



Department of Defense DIRECTIVE

NUMBER 5210.83

November 15, 1991

Administrative Reissuance Incorporating Change 1, November 16, 1994

ASD(C3I)

SUBJECT: Department of Defense Unclassified Controlled Nuclear Information (DoD UCNI)

- References:
- (a) Section 128 of title 10, United States Code
 - (b) [DoD 5400.7-R](#) , "DoD Freedom of Information Act Program," October 1990, authorized by [DoD Directive 5400.7](#), May 13, 1988
 - (c) Section 552 of title 5, United States Code
 - (d) CG-W-5, "Joint DOE/DoD Nuclear Weapon Classification Policy Guide," the Department of Energy and the Department of Defense, January 1984
 - (e) through (k), see enclosure E1.

1. PURPOSE

This Directive implements reference (a) by establishing policy, assigning responsibilities, and prescribing procedures for identifying, controlling, and limiting the dissemination of unclassified information on the physical protection of DoD special nuclear material (SNM), equipment, and facilities. That information shall be referred to as " the Department of Defense Unclassified Controlled Nuclear Information (DoD UCNI)," to distinguish it from a similar Department of Energy (DoE) program.

2. APPLICABILITY AND SCOPE

This Directive:

- 2.1. Applies to the Office of the Secretary of Defense (OSD), the Military

Departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Unified and Specified Commands, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

2.2. Implements reference (a), which is the statutory basis for controlling the DoD UCNI in the Department of Defense. Reference (a) also constitutes the authority for invoking reference (b) to prohibit mandatory disclosure of DoD UCNI under the "Freedom of Information Act (FOIA)" in reference (c).

2.3. Supplements the security classification guidance contained in reference (d) and CG-SS-1 and DoD Instruction 5210.67 (references (e) and (f)) by establishing procedures for identifying, controlling, and limiting the dissemination of unclassified information on the physical protection of DoD SNM.

2.4. Applies to all SNM, regardless of form, in reactor cores to other items under the direct control of the DoD Components.

2.5. Applies equally to DoE UCNI under DoD control, except the statute applicable to DoE UCNI (42 U.S.C. 2011 et seq., reference (g)) must be used with the concurrence of the DoE as the basis for invoking the FOIA (Section 552 of 10 U.S.C., reference (c)).

3. DEFINITIONS

Terms used in this Directive are defined in enclosure E2.

4. POLICY

It is DoD policy:

4.1. To prohibit the unauthorized dissemination of unclassified information on security measures, including security plans, procedures, and equipment for the physical protection of DoD SNM, equipment, or facilities.

4.2. That 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 a significant 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, equipment, or facilities.

4.3. That Government information 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 (reference (a)) necessary to protect the health and safety of the public or the common defense and security.

4.4. That nothing in this Directive prevents a determination that information previously determined to be DoD UCNI is classified information under applicable standards of classification.

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence shall:

5.1.1. Administer the DoD program for controlling DoD UCNI.

5.1.2. Coordinate DoD compliance with the DoE program for controlling DoE UCNI.

5.1.3. Prepare and maintain the reports required by 10 U.S.C. 128 (reference (a)).

5.2. The Assistant Secretary of Defense (Public Affairs) shall provide guidance to the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) (ASD(C3I)), other elements of the OSD, and the Heads of the DoD Components on the FOIA (5 U.S.C. 552, reference (c)), as implemented in DoD 5400.7-R (reference (b)), as it applies to the DoD UCNI Program.

5.3. The Heads of the DoD Components shall:

5.3.1. Implement this Directive in their DoD Components.

5.3.2. Advise the ASD(C3I) of the following, when information not in the guidelines in enclosure E4. is determined to be DoD UCNI:

5.3.2.1. Identification of the type of information to be controlled as DoD UCNI. It is not necessary to report each document or numbers of documents.

5.3.2.2. Justification for identifying the type of information as DoD

UCNI, based on the guidelines in enclosure E4. and prudent application of the adverse effects test.

