

## Office of the Secretary of Defense

## § 223.1

RDD, 8850 Richmond Highway, Suite 300, Alexandria, VA 22309.

(3) *Department of the Navy.*

(i) Department of the Navy, Chief of Naval Operations, CNO N09N2, 2000 Navy Pentagon, Washington, DC 20350-2000. (Collateral MDR).

(ii) Department of the Navy, Chief of Naval Operations, CNO N2/N6, 2000 Navy Pentagon, Washington, DC 20350-2000. (Sensitive Compartmented Information MDR).

(4) *Department of the Air Force.* Department of the Air Force, HAF/IMIO (MDR), 1000 Air Force Pentagon, Washington, DC 20330-1000.

(5) *United States Marine Corps.* Commandant of the Marine Corps, HQMC Code PP&O, Security Division (PS), 3000 Marine Corps Pentagon, Room 4A324, Washington, DC 20350-3000

(6) *Defense Advanced Research Projects Agency.* Defense Advanced Research Projects Agency, 3701 N. Fairfax Drive, Arlington, VA 22203-1714.

(7) *Defense Contract Audit Agency.* Director, Defense Contract Audit Agency, Attention: CPS, 8725 John J. Kingman Road, Suite 2135, Fort Belvoir, VA 22060-6219.

(8) *Defense Information Systems Agency.* Defense Information Systems Agency, Attention: Security Division, MPS 6, 5111 Leesburg Pike, Suite 100, Falls Church, VA 22041.

(9) *Defense Intelligence Agency.* Defense Intelligence Agency, Attention: DAN-1A (FOIA), Washington, DC 20340-5100.

(10) *Defense Logistics Agency.* Defense Logistics Agency, Attention: DLA/DSS-S, 8725 John J. Kingman Road, Suite 2533, Fort Belvoir, VA 22060-6221.

(11) *Defense Security Service.* Defense Security Service, Office of FOIA & Privacy, 1340 Braddock Place, Alexandria, VA 22314-1651.

(12) *Defense Threat Reduction Agency.* Defense Threat Reduction Agency, Attention: SCR 8725 John J. Kingman Road, Fort Belvoir, VA 22060-6201.

(13) *Missile Defense Agency.* Missile Defense Agency, Attention: MDA/DS, 7100 Defense Pentagon, Washington, DC 20301-7100.

(14) *National Geospatial-Intelligence Agency.* National Geospatial-Intelligence Agency, Mail Stop D-10, 4600 Sangamore Road, Bethesda, MD 20816-5003.

(15) *National Reconnaissance Office.* National Reconnaissance Office, NRO-MSO-ASG-IMSC-IART<sup>3</sup>, 14675 Lee Road, Chantilly, VA 20151-1715.

(16) *National Security Agency/Central Security Service.* National Security Agency, Declassification Office, DJP5, 9800 Savage Road, Suite 6884, Fort George G. Meade, MD 20755-6884.

(17) *North American Aerospace Defense Command.* HQ NORAD/CSO, 250 Vandenberg St. Ste B016, Peterson AFB, CO 80914.

(18) *U.S. Africa Command.* US Africa Command, Unit 29951, ATTN: COS-FOIA, APO AE 09751.

(19) *U.S. Central Command.* U.S. Central Command, Attention: CCJ6-RDD, 7115 South Boundary Blvd., MacDill AFB, FL 33621-5101.

(20) *U.S. European Command.* U.S. European Command, Attention: ECJ1-AX, Unit 30400, APO AE 09131.

(21) *U.S. Joint Forces Command.* U.S. Joint Forces Command, Code J02SM, 1562 Mitscher Ave., Suite 200, Norfolk, VA 23511-2488.

(22) *U.S. Northern Command.* U.S. Northern Command, HQ USNORTHCOM/CSO, 250 Vandenberg Street, Suite B016, Peterson AFB, CO 80914-3804.

(23) *U.S. Pacific Command.* U.S. Pacific Command, Attention: J151 FOIA, Box 64017, Camp Smith, HI 96861-4017.

(24) *U.S. Southern Command.* U.S. Southern Command, Attention: SCJ2-SM-CFO (FOIA)<sup>3</sup>, 3511 NW 91st Avenue, Miami, FL 33172-1217.

