



Department of Defense INSTRUCTION

NUMBER 5210.02

June 3, 2011

Incorporating Change 2, August 21, 2018

USD(A&S)

SUBJECT: Access to and Dissemination of Restricted Data and Formerly Restricted Data

References: See Enclosure 1

1. **PURPOSE.** In accordance with the authority in DoD Directive 5143.01 (Reference (a)), this Instruction:

a. Reissues DoD Directive 5210.2 (Reference (b)) as a DoD Instruction to establish policies, assign responsibilities, and prescribe procedures governing access to, and dissemination of data classified as Restricted Data (RD) and Formerly Restricted Data (FRD) by the DoD.

b. Implements sections 2153 and 2161 through 2165 of title 42, United States Code (also known and hereinafter referred to as the "Atomic Energy Act of 1954, as amended" (Reference (c))) and Part 1045 of title 10, Code of Federal Regulations (Reference (d)).

2. **APPLICABILITY.** This Instruction applies to OSD, 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 DoD (hereinafter referred to collectively as the "DoD Components").

3. **DEFINITIONS.** See Glossary.

4. **POLICY.** It is DoD policy that:

a. Access to and dissemination of RD and FRD information within and between DoD Components will be governed by the same criteria that governs the access to other classified information, which is contained in Volume 1 of DoDM 5200.01, DoDM-5200.02, and DoD 5220.22-R (References (e) through (g)), and by the procedures identified within this Instruction.

b. Classification and declassification of RD and FRD information will be governed by the criteria and procedures identified within this Instruction and in Part 1045 of Title 10 (Reference (d)).


5. RESPONSIBILITIES. See Enclosure 2.

6. PROCEDURES. Procedures for implementing this Instruction are described in Enclosure 3.

7. RELEASABILITY. This Instruction is available on the Directives Division Website at <http://www.esd.whs.mil/DD/>.

8. SUMMARY OF CHANGE 2. The change to this issuance reassigns the office of primary responsibility for this issuance to the Under Secretary of Defense for Acquisition and Sustainment in accordance with the July 13, 2018 Deputy Secretary of Defense memorandum (Reference (h)).

9. EFFECTIVE DATE. This Instruction is effective June 3, 2011.



Michael G. Vickers
Under Secretary of Defense for Intelligence

Enclosures

1. References
2. Responsibilities
3. Procedures
4. List of Certifying Officials

Glossary

TABLE OF CONTENTS

ENCLOSURE 1: REFERENCES.....4

ENCLOSURE 2: RESPONSIBILITIES.....5

 UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)).....5

 DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR NUCLEAR MATTERS
 (DASD(NM)).....5

 DEPUTY CHIEF MANAGEMENT OFFICER (DCMO) OF THE DEPARTMENT OF
 DEFENSE.....6

 DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY6

 HEADS OF THE DoD COMPONENTS WITH ACCESS TO RD AND FRD.....6

ENCLOSURE 3: PROCEDURES.....7

 ACCESS7

 DISSEMINATION10

 CLASSIFICATION AND HANDLING12

 DECLASSIFICATION.....16

 TRAINING REQUIREMENTS17

ENCLOSURE 4: LIST OF CERTIFYING OFFICIALS18

GLOSSARY19

 ABBREVIATIONS AND ACRONYMS.....19

 DEFINITIONS.....20

TABLES

 1. DOE, NRC, and DoD Clearances.....10

 2. Markings and Declassification Requirements for RD, FRD, and NSI16

FIGURES

 1. RD Warning.....14

 2. FRD Warning.....14

 3. Sigma 14, Sigma 15, and Sigma 20 Caveat.....14

 4. Sigma 14 Handling Instruction15

ENCLOSURE 1

REFERENCES

- (a) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I)),” October 24, 2014, as amended
- (b) DoD Directive 5210.2, "Access to and Dissemination of Restricted Data,” January 12, 1978 (hereby cancelled)
- (c) Sections 2153, 2161, 2162, 2163, 2164, and 2165 of title 42, United States Code (also known as the "Atomic Energy Act of 1954, as amended")
- (d) Part 1045 of title 10, Code of Federal Regulations
- (e) DoD Manual 5200.01, Volume 1, "Information Security Program: Overview, Classification, and Declassification,” February 24, 2012
- (f) DoD Manual 5200.02, "Procedures for the DoD Personnel Security Program (PSP),” April 3, 2017
- (g) DoD 5220.22-R, "Industrial Security Regulation,” December 4, 1985
- (h) Deputy Secretary of Defense Memorandum, "Establishment of the Office of the Under Secretary of Defense for Research and Engineering and the Office of the Under Secretary of Defense for Acquisition and Sustainment,” July 13, 2018
- (i) DoD Instruction 8500.01, "Cybersecurity,” March 14, 2014
- (j) Executive Order 13526, "Classified National Security Information,” December 29, 2009