6. PROCEDURES

Enclosure E3. outlines the procedures for controlling DoD UCNI. Enclosure E4. provides general and topical guidelines for identifying information that may qualify for protection as DoD UCNI. The procedures and guidelines in enclosures E3. and E4. complement the DoD Component programs to protect other DoD-sensitive unclassified information and may be used with them.

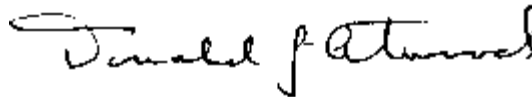
7. INFORMATION REQUIREMENTS

7.1. Section 128 of 10 U.S.C. (reference (a)) requires that the Secretary of Defense prepare on a quarterly basis a report to be made available on the request of any interested person. Enclosure E3. outlines the procedures for preparing the quarterly report.

7.2. The report is exempt from licensing in accordance with DoD 7750.5-M, paragraph 5.4.5. (reference (h)).

8. EFFECTIVE *DATE*

This Directive is effective *immediately*.



Donald J. Atwood
Deputy Secretary of Defense

Enclosures - 4

1. References, continued
2. Definitions
3. Procedures for Identifying and Controlling DoD UCNI
4. Guidelines for the Determination of DoD UCNI

E1. ENCLOSURE 1

REFERENCES, continued

- (e) CG-SS-1, "Safeguards and Security Classification Guide," the Department of Energy, September 1985
- (f) [DoD Instruction 5210.67](#), "Special Nuclear Material Information, Security Classification Guidance," December 3, 1982
- (g) Section 2011 et seq. of title 42, United States Code
- (h) DoD 7750.5-M, "DoD Procedures for Management of Information Requirements," November 1986, authorized by DoD Directive 7750.5, "Management and Control of Information Requirements," August 7, 1986
- (i) DoE GG-2, "Department of Energy Unclassified Controlled Nuclear Information General Guidelines," the Department of Energy, August 1989
- (j) Department of Energy Order 5635.4, "Protection of Unclassified Controlled Nuclear Information," February 3, 1988
- (k) Department of Energy Order 5650.3, "Identification of Unclassified Controlled Nuclear, Information," February 29, 1988

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. Atomic Energy Defense Programs. Activities, equipment, and facilities of the Department of Defense used or engaged in support of the following:

E2.1.1.1. Development, production, testing, sampling, maintenance, repair, modification, assembly, utilization, transportation, or retirement of nuclear weapons or nuclear weapon components.

E2.1.1.2. Production, utilization, or transportation of DoD SNM for military applications.

E2.1.1.3. Safeguarding of activities, equipment, or facilities that support the functions in definitions E2.1.1.1. and E2.1.1.2., above, including the protection of nuclear weapons, nuclear weapon components, or DoD SNM for military applications at a fixed facility or in transit.

E2.1.2. Authorized Individual. A person who has been granted routine access to specific DoD UCNI under 10 U.S.C. 128 (reference (a)).

E2.1.3. Denying Official. An individual who denies a request made under 5 U.S.C. 552 for all, or any portion, of a document or material containing DoD UCNI.

E2.1.4. Document or Material. The physical medium on, or in, which information is recorded, or a product or substance which contains or reveals information, regardless of its physical form or characteristics.

E2.1.5. 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.

E2.1.6. Reviewing Official. An individual who may make a determination that a document or material contains, does not contain, or no longer contains DoD UCNI.

E2.1.7. Safeguards. An integrated system of physical protection, material accounting, and material control measures designed to deter, prevent, detect, and respond to unauthorized possession, use, or sabotage of DoD SNM, equipment or facilities.

E2.1.8. Special Nuclear Material Facility. A DoD facility that performs a sensitive function (see definition E2.1.9., below).

E2.1.9. Sensitive Function. A function in support of atomic energy defense programs whose disruption could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security (see definition E2.1.1., above).

E2.1.10. Special Nuclear Material (SNM). Plutonium, uranium enriched in the isotope-233 or in the isotope-235, except source material or any material artificially enriched by any of the foregoing.