(25) *U.S. Special Operations Command.* U.S. Special Operations Command, Attention: SOCS-SJS-SI (FOIA), 7701 Tampa Point Blvd., MacDill AFB, FL 33621-5323.

(26) *U.S. Strategic Command.* U.S. Strategic Command, Attention: CS50, 901 SAC Blvd., STE 1C17, Offutt AFB, NE 68113-6000.

(27) *U.S. Transportation Command.* U.S. Transportation Command, Chief, Command Information Management, ATTN: TCCSIM, 508 Scott Drive, Scott AFB IL 62225-5357.

(28) *Interagency Security Classification Appeals Panel* <http://www.archives.gov/isoo/oversight-groups/iscap/index.html>.

(29) *Principal Mandatory Declassification Review (MDR) Contacts at Federal Agencies* <http://www.archives.gov/isoo/contact/mdr-contact.html>.

## PART 223—DOD UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION (UCNI)

Sec.

223.1 Purpose.

223.2 Applicability.

223.3 Definitions.

223.4 Policy.

223.5 Responsibilities.

223.6 Procedures-identifying and controlling DoD UCNI.

223.7 Procedures-determination of DoD UCNI.

AUTHORITY: 10 U.S.C. 128 and 5 U.S.C. 552(b)(3).

SOURCE: 77 FR 43506, July 25, 2012, unless otherwise noted.

### § 223.1 Purpose.

This part:

(a) Updates policies, assigns responsibilities and prescribes procedures for the implementation of 10 United States

## § 223.2

## 32 CFR Ch. I (7–1–18 Edition)

Code (U.S.C.) 128, which is the statutory basis for controlling unclassified information on the physical protection of DoD special nuclear material (SNM), SNM equipment, and SNM facilities. Such information is referred to as DoD UCNI, to distinguish it from a similar Department of Energy (DOE) program.

(b) Identifies the authority to be used for denying disclosure of DoD UCNI pursuant to 5 U.S.C. 552.

(c) Supplements security classification guidance contained in DoD Instruction 5210.67,<sup>1</sup> DOE classification guide CG-SS-4,<sup>2</sup> and DoD/DOE joint classification guides by establishing procedures for identifying, controlling, and limiting the dissemination of unclassified information on the physical protection of DoD SNM.

### § 223.2 Applicability.

This part applies to:

(a) Office of the Secretary of Defense, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff 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 Department of Defense (hereinafter referred to collectively as the “DoD Components”).

(b) All SNM, regardless of form, whether in reactor cores or other items under the direct control of the DoD Components (hereinafter referred to as “DoD SNM”).

(c) Nuclear weapons containing SNM that are in DoD custody (hereinafter referred to as “nuclear weapons in DoD custody”).

(d) Contractors, consultants, and grantees of the Department of Defense.

### § 223.3 Definitions.

These terms and their definitions are for the purposes of this part:

(a) *Atomic Energy Defense Programs*. Activities, equipment, and facilities of

the Department of Defense that are capable of the following:

(1) Development, production, testing, sampling, maintenance, repair, modification, assembly, utilization, transportation, or retirement of nuclear weapons or nuclear weapon components.

(2) Production, utilization, or transportation of DoD SNM for military applications.

(3) Safeguarding of activities, equipment, or facilities that support the functions in paragraphs (a)(1) and (a)(2) of this section, including the protection of nuclear weapons, nuclear weapon components, or DoD SNM for military applications at a fixed facility or in transit.

(b) *Document or material*. The physical medium on or in which information is recorded, or a product or substance that contains or reveals information, regardless of its physical form or characteristics.

(c) *DoD UCNI*. Unclassified information on the physical protection of DoD SNM, SNM equipment, and SNM facilities, including unclassified information on the physical protection of nuclear weapons containing SNM that are in DoD custody.

(d) *Information*. Any fact or concept, regardless of the physical form or characteristics of the medium on or in which it is recorded, contained, or revealed.

(e) *Intelligence Community*. An element or agency of the U.S. Government identified in or designated pursuant section 3.5(h) of Executive Order 12333, as amended.

(f) *Reviewing official*. An individual appointed by the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs who may make a determination that a document or material contains, does not contain, or no longer contains DoD UCNI.