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)). The USD(I) shall:

a. Develop policy and procedures to implement and manage the RD and FRD security program for access, dissemination, classification, declassification, and handling of RD and FRD information within the DoD in accordance with the Atomic Energy Act of 1954, as amended.

b. Oversee DoD implementing policies and conduct on-site reviews for DoD Component security programs established in accordance with this Instruction.

2. DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR NUCLEAR MATTERS (DASD(NM)). The DASD(NM), under the authority, direction, and control of the Under Secretary of Defense for Acquisition, Technology, and Logistics (through the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs (ASD(NCB))), shall:

a. In consultation with DOE:

(1) Develop classification guides for programs over which both DoD and DOE have cognizance.

(2) Determine which information in the RD category relating primarily to the military utilization of nuclear weapons may be placed in the FRD category.

(3) Prepare classification guides for FRD and RD relating primarily to the military utilization of nuclear weapons.

(4) Declassify FRD information, relating primarily to the military utilization of nuclear weapons, which may be published without undue risk to the common defense and security.

(5) Prepare and maintain the list of DoD officials authorized to request access to RD data in the possession of DOE at Enclosure 4. Provide a copy of this list to DOE.

b. Disseminate classification and declassification guides for RD and FRD information within the DoD.

c. Assist the DoD Components, when requested, in determining what information relating to the military utilization of nuclear weapons may be designated as FRD even if it has never been in the RD category.

d. Provide information as necessary to the DOE Director of Classification to fulfill responsibilities under this section and section 1045.4 of Reference (d).

3. DEPUTY CHIEF MANAGEMENT OFFICER (DCMO) OF THE DEPARTMENT OF DEFENSE. The DCMO shall, in consultation with the USD(I) and the ASD(NCB), develop appropriate guidelines and management controls for Federal advisory committee and subcommittee members whose positions are established by or supported by the DoD who need access to RD, FRD, and Critical Nuclear Weapons Design Information (CNWDI).

4. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY. The Director, Defense Information Systems Agency, under the authority, direction, and control of the DoD Chief Information Officer, shall ensure DoD Component compliance with this Instruction during inspections of files on the Secret Internet Protocol Router Network (SIPRNET).

5. HEADS OF THE DoD COMPONENTS WITH ACCESS TO RD AND FRD. The Heads of DoD Components with access to RD and FRD shall:

a. Ensure that RD and FRD are classified in accordance with the policies in this Instruction and Reference (d).

b. Designate an RD management official to direct and administer the RD classification program within the DoD Component and whose duties shall include:

(1) Dissemination of implementing directives and classification guides, as needed.

(2) Ensuring that U.S. Government and contractor personnel with access to RD and FRD are trained on the procedures for derivative classification, marking, recognizing, and handling RD and FRD information and documents.

c. Incorporate classification guidance into appropriate security classification guides relevant to their systems, programs, plans or projects, as appropriate.

d. Assist the DASD(NM) with determining what information, to include RD and FRD relating primarily to the military utilization of nuclear weapons, may be placed in the FRD category.

e. Request changes or additions to the DoD List of Certifying Officials, as described in Enclosure 4, through the DASD(NM).

ENCLOSURE 3

PROCEDURES

1. ACCESS

a. Criteria. Access to RD information within and between DoD Components, including contractor activities, will be governed by the same procedures and criteria that govern the access to other classified information in accordance with References (e) through (g). Individuals granted access shall:

(1) Require access in the performance of official duties (also known as “need to know”).