E2.1.11. Special Nuclear Material 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.

E2.1.12. 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 Enclosure E3., to any person or entity other than an authorized individual or a person granted special access to specific DoD UCNI under 10 U.S.C. 128 (reference (a)).

E3. ENCLOSURE 3

PROCEDURES FOR IDENTIFYING AND CONTROLLING DoD UCNI

E3.1. GENERAL

E3.1.1. The Secretary of Defense's authority for prohibiting the unauthorized disclosure and dissemination of DoD UCNI may be exercised by the Heads of the DoD Components and by the officials to whom such authority is specifically delegated by the Heads of the DoD Components. These procedures for identifying and controlling DoD UCNI are provided as guidance for the Heads of the DoD Components to implement the Secretary of Defense's authority to prohibit the unauthorized dissemination of unclassified information on security measures, including security plans, procedures, and equipment, for the physical protection of DoD SNM, equipment, or facilities.

E3.1.2. 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 increasing significantly the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of DoD SNM, equipment, or facilities.

E3.1.3. Government information 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 (reference (a)) necessary to protect the health and safety of the public or the common defense and security.

E3.1.4. DoD personnel, in making a determination to protect unclassified information as DoD UCNI, shall consider the probability of an illegal production, theft, diversion, or sabotage if the information proposed for protection were made available for public disclosure and dissemination. The determination to protect specific documents or information is not related to the ability of DoD UCNI to be obtained by other sources. For determining the control of DoD UCNI, the cognizant official should consider how the unauthorized disclosure or dissemination of such information could assist a potential adversary in the following:

E3.1.4.1. Selecting a target for an act of theft, diversion, or sabotage of DoD SNM, equipment, or 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.

E3.1.4.2. Planning or committing an act of theft, diversion, or sabotage of DoD SNM, equipment, or facilities (e.g., design of security systems; building plans; methods and procedures for transfer, accountability, and handling of DoD SNM; or security plans, procedures, and capabilities).

E3.1.4.3. Measuring the success of an act of theft, diversion, or sabotage of DoD SNM, equipment, or facilities (e.g., actual or hypothetical consequences of the sabotage of specific vital equipment or facilities).

E3.1.4.4. 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).

E3.1.4.5. Dispersing DoD SNM in the environment (e.g., location, form, and quantity of DoD SNM).

E3.1.5. DoD UCNI shall be identified, controlled, marked, transmitted, and safeguarded in the DoD Components, the North Atlantic Treaty Organization (NATO), and among DoD contractors, consultants, and grantees authorized to conduct official business for the Department of Defense. Contracts requiring the preparation of unclassified information that could be DoD UCNI shall have the requirements for identifying and controlling the DoD UCNI.

E3.1.6. DoE GG-2 and DoE Orders 5635.4 and 5650.3 (references (i), (j), and (k)) provide background on implementation of the UCNI Program in the DoE. The DoD Components maintaining custody of DoE UCNI should refer to those documents for its identification and control.

E3.2. IDENTIFYING DoD UCNI

E3.2.1. To be considered for protection as DoD UCNI, the information must:

E3.2.1.1. Be unclassified.

E3.2.1.2. Pertain to security measures, including plans, procedures, and equipment, for the physical protection of DoD SNM, equipment, or facilities.

E3.2.1.3. Meet the adverse effects test; i.e., 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, equipment, or facilities.

E3.2.2. Information, in the categories in section E4.3. of enclosure E4., about DoD SNM should be considered for protection as DoD UCNI.

E3.2.3. Material originated before the effective date of those procedures, which is found in the normal course of business to have DoD UCNI, shall be protected as DoD UCNI. There is no requirement to conduct detailed file searches to retroactively identify and control DoD UCNI. As existing documents or materials are withdrawn from file, they should be reviewed to determine if they meet the criteria for protection as DoD UCNI and marked and controlled, accordingly.