(g) *Safeguards*. An integrated system of physical protection, document and material accounting, and control measures designed to deter, prevent, detect, and respond to unauthorized possession, use, or sabotage of DoD SNM, SNM equipment, SNM facilities, or nuclear weapons in DoD custody.

(h) *SNM*. Defined in 42 U.S.C. 2014.

<sup>1</sup>Copies available on the Internet at <http://www.dtic.mil/whs/directives/corres/pdf/521067p.pdf>.

<sup>2</sup>Copies available to authorized recipients from the Director of Classification, Department of Energy.

(i) *SNM equipment.* Equipment, systems, or components whose failure or destruction would cause an impact on safeguarding DoD SNM resulting in an unacceptable interruption to a national security program or an unacceptable impact on the health and safety of the public.

(j) *SNM facility.* A DoD facility that performs a function in support of Atomic Energy Defense Programs whose disruption could reasonably be expected to have a significant adverse effect on safeguarding DoD SNM, the health and safety of the public or the common defense and security.

(k) *Unauthorized dissemination.* The intentional or negligent transfer, in any manner and by any person, of information contained in a document or material determined by a reviewing official to contain DoD UCNI, and so marked in accordance with the procedures in §223.6 of this part, to any person or entity other than an individual or entity authorized access to DoD UCNI in accordance with 10 U.S.C. 128 and this part.

#### § 223.4 Policy.

It is DoD policy that:

(a) Unauthorized dissemination of unclassified information pertaining to security measures, including security plans, procedures, and equipment, for the physical protection of DoD SNM, SNM equipment, SNM facilities, or nuclear weapons in DoD custody is prohibited.

(b) Unclassified information shall be protected as DoD UCNI based on a determination that the unauthorized dissemination of such information could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of DoD SNM, SNM equipment, SNM facilities, or nuclear weapons in DoD custody.

(c) Unclassified information regarding physical protection of DoD SNM and nuclear weapons in DoD custody shall be made publicly available to the fullest extent possible by applying the minimum restrictions, consistent with the requirements of 10 U.S.C. 128, nec-

essary to protect the health and safety of the public or the common defense and security.

(d) This part and title 10 of the Code of Federal Regulations (CFR) part 1017 shall be used as guidance for handling DOE UCNI that is under DoD control.

(e) This part does not prevent a determination that information previously determined to be DoD UCNI is classified information in accordance with Volume 1 of DoD Manual 5200.01<sup>3</sup> and other applicable standards of classification.

#### § 223.5 Responsibilities.

(a) The Under Secretary of Defense for Intelligence (USD(I)) shall oversee the DoD program for controlling DoD UCNI and coordinate DoD compliance with the DOE program for controlling DOE UCNI.

(b) The Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs (ASD(NCB)), under the authority, direction, and control of the Under Secretary of Defense for Acquisition, Technology, and Logistics, shall:

(1) Identify information regarding nuclear weapons security and the protection of SNM at DoD nuclear reactor facilities as DoD UCNI and protect it from unauthorized dissemination, consistent with the requirements of 10 U.S.C. 128 and this part.

(2) Advise the USD(I) on implementation of the DoD UCNI program.

(3) Designate a DoD UCNI reviewing official, who shall be authorized to determine that materials or documents contain, do not contain, or no longer contain DoD UCNI.

(c) The Director, Administration and Management shall provide guidance, as needed, to the Heads of the DoD Components regarding 5 U.S.C. 552, as implemented by 32 CFR part 286, as it applies to the DoD UCNI program.

(d) The Heads of the DoD Components shall identify DoD UCNI within their Component and protect it from unauthorized dissemination, consistent with the requirements of 10 U.S.C. 128 and this part.

<sup>3</sup>Available on the Internet at [http://www.dtic.mil/whs/directives/corres/pdf/520001\\_vol1.pdf](http://www.dtic.mil/whs/directives/corres/pdf/520001_vol1.pdf).

**§ 223.6 Procedures-identifying and controlling DoD UCNI.**

(a) *General.* (1) The decision to protect unclassified information as DoD UCNI shall be based on a 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 or the common defense and security by increasing significantly the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of DoD SNM, SNM equipment, SNM facilities, or nuclear weapons in DoD custody. This is called the “adverse effects test.”