(2) Have a valid DoD security clearance at a level commensurate with the information concerned.

b. Requests for Access. Requests for access to RD in the possession of the DOE or other Federal agencies designated by the DOE, other than DoD and the National Aeronautics and Space Administration (NASA), will be made utilizing DOE Form 5631.20, “Request for Visit or Access Approval.” DOE Form 5631.20 may be accessed at the following DOE website: http://cio.energy.gov/program_planning&mgmt_5000-5999.htm.

(1) The Secretary of Defense; the Deputy Secretary of Defense; the Secretaries of the Military Departments; the Chairman of the Joint Chiefs of Staff; the Under Secretaries of Defense; the Chairman, Nuclear Weapons Council; the Directors of the Defense Agencies; and their designees, are authorized to certify the need of DoD personnel, under their jurisdiction, to have access to RD in the possession of the DOE and other Federal agencies designated by the DOE. These officials shall forward their lists of designees to the DASD(NM), who shall transmit a composite list to the DOE and to the Deputy Under Secretary of Defense for Policy Review for incorporation into Enclosure 4 of this Instruction. Strict adherence to need-to-know principles will be followed.

(a) For the Navy and the Air Force, the authority to certify for RD access in the possession of DOE shall not be designated below the level of the authority granting the security clearance.

(b) For the Army, the authority to certify for RD access shall not be designated below brigade level or equivalent.

(c) For contractor employees, the need for access to RD will, in all cases, be certified by a Government Contracting Officer.

(2) Those persons listed in subparagraph 1.b.(1) of this Enclosure, or their designees, shall submit requests for access to RD through established security channels directly to:

Department of Energy
Director of Safeguards and Security
Washington, DC 20545

(3) DoD requests for access to RD in the possession of Federal agencies other than DoD pertaining to the Army Research Reactor Program and the Navy Research Reactor Program shall be submitted to:

U.S. Nuclear Regulatory Commission
Division of Security
Washington, DC 20555

(4) In situations other than specified in subparagraphs 1.b.(2) and 1.b.(3) of this Enclosure, DoD requests for access to RD in the custody of DOE personnel shall be submitted to the DOE Headquarters Division having responsibility for the subject matter involved.

(5) When it is necessary for a DoD activity to establish authority for requesting access directly from DOE Managers of Operations, a request for such authority shall be submitted to the DOE Headquarters Division responsible for the program to which access is required.

(6) DOE has authorized its personnel to accept oral requests in emergencies. In those instances, all of the information required in DOE Form 5631.20 shall be provided. Thereafter, an appropriate written confirmation shall be forwarded within 15 days following an oral request. Personnel authorized to approve requests for access to or release of RD shall make determinations of emergency situations or conditions.

(7) If an individual requires repeated access to the same type of information or continuing visits to a facility, under the cognizance of the same approving authority, the request shall so specify. Local arrangements for continuing access may be made for a specified period not to exceed 1 year. Access by members of the Military Services may be arranged for the specified period of the assignment for which access was originally approved.

c. Access to CNWDI. Access to and dissemination of CNWDI, as defined in the Glossary, is of particular concern to the DoD. Because of the extreme sensitivity of this type of information, access must be limited to the absolute minimum number of persons who need it to accomplish their assigned responsibilities. To meet this objective, the following special procedures for controlling CNWDI information have been established.

(1) At a minimum, the required security clearances for personnel eligible for access to CNWDI shall be final TOP SECRET or SECRET (as appropriate), or DOE "Q" for non-DoD personnel.

(2) U.S. citizenship is required, except in rare instances when an immigrant alien may possess a unique or very unusual talent or skill that is essential to the U.S. Government and not possessed to a comparable degree by an available U.S. citizen. In such exceptional cases, an affirmative determination shall be made that it is in the overall best interests of the United States

to grant CNWDI access to an immigrant alien. Such a determination shall be made by the Secretary of Defense or his designee, based upon the recommendation of the responsible DoD Component Head.

(3) Written or oral communication of CNWDI shall be strictly limited to those personnel who have a need to know. Management personnel at all levels shall not automatically approve requests for access to CNWDI, but shall insist upon full justification and shall reject any requests that are not completely justified. The Head of each DoD Component and management personnel at all levels are assigned a special responsibility to ensure that this need-to-know principle is strictly enforced.

(4) Personnel having a need for access to CNWDI shall be briefed on its sensitivity. Briefing and access authorizations will be recorded in appropriate security records. Records of CNWDI briefings and access authorizations will be maintained in a manner that would facilitate verification.