E3.3. ACCESS TO DOD UCNI

E3.3.1. A Reviewing Official is an Authorized Individual for documents or materials that the Reviewing Official determines to contain DoD UCNI. An Authorized Individual, for DoD UCNI, may determine that another person is an Authorized Individual who may be granted routine access to the DoD UCNI, and who may further disseminate the DoD UCNI under the procedures specified in paragraph E3.3.5., below. This recipient of DoD UCNI from an Authorized Individual is also an Authorized Individual for the specific DoD UCNI to which routine access has been granted. An Authorized Individual designates another person to be an Authorized Individual by the act of giving that person a document or material that contains DoD UCNI. No explicit designation or security clearance is required. This second Authorized Individual may further disseminate the UCNI under the procedures specified in paragraph E3.3.5., below.

E3.3.2. A person granted routine access to DoD UCNI must have a need-to-know the specific DoD UCNI in the performance of official duties or of DoD-authorized activities. The recipient of the document or material shall be informed of the physical protection and access requirements for DoD UCNI. In addition to a need-to-know, the person must meet at least one of the following requirements:

E3.3.2.1. The person is a U.S. citizen who is one of the following:

E3.3.2.1.1. A Federal Government employee or member of the U.S. Armed Forces;

E3.3.2.1.2. An employee of a Federal Government contractor, subcontractor, or of a prospective Federal Government contractor or subcontractor who will use the DoD UCNI for the purpose of bidding on a Federal Government contract or subcontract;

E3.3.2.1.3. A Federal Government consultant or DoD advisory committee member;

E3.3.2.1.4. A Member of Congress;

E3.3.2.1.5. A staff member of a congressional committee or of an individual Member of Congress;

E3.3.2.1.6. The Governor of a State or designated State government official or representative;

E3.3.2.1.7. A local government official or an Indian tribal government official; or

E3.3.2.1.8. A member of a State, local, or Indian tribal law enforcement or emergency response organization.

E3.3.2.2. The person is other than a U.S. citizen, and is one of the following:

E3.3.2.1.1. A Federal Government employee or a member of the U.S. Armed Forces;

E3.3.2.2.2. An employee of a Federal Government contractor or subcontractor; or

E3.3.2.2.3. A Federal Government consultant or DoD advisory committee member.

E3.3.2.3. The person may be other than a U.S. citizen who is not otherwise eligible for routine access to DoD UCNI under paragraph E3.2.2., above, but who requires routine access to specific DoD UCNI in conjunction with one of the following:

E3.3.2.3.1. An international nuclear cooperative activity approved by

the Federal Government;

E3.3.2.3.2. U.S. diplomatic dealings with foreign government officials;

or

E3.3.2.3.3. Provisions of treaties, mutual defense acts, or Government contracts or subcontracts.

E3.3.3. A person not authorized routine access to DoD UCNI under paragraph E3.3.2., above, may submit a request for special access to DoD UCNI to Heads of DoD Components, or their designated representative, as appropriate. A special access request must include the following information:

E3.3.3.1. The name, current residence or business address, birthplace, birth date, and country of citizenship of the person submitting the request;

E3.3.3.2. A description of the DoD UCNI for which special access is being requested;

E3.3.3.3. A description of the purpose for which the DoD UCNI is needed;
and

E3.3.3.4. Certification by the requester of his or her understanding of, and willingness to abide by, the requirements for the protection of DoD UCNI contained in this Directive.

E3.3.4. Heads of DoD Components, or their designated representative, shall base his or her decision to grant special access to DoD UCNI on an evaluation of the following criteria:

E3.3.4.1. The sensitivity of the DoD UCNI for which special access is being requested (i.e., the worst-case, adverse effect on the health and safety of the public or the common defense and security which would result from unauthorized use of the DoD UCNI);

E3.3.4.2. The purpose for which the DoD UCNI is needed (e.g., the DoD UCNI will be used for commercial or other private purposes, or will be used for public benefit to fulfill statutory or regulatory responsibilities);

E3.3.4.3. The likelihood of an unauthorized dissemination by the requester of the DoD UCNI; and

E3.3.4.4. The likelihood of the requester using the DoD UCNI for illegal purposes.