(2) DoD UCNI shall be identified, controlled, marked, transmitted, and safeguarded in the DoD Components, the Intelligence Community, and the North Atlantic Treaty Organization (NATO), and among DoD contractors, consultants, and grantees. Within NATO, DoD UCNI shall be marked, controlled, and safeguarded as “NATO RESTRICTED” information.

(3) Contracts requiring access to or the preparation of unclassified information that is or could be DoD UCNI shall require compliance with this part and any applicable DoD Component regulations, and shall specify requirements for identifying, marking, handling, and safeguarding DoD UCNI.

(b) *Identifying DoD UCNI.* (1) To be designated and protected as DoD UCNI, information must:

(i) Be unclassified.

(ii) Pertain to security measures, including plans, procedures, and equipment, for the physical protection of DoD SNM, SNM equipment, SNM facilities, or nuclear weapons in DoD custody.

(iii) Meet the adverse effects test.

(2) Information shall be protected as DoD UCNI if it qualifies for one or more of the categories listed in § 223.7(c) and meets the criteria in paragraph (b)(1) of this section.

(3) DoD personnel, in making a determination to protect unclassified information as DoD UCNI, shall consider the probability of illegal production of nuclear weapons or of theft, diversion, or sabotage of DoD SNM, SNM equipment, SNM facilities, or nuclear weapons in DoD custody if the information

proposed for protection were made available for public disclosure and dissemination. The cognizant official shall consider how the unauthorized disclosure or dissemination of such information could assist a potential adversary in:

(i) Selecting a target for an act of theft, diversion, or sabotage of nuclear weapons in DoD custody, DoD SNM, SNM equipment, or SNM facilities (e.g., relative importance of a facility or the location, form, and quantity of DoD SNM). Information that can be obtained by observation from public areas outside controlled locations should not be considered as DoD UCNI.

(ii) Planning or committing an act of theft, diversion, or sabotage of nuclear weapons in DoD custody, DoD SNM, SNM equipment, or SNM facilities (e.g., design of security systems; building plans; methods and procedures for transfer, accountability, and handling of nuclear weapons or DoD SNM; or security plans, procedures, and capabilities).

(iii) Measuring the success of an act of theft, diversion, or sabotage of nuclear weapons in DoD custody, DoD SNM, SNM equipment, or SNM facilities (e.g., actual or hypothetical consequences of the sabotage of specific vital equipment or facilities).

(iv) Illegally producing a nuclear explosive device (e.g., unclassified nuclear weapon design information useful in designing a primitive nuclear device; location of unique DoD SNM needed to fabricate such a device; or location of a nuclear weapon).

(v) Dispersing DoD SNM in the environment (e.g., location, form, and quantity of DoD SNM).

(c) Where questions or disagreements arise on designation or continued protection of information as DoD UCNI, the reviewing official appointed by the ASD(NCB) shall make the final determination. If a determination cannot be made because applicable guidance is unclear or does not exist, the document or material in question shall be referred to the reviewing official for a determination.

(d) *Access to DoD UCNI.* (1) No explicit designation or security clearance is required for access to DoD UCNI; however, a person granted access to DoD

UCNI must have a need to know the specific DoD UCNI to which access is granted in the performance of official duties or of DoD-authorized activities.

(2) The individual granting access to DoD UCNI shall notify each person granted such access of applicable regulations, including the physical protection and access requirements, concerning the protection of DoD UCNI as well as any special dissemination limitations that apply to the specific DoD UCNI to which access is being granted, prior to dissemination of the DoD UCNI to the person.

(3) The requirement to notify persons granted access to DoD UCNI of applicable regulations concerning protection and dissemination of DoD UCNI may be met by attachment of an appropriate cover sheet to the front of each document or material containing DoD UCNI prior to its transmittal to the person granted access.

(e) *Marking DoD UCNI.* (1) An unclassified document with DoD UCNI shall be marked "DOD UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION" (or abbreviated "DOD UCNI") at the bottom on: the outside of the front cover, if any; the outside of the back cover, if any; the first page; and each individual page containing DoD UCNI.