(5) Documents or other media as defined in Reference (e), that contain CNWDI shall be clearly marked, "Critical Nuclear Weapons Design Information - DoD Instruction 5210.02 applies." Similar documents published prior to the date of this Instruction will be similarly marked when they are withdrawn from files. In addition, paragraphs of documents that contain CNWDI will be marked with "(N)" following the classification (e.g., (S-RD)(N)). This additional marking denotes that the classified material is additionally identified as CNWDI.

(6) Except for the special requirements enumerated in subparagraph 1.c.(5) of this Enclosure, access to CNWDI within and between DoD Components, including DoD contractors, will be controlled in the same manner as other classified information in accordance with References (e) through (g).

d. Access to Sigma 14, Sigma 15, and Sigma 20 Information. Access and distribution of Sigma 14, Sigma 15, and Sigma 20 nuclear weapon data (NWD) is restricted to those individuals with:

(1) Appropriate Sigma 14, Sigma 15, or Sigma 20 authorization requested and approved through the DASD(NM).

(2) Valid need to know.

(3) Final TOP SECRET clearance based on a single scope background investigation or TOP SECRET "Q" for non-DoD personnel.

(4) Access authorization does not imply need to know for all Sigma 14, Sigma 15, and Sigma 20 NWD.

(5) Access authorization of Sigma 15 or Sigma 20 does not grant access to Sigma 14 NWD.

(6) Access verification for Sigma 14, Sigma 15, and Sigma 20 information shall be requested through the DoD Use Control Site Coordinator, Office of the Deputy Assistant Secretary of Defense for Nuclear Matters (ODASD(NM)).

e. Reciprocity. For other Federal agencies who have a need to know in the performance of their official duties, DoD Components will accept DOE and Nuclear Regulatory Commission (NRC) clearances for access to classified information including RD as shown in Table 1.

Table 1. DOE, NRC, and DoD Clearances

<u>DOE and NRC Clearances</u>	<u>Equivalent DoD Clearances</u>
“L” (Valid for access up to and including SECRET National Security Information (NSI) and FRD. RD access is at the CONFIDENTIAL level.)	SECRET
“Q” TOP SECRET	TOP SECRET

2. DISSEMINATION

a. Criteria. DoD personnel may disseminate RD information only in accordance with the following guidelines:

(1) Dissemination of RD information within and between DoD Components, including DoD contractors, will be governed by the same procedures and criteria as govern the dissemination of other classified information in accordance with References (e) through (g).

(2) Dissemination of RD information may be made to properly cleared DOE personnel and to DOE-cleared personnel of other Federal agencies.

(3) Dissemination of RD information pertaining only to nuclear research reactors or nuclear electric power generating reactors may be made to NRC personnel. RD not related to these reactors may be released to NRC personnel only through DOE.

(4) Dissemination of RD information other than that pertaining to aeronautical and space activities may be released to NASA personnel only through DOE.

(5) In all cases in subparagraphs 2.a.(1) through 2.a.(4) of this Enclosure, dissemination of RD information will be made only after the holder of the information has verified:

- (a) The identification of the prospective recipient.
- (b) The validity of the prospective recipient’s clearance.

(c) The need to know of the prospective recipient in connection with official duties.

b. Disclosure Prohibitions

(1) Dissemination of RD and FRD to any nation or regional defense organization or to a representative of such nation or organization is prohibited except in accordance with agreements for cooperation entered into pursuant to the Atomic Energy Act of 1954, as amended.

(2) Except as provided in subparagraph 2.b.(1) of this Enclosure, FRD will be treated and disseminated in the manner prescribed for classified information in Reference (e).

c. Protection and Accountability of Sigma 14, Sigma 15, and Sigma 20 Information

(1) Technical discussion of Sigma 14, Sigma 15, and Sigma 20 information is permitted within facilities cleared for classified discussions at the same collateral level.

(2) Verification of clearance, Sigma authorizations, and need to know must be verified for all participants prior to discussions.

(3) Sigma 14 documents shall be inventoried annually.

(a) Inventory results of Sigma 14 holdings will be reported annually to the DoD Use Control Program Coordinator (UCPC), ODASD(NM).

