allocate or authorize personnel resources. Specifically, those personnel assigned and dedicated to the defense and protection of a nuclear weapon or nuclear weapon system.

priority intelligence requirements. Defined in JP 1-02.

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

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

restricted area. Defined in JP 1-02.

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

risk. Defined in JP 1-02.

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

security awareness. An individual's knowledge of the existence of a security program and understanding and acceptance that the program is relevant to his or her behavior.

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

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

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

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

SRT. A quick response element of at least two armed persons, equipped in accordance with applicable Military Department direction, dedicated to the protection of nuclear resources, and normally tasked with patrolling the protected area and providing the initial response to alarms and detected threats. SRTs may come together to form a fire team. They normally have a mix of weapons, including automatic weapons and grenade launchers, to provide a variety of suppressive capabilities.

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

use control. Positive measures to prevent the deliberate pre-arming, arming, launching, or releasing of nuclear weapons except when directed by competent authority. Use control is applied through a combination of design features, operational procedures, and weapon system safety rules.

vulnerability assessment. Defined in JP 1-02.

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