(2) Within an unclassified document, an individual page containing DoD UCNI shall be marked to show which of its portions contain DoD UCNI. In marking sections, parts, paragraphs, or similar portions, the parenthetical term "(DCNI)" shall be used and placed at the beginning of the applicable portions.

(3) In a classified document, an individual page that has both DoD UCNI and classified information shall be marked at the top and bottom of the page with the highest security classification of information appearing on that page or with the overall classification of the document. In marking sections, parts, paragraphs, or similar portions, the parenthetical term "(U//DCNI)" shall be used and placed at the beginning of those portions containing DoD UCNI. In a classified document, an individual page that has DoD UCNI, but no classified information, shall be marked "UNCLASSIFIED//DOD UN-

CLASSIFIED CONTROLLED NUCLEAR INFORMATION" (or "UNCLASSIFIED//DOD UCNI") at the top and bottom of the page, unless the page is marked with the overall classification of the document. The DoD UCNI information may be included in the same portion with other classified or unclassified information, if all relevant statutory and regulatory markings and citations are included. Volume 2 of DoD Manual 5200.01<sup>4</sup> provides additional guidance on marking classified documents.

(4) Other material (e.g., electronic media, photographs, films, tapes, or slides) containing DoD UCNI shall be conspicuously marked "DOD UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION" (or "DOD UCNI"), in accordance with paragraphs (d)(1) through (d)(3) of this section, to ensure that a recipient or viewer is aware of the status of the information.

(e) *Dissemination and Transmission.* (1) DoD UCNI may be disseminated among the DoD Components, members of the Intelligence Community, NATO, and DoD contractors, consultants, and grantees on a need-to-know basis for the conduct of official business for the Department of Defense. Dissemination to NATO or other foreign or international entities requires prior review and approval by the appropriate dissemination entity.

(2) Recipients shall be made aware of the status as DoD UCNI for all such information disseminated to them. Transmission of DoD UCNI shall be by means which preclude unauthorized disclosure or dissemination (e.g., secure phone, encrypted email).

(3) Documents containing DoD UCNI shall be marked as prescribed in paragraph (d) of this section. Transmittal documents shall call attention to the presence of DoD UCNI attachments using an appropriate statement in the text or including at the bottom of the transmittal document a statement similar to: "The attached document contains DoD Unclassified Controlled Nuclear Information (DoD UCNI)."

<sup>4</sup>Available on the Internet at [http://www.dtic.mil/whs/directives/corres/pdf/520001\\_vol2.pdf](http://www.dtic.mil/whs/directives/corres/pdf/520001_vol2.pdf).

(4) DoD UCNI transmitted outside the Department of Defense requires application of an expanded marking to explain the significance of the DoD UCNI marking. That may be accomplished by adding the transmittal statement “DEPARTMENT OF DEFENSE/UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION/EXEMPT FROM MANDATORY DISCLOSURE PURSUANT TO 5 U.S.C. 552(b)(3), AS AUTHORIZED BY 10 U.S.C. 128” to the document cover before transfer.

(5) When not commingled with classified information, DoD UCNI may be sent by first-class mail in a single, opaque envelope, or wrapping.

(6) DoD UCNI shall not be discussed or transmitted over an unprotected telephone or telecommunications circuit (to include facsimile transmissions) except in case of an emergency.

(7) Each part of electronically transmitted messages containing DoD UCNI portions shall be marked appropriately. Unclassified messages, including email, with DoD UCNI portions shall have the abbreviation “DOD UCNI” at the top of the message, before the beginning of the text, and the parenthetical marking “(DCNI)” preceding each portion of text containing DoD UCNI information. Classified messages containing DoD UCNI portions shall be marked with the highest classification of information within the message; use the parenthetical marking “(U/DCNI)” preceding each portion of text containing DoD UCNI information.

(8) DoD UCNI processed, stored, or produced on stand-alone or networked computers or other information technology systems shall enforce protection from unauthorized disclosure or dissemination, in accordance with the procedures in paragraph (f) of this section.

(9) A document marked as having DoD UCNI may be reproduced minimally without permission of the originator and consistent with the need to carry out official business.