(b) The ODASD(NM) UCPC will report Sigma 14 holdings to the National Nuclear Security Administration (NNSA) UCPC annually.

(c) Requests for transfer of Sigma 14 information outside of the NNSA require prior NNSA approval through the DoD UCPC, ODASD(NM).

(4) Storage requirements for classified material must be consistent with Reference (e), with the following additions for Sigma 14, Sigma 15, and Sigma 20 materials:

(a) Sigma 14 documents must be physically separated by a separate safe or combination-protected safe drawer from non-Sigma 14 documents.

(b) Sigma 15 and Sigma 20 documents may be co-mingled with non-Sigma classified documents.

(c) Access to the safe containing Sigma 15 or Sigma 20 must be restricted to those who are authorized access to Sigma 15 or Sigma 20 information.

(d) Safes containing TOP SECRET Sigma 14 information must be located in a vault or vault-type room.

d. Processing of RD and CNWDI on the SIPRNET

(1) RD and CNWDI shall be e-mailed only after confirmation that the recipient has a final security clearance at the appropriate level, has a need to know the information, and, for CNWDI, has received the additional security briefing in subparagraph 1.c.(4) of this Enclosure.

(2) All RD and CNWDI files stored on shared and personal local drives shall be password-protected using the standard Microsoft Office file password protection protocol.

(3) Websites posting RD and CNWDI information must ensure access is limited to authorized recipients by, at a minimum, a properly administered and protected individual identifier and password consistent with DoD Instruction 8500.01 (Reference (i)).

(4) Systems logons and properly configured screensavers are sufficient protection for e-mail files.

(5) Files contained on the SIPRNET are subject to Defense Information Systems Agency inspections to ensure compliance with this Instruction.

(6) Sigma 14, 15, and 20 information shall not be processed on the SIPRNET.

3. CLASSIFICATION AND HANDLING

a. Classification. NSI describes any information that has been determined, pursuant to Executive Order 13526 (Reference (j)), to require protection against unauthorized disclosure. There are 3 levels of NSI:

(1) TOP SECRET is the classification level assigned to information of the utmost importance to national defense and security. Unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to national security that the original classification authority is able to identify or describe.

(2) SECRET is the classification level applied to information the unauthorized disclosure of which could reasonably be expected to cause serious damage to national security that the original classification authority is able to identify or describe.

(3) CONFIDENTIAL is the classification level applied to information the unauthorized disclosure of which could reasonably be expected to cause damage to national security that the original classification authority is able to identify or describe.

b. Handling Instructions

(1) RD, pursuant to the Atomic Energy Act of 1954, as amended, describes all data concerning the design, manufacture, or utilization of atomic weapons; production of special nuclear material (SNM); or use of SNM in the production of energy. SNM includes plutonium, uranium-233, and uranium enriched in isotope 235. A few examples of RD are:

(a) Nuclear weapons design information.

1. Specification and amount of SNM.
2. Dimensions, sketches, drawings, and blueprints.
3. Materials or weapon parts.
4. Detonation systems (amount of high explosives, number of detonators).
5. Nuclear testing information.

(b) Production of SNM.

1. Uranium-enriched technology such as gaseous diffusion, gas centrifuge, and laser isotope separation.
2. Production reactors and related technologies such as fuel and target technology and chemical processing of tritium and plutonium.
3. Allocations to weapons programs.

(c) Use of SNM in the Production of Energy.

1. Naval reactors.
2. Military reactors.
3. Space reactor power systems.

(2) FRD describes classified information jointly determined by the DOE or its predecessor agencies and the DoD to be related primarily to the military utilization of atomic weapons and protected as NSI. A few examples of FRD are:

- (a) Nuclear weapon stockpile quantities.
- (b) Nuclear weapon safety and storage.
- (c) Nuclear weapon yield and effects.
- (d) Nuclear weapon storage and deployment locations.

c. Markings

(1) All documents marked RD or FRD must also be marked either TOP SECRET, SECRET, or CONFIDENTIAL and with an appropriate warning as illustrated in Figures 1 and 2.

Figure 1. RD Warning

RESTRICTED DATA
This document contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to Administrative and Criminal Sanctions.