E3.3.5. Heads of DoD Components, or their designated representative, shall attempt to notify a person who requests special access to DoD UCNI within 30 days of receipt of the request as to whether or not special access to the requested DoD UCNI is granted. If a final determination on the request cannot be made within 30 days of receipt of the request, Heads of DoD Components, or their designated representative, shall notify the requester, within 30 days of the request, as to when the final determination on the request may be made.

E3.3.6. A person granted special access to specific UCNI is not an Authorized Individual and shall not further disseminate the DoD UCNI to which special access has been granted.

E3.3.7. An Authorized Individual granting routine access to specific DoD UCNI to another person shall notify each person granted access (other than when the person being granted such access is a Federal Government employee, a member of the U.S. Armed Forces, or an employee of a Federal Government contractor or subcontractor) of applicable regulations concerning the protection of DoD UCNI and of any special dissemination limitations that the Authorized Individual determines to apply for the specific DoD UCNI to which routine access is being granted.

E3.3.8. Heads of DoD Components, or their designated representative, shall notify each person granted special access to DoD UCNI of applicable regulations concerning the protection of DoD UCNI prior to dissemination of the DoD UCNI to the person.

E3.3.9. The requirement to notify persons granted routine access or special access to specific 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.

E3.4. MARKINGS

E3.4.1. An unclassified document with DoD UCNI shall be marked "DoD Unclassified Controlled Nuclear Information" at the bottom on the outside of the front cover, if any, and on the outside of the back cover, if any.

E3.4.2. In an unclassified document, an individual page that has DoD UCNI shall be marked to show which of its portions contain DoD UCNI information. In marking sections, parts, paragraphs, or similar portions, the parenthetical term "(DoD UCNI)" shall be used and placed at the beginning of those portions with DoD UCNI.

E3.4.3. 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. In marking sections, parts, paragraphs, or similar portions, the parenthetical term "(DoD UCNI)" shall be used and placed at the beginning of those portions with DoD UCNI. In a classified document, an individual page that has DoD UCNI, but no classified information, shall be marked "DoD Unclassified Controlled Information" at the bottom of the page. The DoD UCNI marking may be combined with other markings, if all relevant statutory and regulatory citations are included.

E3.4.4. Other material (e.g., photographs, films, tapes, or slides) shall be marked "DoD Unclassified Controlled Nuclear Information" to ensure that a recipient or viewer is aware of the status of the information.

E3.5. DISSEMINATION AND TRANSMISSION

E3.5.1. DoD UCNI may be disseminated in the DoD Components, the NATO, and among the DoD contractors, consultants, and grantees on a need-to-know basis to conduct official business for the Department of Defense. Recipients shall be made aware of the status of such information, and transmission shall be by means to preclude unauthorized disclosure or dissemination. Contracts that shall require access to DoD UCNI shall require compliance with this Directive and the DoD Component regulations and have the requirements for the marking, handling, and safeguarding of DoD UCNI.

E3.5.2. DoD holders of DoD UCNI are authorized to convey such information to officials in other Departments or Agencies on a need-to-know basis to fulfill a Government function. Transmittal documents shall call attention to the presence of DoD UCNI attachments using an appropriate statement in the text, or marking at the bottom of the transmittal document, that "The attached document contains DoD Unclassified Controlled Nuclear Information (DoD UCNI)." Similarly, documents transmitted shall be marked, as prescribed in section E3.5.1., above.

E3.5.3. 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 typing or stamping the following statement on the document before transfer:

DEPARTMENT OF DEFENSE
UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION
EXEMPT FROM MANDATORY DISCLOSURE
(5 U.S.C. 552(b)(3), as authorized by 10 U.S.C.128)

E3.5.4. When not commingled with classified information, DoD UCNI may be sent by first-class mail in a single, opaque envelope or wrapping.