(f) *Safeguarding DoD UCNI.* (1) During normal working hours, documents and materials determined to contain DoD UCNI shall be safeguarded and con-

trolled by measures designed to reduce the risk of access to DoD UCNI by unauthorized individuals. Particular attention should be paid to areas where DoD UCNI is used or stored if unescorted access by unauthorized individuals is possible.

(2) At the close of business, DoD UCNI shall be stored to preclude disclosure. Storage of such information with other unclassified information in unlocked receptacles (e.g., desks, bookcases) is adequate if Government or Government-contractor internal building security is provided during non-duty hours. When such internal building security is not provided, locked rooms or buildings normally provide adequate after-hours protection. If such protection is not considered adequate, DoD UCNI shall be stored in locked receptacles (e.g., locked file cabinet, locked desk drawer, safe).

(3) Non-record copies of DoD UCNI shall be destroyed by shredding or burning or, if the sensitivity or volume of the information justifies it, in accordance with the procedures specified by Volume 3 of DoD Manual 5200.01<sup>5</sup> for classified information. Record copies of DoD UCNI shall be disposed of in accordance with the DoD Component’s record management regulations. DoD UCNI on magnetic storage media shall be disposed of by overwriting to preclude its reconstruction. DoD UCNI in electronic form shall be deleted and also removed from any desktop trash or recycling files.

(4) Unauthorized dissemination and disclosure of DoD UCNI justifies investigative and administrative actions to determine cause, assess impact, and fix responsibility. The DoD Component that originated the DoD UCNI shall be informed of its unauthorized disclosure and the outcome of the investigative and administrative actions. Unauthorized disclosure of DoD UCNI does not constitute a compromise of classified information.

(g) *Retirement of Document or Material.*

(1) Any unclassified document or material that is not marked as containing DoD UCNI but that may contain DoD

<sup>5</sup> Available on the Internet at [http://www.dtic.mil/whs/directives/corres/pdf/520001\\_vol3.pdf](http://www.dtic.mil/whs/directives/corres/pdf/520001_vol3.pdf).

UCNI shall be marked upon retirement in accordance with the DoD Component's record management regulations.

(2) A document or material marked as containing DoD UCNI is not required to be reviewed upon, or subsequent, to retirement. Retired documents or materials shall be reviewed in accordance with paragraph (h) of this section upon a request for their release made pursuant to 5 U.S.C. 552.

(h) *Requests for Public Release of UCNI.* (1) Pursuant to 10 U.S.C. 128, information that qualifies as DoD UCNI is exempt from mandatory disclosure pursuant to 5 U.S.C. 552. Requests for the public release of DoD UCNI shall be denied, in accordance with procedures established in 32 CFR part 286, pursuant to 5 U.S.C. 552(b)(3), citing 10 U.S.C. 128 as authority.

(2) Requests for DOE UCNI contained within DoD documents shall also be denied pursuant to 5 U.S.C. 552(b)(3), but 42 U.S.C. 2168 shall be cited, after formal FOIA consultation with the DOE, as the basis for invoking the exemption. Requests for DOE documents will be formally referred to DOE for final adjudication and response to the requestor.

(3) The reviewing official designated by the ASD (NCB) shall review any retired DoD UCNI document or material upon a request for its release made pursuant to 5 U.S.C. 552.

#### § 223.7 Procedures-determination of DoD UCNI.

(a) *Use of the Guidelines.* (1) The guidelines in this section are the basis for determining what unclassified information regarding the physical protection of DoD SNM, SNM equipment, SNM facilities, or nuclear weapons in DoD custody, in a given technical or programmatic subject area are to be designated as DoD UCNI.

(2) The decision to protect unclassified information as DoD UCNI shall be based on a 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 or the common defense and security by significantly increasing the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of SNM,

SNM equipment, SNM facilities, or nuclear weapons in DoD custody.

(b) *General Guidance.* (1) Unclassified information relating to the physical protection of DoD SNM, SNM equipment, SNM facilities, or nuclear weapons in DoD custody is to be protected from public disclosure to prevent the adverse effects identified in paragraph (a)(2) of this section. Public availability of information that would not result in such adverse effects is not to be restricted.

(2) In controlling DoD SNM information, only the minimum restrictions needed to protect the health and safety of the public or the common defense and security shall be applied to prohibit the disclosure and dissemination of DoD UCNI.