Figure 2. FRD Warning

FORMERLY RESTRICTED DATA
Unauthorized disclosure subject to Administrative and Criminal Sanctions. Handle as restricted Data in Foreign Dissemination Section 144.b, Atomic Energy Act of 1954

(2) All documents containing Sigma 14, Sigma 15, and Sigma 20 information will be marked with an additional caveat marking (e.g., Sigma 14) above the category marking as illustrated in Figure 3.

Figure 3. Sigma 14, Sigma 15, and Sigma 20 Caveat

Sigma 14
RESTRICTED DATA
This document contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to Administrative and Criminal Sanctions.

(3) All documents containing Sigma 14 information will be marked with the additional handling instruction illustrated in Figure 4.

Figure 4. Sigma 14 Handling Instruction

This document may not be reproduced or disseminated beyond original distribution without approval of the originator, the originating agency Use Control Site Coordinator, or the National Nuclear Security Administration Headquarters Use Control Program Coordinator.

d. Differences Between RD and FRD and NSI. Table 2 illustrates the differences between markings and declassification requirements for RD, FRD, and NSI.

Table 2. Markings and Declassification Requirements for RD, FRD, and NSI

	RD AND FRD	NSI
Authority	Atomic Energy Act of 1954	Executive Order 13526 (Reference (j))
Declassification	<p>Documents containing RD or FRD are not subject to automatic declassification; in accordance with the Atomic Energy Act of 1954, as amended, they always require review prior to declassification.</p> <p>Documents containing RD can only be declassified by authorized DOE reviewers.</p> <p>Documents containing FRD can only be declassified if it is jointly agreed to by both DOE and DoD reviewers and approved by the designated representative of both departments. Normally, DoD initiates declassification requests of FRD material.</p>	<p>Documents containing only NSI are automatically declassified on occurrence of an event or date unless specifically exempted.</p> <p>Documents containing only NSI can be declassified by any reviewer designated by the originating agency.</p>
Marking	<p>Documents containing RD or FRD must have a special warning notice on the front page indicating the presence of RD or FRD. Additional markings on the interior pages are also required.</p> <p>Documents containing RD or FRD do not have automatic declassification instructions on the front page, even if NSI is also present in the document.</p> <p>DoD documents containing RD or FRD require portion marking.</p>	<p>Documents containing only NSI are marked in accordance with Reference (e).</p> <p>Documents containing only NSI must contain automatic declassification instructions.</p> <p>Documents containing only NSI must be portion marked.</p>

4. DECLASSIFICATION

a. Declassification of RD and FRD documents. Only designated individuals within the DOE may declassify RD documents. Only designated individuals within the DoD (Office of the ASD(NCB)) and the DOE may declassify documents marked as FRD as a joint determination by both departments in accordance with joint DoD-DOE classification guides or DoD guides coordinated with DOE.

b. Automatic declassification prohibition.

(1) Documents containing RD and FRD remain classified until a positive action by an authorized individual is taken within DOE for RD information and jointly by DoD-DOE for FRD or in accordance with joint DoD-DOE classification guides or DoD guides coordinated with DOE.

(2) In accordance with the Atomic Energy Act of 1954, as amended, and section 1045.38 of Reference (d), no date or event for automatic declassification will be applied to RD and FRD documents, even if such documents also contain NSI.

(3) RD and FRD are exempt from all provisions of Reference (j) or its predecessor Executive orders, as amended, including automatic declassification.

5. TRAINING REQUIREMENTS

a. In accordance with section 1045.35 of Reference (d), RD management officials shall ensure that persons with access to RD and FRD information are informed on the authorities required to classify and declassify RD and FRD information and documents and on handling procedures. RD classifiers shall be trained on the procedures for classifying, declassifying, marking, and handling RD and FRD information and documents.

b. Training shall be at a DOE-certified course or with training materials provided by or coordinated with DOE by authorized DoD RD management officials.