E3.5.5. DoD UCNI may only be discussed or transmitted over an unprotected telephone or telecommunications circuit (to include facsimile transmissions) in an emergency.

E3.5.6. Each part of electronically transmitted messages with DoD UCNI shall be marked appropriately. Unclassified messages with DoD UCNI shall have the abbreviation "DoD UCNI" before the beginning of the text.

E3.5.7. DoD UCNI may be processed, stored, or produced on stand-alone personal computers, or shared-logic word processing systems, if protection from unauthorized disclosure or dissemination, in accordance with the procedures in section E3.6., below, can be ensured.

E3.5.8. 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.

E3.6. SAFEGUARDING DoD UCNI

E3.6.1. During normal working hours, documents determined to have DoD UCNI shall be placed in an out-of-sight location, or otherwise controlled, if the work area is accessible to unescorted personnel.

E3.6.2. At the close of business, DoD UCNI material shall be stored so to preclude disclosure. Storage of such material with other unclassified documents in unlocked receptacles; i.e., file cabinets, desks, or bookcases, is adequate, when normal Government or Government-contractor internal building security is provided during nonduty 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 material shall be stored in locked receptacles; i.e., file cabinets, desks, or bookcases.

E3.6.3. Nonrecord copies of DoD UCNI materials must be destroyed by tearing each copy into pieces to reasonably preclude reconstruction and placing the pieces in regular trash containers. If the sensitivity or volume of the information justifies it, DoD UCNI material may be destroyed in the same manner as classified material rather than by tearing. Record copies of DoD UCNI documents shall be disposed of, in accordance with the DoD Components' record management regulations. DoD UCNI on magnetic storage media shall be disposed of by overwriting to preclude its reconstruction.

E3.6.4. The unauthorized disclosure of DoD UCNI material does not constitute disclosure of DoD information that is classified for security purposes. Such 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 information shall be informed of its unauthorized disclosure and the outcome of the investigative and administrative actions.

E3.7. RETIREMENT OF DOCUMENT OR MATERIAL

E3.7.1. Any unclassified document or material which is not marked as containing DoD UCNI but which may contain DoD UCNI shall be marked upon retirement in accordance with the DoD Components record management regulations.

E3.7.2. A document or material marked as containing DoD UCNI is not required to be reviewed by a Reviewing Official upon or subsequent to retirement. A Reviewing Official shall review any retired document or material upon a request for its release made under 5 U.S.C. 552 (reference (c)).

E3.8. REQUESTS FOR PUBLIC RELEASE OF DoD UCNI

DoD 5400.7-R (reference (b)) applies. Information that qualifies as DoD UCNI, under 10 U.S.C. 128 (reference (a)), is exempt from mandatory disclosure under 5 U.S.C. 552 (reference (c)). Consequently, requests for the public release of DoD UCNI shall be denied under Section 552(b)(3) of reference (c), citing reference (a) as authority.

E3.9. REPORTS

The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)) shall prepare and maintain the quarterly reports required by 10 U.S.C. 128 (reference (a)). The Heads of the DoD Components shall advise the ASD(C3I) when information not in the guidelines in enclosure E4. is determined to be DoD UCNI. Those reports shall have the following information:

E3.9.1. Identification of the information to be controlled as DoD UCNI. It is not necessary to report each document or numbers of documents.

E3.9.2. Justification for identifying the type of information to be controlled as DoD UCNI.

E3.9.3. Certification that only the minimal information necessary to protect the health and safety of the public or the common defense and security is being controlled as DoD UCNI.

E4. ENCLOSURE 4

GUIDELINES FOR THE DETERMINATION OF DoD UCNI

E4.1. USE OF DETERMINATION OF DoD UCNI GUIDELINES

E4.1.1. These guidelines for determining DoD UCNI are the basis for determining what unclassified information about the physical protection of DoD SNM, equipment, or facilities in a given technical or programmatic subject area is DoD UCNI.

E4.1.2. 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 increasing significantly the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of SNM, equipment, or facilities.