(3) Any information that has been, or is, widely and irretrievably disseminated in the public domain and whose dissemination was not, or is not, under Government control is exempt from control under these guidelines. However, the fact that information is in the public domain is not a sufficient basis for determining that similar or updated Government-owned and -controlled information in another document or other material is not, or is no longer, DoD UCNI; case-by-case determinations are required.

(c) *Topical Guidance.* DoD Components shall consider the topics discussed in this section during the preparation of unclassified information that addresses the physical protection of DoD SNM or nuclear weapons in DoD custody to determine if it qualifies for control as DoD UCNI.

(1) *Vulnerability Assessments.* (i) General vulnerabilities that could be associated with specific DoD SNM, SNM equipment, SNM facility locations, or DoD nuclear weapons storage facilities.

(ii) The fact that DoD SNM or nuclear weapons facility security-related projects or upgrades are planned or in progress, if not observable from a public area.

(iii) Identification and description of security system components intended to mitigate the consequences of an accident or act of sabotage at a DoD SNM or nuclear weapons facility.

(2) *Material Control and Accountability.* (i) Total quantity or categories of DoD SNM at a facility.

(ii) Control and accountability plans or procedures.

(iii) Receipts that, cumulatively, would reveal quantities and categories of DoD SNM of potential interest to an adversary.

(iv) Measured discards, decay losses, or losses due to fission and transmutation for a reporting period.

(v) Frequency and schedule of DoD SNM inventories.

(3) *Facility Description.* (i) Maps, conceptual design, and construction drawings of a DoD SNM or nuclear weapons facility showing construction characteristics of building(s) and associated electrical systems, barriers, and backup power systems not observable from a public area.

(ii) Maps, plans, photographs, or drawings of man-made or natural features in a DoD SNM or nuclear weapons facility not observable from a public area; e.g., tunnels, storm or waste sewers, water intake and discharge conduits, or other features having the potential for concealing surreptitious movement.

(iii) Communications and computer network configurations and capabilities.

(4) *Intrusion Detection and Security Alarm Systems.* (i) Information on the layout or design of security and alarm systems at a specific DoD SNM or nuclear weapons facility, if the information is not observable from a public area.

(ii) The fact that a particular system make or model has been installed at a specific DoD SNM or nuclear weapons facility, if the information is not observable from a public area.

(iii) Performance characteristics of installed systems.

(5) *Keys, Locks, Combinations, and Tamper-Indicating Devices.* (i) Types and models of keys, locks, and combinations of locks used in DoD SNM or nuclear weapons facilities and during shipment.

(ii) Method of application of tamper-indicating devices.

(iii) Vulnerability information available from unclassified vendor specifications.

(6) *Threat Response Capability and Procedures.* (i) Information about arrangements with local, State, and Federal law enforcement agencies of potential interest to an adversary.

(ii) Information in “non-hostile” contingency plans of potential value to an adversary to defeat a security measure, e.g., fire, safety, nuclear accident, radiological release, or other administrative plans.

(iii) Required response time of security forces.

(7) *Physical Security Evaluations.* (i) Method of evaluating physical security measures not observable from public areas.

(ii) Procedures for inspecting and testing communications and security systems.

(8) *In-Transit Security.* (i) Fact that a shipment is going to take place.

(ii) Specific means of protecting shipments.

(iii) Number and size of packages.

(iv) Mobile operating and communications procedures that an adversary could exploit.

(v) Information on mode, routing, protection, communications, and operations that must be shared with law enforcement or other civil agencies, but not visible to the public.

(vi) Description and specifications of transport vehicle compartments or security systems not visible to the public.

(9) *Information on Nuclear Weapon Stockpile and Storage Requirements, Nuclear Weapon Destruction and Disablement Systems, and Nuclear Weapon Physical Characteristics.* Refer to DOE CG-SS-4 for guidance about the physical protection of information on nuclear weapon stockpile and storage requirements, nuclear weapon destruction and disablement systems, and nuclear weapon physical characteristics that may, under certain circumstances, be unclassified. Such information meeting the adverse effects test shall be protected as DoD UCNL.

## PART 226—SHELTER FOR THE HOMELESS

Sec.

226.1 Purpose.

226.2 Applicability.