ENCLOSURE 4

LIST OF CERTIFYING OFFICIALS

The DASD(NM) maintains the DoD List of Certifying Officials authorized to certify personnel under their jurisdiction for access to RD information (to include CNWDI) in the possession of DOE employees, DOE contractors, and employees of other Federal agencies and their contractors at <https://extranet.acq.osd.mil/nm>.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ASD(NCB)	Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs
CFR	Code of Federal Regulations
CNWDI	Critical Nuclear Weapons Design Information
DCMO	Deputy Chief Management Officer of the Department of Defense
DASD(NM)	Deputy Assistant Secretary of Defense for Nuclear Matters
DOE	Department of Energy
FRD	Formerly Restricted Data
NASA	National Aeronautics and Space Administration
NNSA	National Nuclear Security Administration
NRC	Nuclear Regulatory Commission
NSI	National Security Information
NWD	Nuclear Weapon Data
ODASD(NM)	Office of the Deputy Assistant Secretary of Defense for Nuclear Matters
RD	Restricted Data
SIPRNET	Secret Internet Protocol Router Network
SNM	Special Nuclear Material
UCPC	Use Control Program Coordinator
UCSC	Use Control Site Coordinator
USD(I)	Under Secretary of Defense for Intelligence

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purpose of this Instruction.

classified information. Official information that has been determined to require, in the interests of national security, protection against unauthorized disclosure and that has been so designated.

CNWDI. That TOP SECRET RD or SECRET RD revealing the theory of operation or design of the components of a thermonuclear or implosion-type fission bomb, warhead, demolition munition, or test device. Specifically excluded is information concerning arming, fusing, and firing systems; limited-life components; and total contained quantities of fissionable, fusionable, and high explosive materials by type. Among these excluded items are the components that DoD personnel set, maintain, operate, test, or replace.

DoD personnel. Military Service personnel, including members of the Reserve Forces and federally recognized members of the National Guard; employees of a DoD Component, including consultants, full-time and temporary part-time employees, and personnel paid from nonappropriated funds; contractors of a DoD Component; and members of Federal advisory committees established or supported by DoD.

DoD security clearance. A clearance granted by a DoD Component pursuant to the provisions of References (f) and (g). A contractor-granted CONFIDENTIAL security clearance is not valid for access to RD.

DOE personnel. DOE employees, DOE contractors and their employees, and Federal Executive Branch component personnel assigned to the DOE for duty (e.g., the DoD, State Department, NASA).

DOE security clearance. A clearance granted by the DOE pursuant to provisions of the Atomic Energy Act of 1954, as amended.

FRD. Data removed from the RD category upon joint determination by the DOE and DoD that such data relates primarily to the military utilization of atomic weapons and can be adequately safeguarded as classified information. However, such information is treated the same as RD for purposes of foreign dissemination.

NASA personnel. Any officer, employee, member of an advisory committee, contractor, subcontractor, or officer or employee of a contractor or subcontractor, of NASA, and Federal Executive Branch component personnel assigned to NASA for duty (e.g., the DoD, State Department, DOE).

NASA security clearance. A clearance granted by NASA, pursuant to regulations issued by NASA.

need to know. A determination that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

NNSA. All Federal and contractor employees that design, manufacture, or test nuclear weapons and/or explosive devices; retire nuclear weapon components; or administer the preceding programs.

NRC personnel. NRC employees, NRC contractors and their employees, and Federal Executive Branch component personnel assigned to the NRC for duty (e.g., the DoD, State Department, NASA).

NRC security clearance. A clearance granted by the NRC, pursuant to regulations issued by the NRC.

NSI. Any information that has been determined, pursuant to Reference (j), to require protection against unauthorized disclosure.

NWD. RD or FRD concerning the design, manufacture, or utilization (including theory, development, storage, characteristics, performance, and effects) of nuclear weapons or nuclear weapon components, including information incorporated in or related to nuclear explosive devices.

RD. All data (information) concerning the design, manufacture, or utilization of atomic weapons; the production of SNM; or the use of SNM in the production of energy. The term does not include data declassified or removed from the RD category pursuant to section 142 of the Atomic Energy Act of 1954, as amended. See FRD.

sensitive use control information. Information that significantly enhances an adversary's ability to obtain an unauthorized nuclear detonation from a nuclear weapon or device.

Sigma 14 information. The category of sensitive information (including bypass scenarios) concerning the vulnerability of nuclear weapons to a deliberate unauthorized nuclear detonation.

Sigma 15 information. The category of sensitive information concerning the design and function of nuclear weapon use control systems, features, and components. This includes use control for passive and active systems. It may include weapon design features not specifically part of a use control system. Not all use control design information is Sigma 15.

Sigma 20 information. The category of NWD that pertains to sensitive improvised nuclear device information.