E4.2. GENERAL

E4.2.1. The policy for protecting unclassified information about the physical protection of DoD SNM, equipment, or facilities is to protect the public's interest by controlling certain unclassified Government information so to prevent the adverse effects described in section 4. of this Directive and in enclosure E3., without restricting public availability of information that would not result in those adverse effects.

E4.2.2. 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.

E4.2.3. Any material that has been, or is, widely and irretrievably disseminated into 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 material is not, or is no longer, DoD UCNI; case-by-case determinations are required.

E4.3. TOPICAL GUIDANCE

The following elements of information shall be considered by the DoD Components during the preparation of unclassified information about the physical protection of DoD SNM to determine if it qualifies for control as DoD UCNI:

E4.3.1. Vulnerability Assessments

E4.3.1.1. General vulnerabilities that could be associated with specific DoD SNM, equipment, or facility locations.

E4.3.1.2. The fact that DoD SNM facility security-related projects or upgrades are planned or in progress.

E4.3.1.3. Identification and description of security system components intended to mitigate the consequences of an accident or act of sabotage at a DoD SNM facility.

E4.3.2. Material Control and Accountability

E4.3.2.1. Total quantity or categories of DoD SNM at a facility.

E4.3.2.2. Control and accountability plans or procedures.

E4.3.2.3. Receipts that, cumulatively, would reveal quantities and categories of DoD SNM of potential interest to an adversary.

E4.3.2.4. Measured discards, decay losses, or losses due to fission and transmutation for a reporting period.

E4.3.2.5. Frequency and schedule of DoD SNM inventories.

E4.3.3. Facility Description

E4.3.3.1. Maps, conceptual design, and construction drawings of a DoD SNM facility showing construction characteristics of building and associated electrical systems, barriers, and back-up power systems not observable from a public area.

E4.3.3.2. Maps, plans, photographs, or drawings of man-made or natural features in a DoD SNM facility not observable from a public area; i.e., tunnels, storm or waste sewers, water intake and discharge conduits, or other features having the potential for concealing surreptitious movement.

E4.3.4. Intrusion Detection and Security Alarm Systems

E4.3.4.1. Information on the layout or design of security and alarm systems at a specific DoD SNM facility, if the information is not observable from a public area.

E4.3.4.2. The fact that a particular system make or model has been installed at a specific DoD SNM facility, if the information is not observable from a public area.

E4.3.4.3. Performance characteristics of installed systems.

E4.3.5. Keys, Locks, Combinations, and Tamper-Indicating Devices

E4.3.5.1. Types and models of keys, locks, and combinations of locks used in DoD SNM facilities and during shipment.

E4.3.5.2. Method of application of tamper-indicating devices.

E4.3.5.3. Vulnerability information available from unclassified vendor specifications.

E4.3.6. Threat Response Capability and Procedures

E4.3.6.1. Information about arrangements with local, State, and Federal law enforcement Agencies of potential interest to an adversary.

E4.3.6.2. Information in "nonhostile" contingency plans of potential value to an adversary to defeat a security measure; i.e., fire, safety, nuclear accident, radiological release, or other administrative plans.

E4.3.6.3. Required response time of security forces.

E4.3.7. Physical Security Evaluations

E4.3.7.1. Method of evaluating physical security measures not observable from public areas.

E4.3.7.2. Procedures for inspecting and testing communications and security systems.

E4.3.8. In-Transit Security

E4.3.8.1. Fact that a shipment is going to take place.

E4.3.8.2. Specific means of protecting shipments.

E4.3.8.3. Number and size of packages.

E4.3.8.4. Mobile operating and communications procedures that could be exploited by an adversary.

E4.3.8.5. 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.

E4.3.8.6. Description and specifications of transport vehicle compartments or security systems not visible to the public.

E4.3.9. Information on Nuclear Weapon Stockpile and Storage Requirements, Nuclear Weapon Destruction and Disablement Systems and Nuclear Weapon Physical Characteristics. Refer to CG-W-5 (reference (d)) 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 UCNI.