



CHAPTER 18

CLASSIFICATION

OVERVIEW

Throughout history, U.S. national defense has required that certain information be maintained in confidence to safeguard U.S. citizens, democratic institutions, homeland security, and interactions with foreign nations. Today, preserving critical U.S. national security information remains a top priority.

The U.S. government has created a classification system for safeguarding information which includes marking and granting clearances and access to obtain or view documents containing classified information. This chapter provides a classification reference for general issues related to nuclear matters. It includes a discussion of information classification, classification authorities, security clearances, access to classified information, marking classified documents, and Unclassified Controlled Nuclear Information (UCNI).

INFORMATION CLASSIFICATION

The two categories of classified information are national security information (NSI) and atomic energy (nuclear) information.

NATIONAL SECURITY INFORMATION

Executive Order (EO) 13526, *Classified National Security Information*, prescribes the system for classifying, safeguarding, and declassifying NSI. EO 13526 states national security information may be classified at one of the following three levels:

- *Top Secret (TS)* shall be applied to information, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

- *Secret (S)* shall be applied to information, the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.
- *Confidential (C)* shall be applied to information, the unauthorized disclosure of which could reasonably be expected to cause damage to the national security that the original classification authority is able to identify or describe.

NUCLEAR INFORMATION

Nuclear information is protected by the *Atomic Energy Act (AEA) of 1954*, as amended, and is a caveat added to the classification level of specific types of information. Information can be classified as S//Restricted Data (S//RD) or TS//RD or S//Formerly Restricted Data (S//FRD) or TS//FRD. The DOE implements the AEA requirements for classification and declassification of nuclear information via 10 CFR 1045, *Nuclear Classification and Declassification*. The AEA classifies nuclear information as RD, which is not subject to EO 13526. DOE oversees the classification and declassification of all nuclear information protected by the AEA. RD is never automatically declassified and maybe declassified only by DOE.

RD comprises all data related to: the design, manufacture, or use of nuclear weapons; production of special nuclear material (SNM); or use of SNM in the production of energy. RD does not include data removed from the Restricted Data category, i.e., data that is designated Formerly Restricted Data (FRD) or Transclassified Foreign Nuclear Information (TFNI).

FRD is still a category of classified information related to nuclear weapons. It does **not** mean it is formerly classified and therefore is now unclassified. FRD is jointly determined by DoD and DOE to relate primarily to the military use of nuclear weapons, and is safeguarded as defense information (e.g., weapon yield, deployment locations, weapons safety and storage, and stockpile quantities).

Information characterized as FRD is not subject to EO 13526. FRD is stored, transmitted, and destroyed in the same ways as RD of the same classification level. FRD is never automatically declassified. Declassification requires a joint determination by DoD and DOE.

TFNI is information from any intelligence source that concerns the nuclear programs of foreign governments that was removed from the RD category (by transclassification) under section 142 of the *Atomic Energy Act*, by past joint agreements between DOE and the Director of Central Intelligence, or past and future agreements with the Director of National Intelligence. When removed from the RD category, TFNI information is stored, transmitted, and destroyed in the same ways as NSI of the same classification level.

DoD and DOE have separate systems for controlling nuclear information, as follows.

DoD System for Controlling Nuclear Information

DoD policy governing access to and dissemination of RD is provided in DoD Instruction 5210.02, *Access to and Dissemination of Restricted Data and Formerly Restricted Data*. DoD categorizes RD information as Confidential RD, S//RD, or TS//RD. Critical Nuclear Weapon Design Information (CNWDI) is a DoD access control caveat for a specific subset of Restricted Data. CNWDI information is S//RD or TS//RD; that reveals the theory of operation or design of components of a thermonuclear or implosion-type fission bomb, warhead,

demolition munition, or test device. Finally, DoD recognizes DOE designations of Sigma 14, Sigma 15, Sigma 18, and Sigma 20 as additional subsets of Restricted Data.

DOE System for Controlling Nuclear Information

DOE policy of categorizing Restricted Data into defined subject areas is known as the Sigma system. The Secret and Top Secret Nuclear Weapon Data (NWD) subsets of RD regard nuclear weapons, components, or explosive devices or materials that have been determined to require additional protection. The current categories of NWD are Sigma 14, Sigma 15, Sigma 18, and Sigma 20; previous Sigma categories 1-13 are no longer in use. DOE controls access to all Sigma categories on a strict need-to-know basis, and DoD personnel requiring access to Sigma information must obtain DOE approval.

DOE Order 452.7, *Protection of Use Control Vulnerabilities and Designs*, establishes the policy, process, and procedures for control of sensitive use control information in NWD categories Sigma 14 and Sigma 15 to ensure the dissemination of the information is restricted to individuals with a valid need-to-know.

- *Sigma 14* – Category of sensitive information, including bypass scenarios, concerning the vulnerability of nuclear weapons to a deliberate, unauthorized nuclear detonation or to the denial of authorized use.
- *Sigma 15* – 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 and may include security verification features or weapon design features not specifically part of a use control system.

DOE Order 452.8, *Control of Nuclear Weapon Data*, sustains Sigma 14 and 15 and establishes Sigma 18.

- *Sigma 18* – Category of NWD including information that allows or significantly facilitates a nation or entity to fabricate a credible nuclear weapon or nuclear explosive device based on a proven, certified, or endorsed U.S. nuclear weapon or device. This information would enable the establishment or improvement of nuclear capability without nuclear testing or with minimal research and development. DOE determines the information placed in the Sigma 18 category, which includes: complete design of a gun-assembled weapon; complete design of a primary or single stage implosion-assembled weapon; complete design of a secondary stage; weapon design codes with one-dimensional hydrodynamics and radiation transport with fission and/or thermonuclear burn; and weapon design codes with two- and three-dimensional capabilities.

DOE Order 457.1A, *Nuclear Counterterrorism*, provides the basis for implementing procedures regulating strict control of and access to Sigma 20 information.

- *Sigma 20* – Specific category of NWD that pertains to “crude, simple, or innovative” improvised nuclear device (IND) designs, concepts, and related manufacturing or processing pathways. Not all INDs fall within the Sigma 20 category.

FOREIGN NUCLEAR INFORMATION

Foreign nuclear information is information on foreign government nuclear programs. It includes the design, manufacture, or use of nuclear weapons; the production of SNM; or the use of SNM in the production of energy. This information is treated as RD.

Considerations for the removal of foreign nuclear information from the RD category include there being no automatic declassification of the information; DOE determination that it can be removed from RD; and the use of appropriate classification markings on the remainder of the information. At a minimum, access to the information will be the same as NSI, and it will be safeguarded based upon the classification determination. Foreign nuclear information which has been removed from RD is categorized as TFNI.

SHARING INFORMATION WITH THE UNITED KINGDOM

DoD and DOE have joint guidelines for complying with each Department's requirements for export controls and classified information exchange for stockpile weapon activities related to the 1958 U.S.-UK Mutual Defense Agreement (MDA), under the authorities of the AEA. Using Joint Atomic Information Exchange Group (JAIEG)-approved processes, DoD and DOE management may disclose to the United Kingdom transmissible RD, FRD, and unclassified information, which may include Controlled Unclassified Information (CUI) internal to the nuclear weapon.

CLASSIFYING DOCUMENTS

To properly classify a document, an individual must have classification authority. DoD Manual 5200.01-V1, *DoD Information Security Program*, describes two types of classification authority: original and derivative. A classifier is any person who makes a classification determination and applies a classification category to information or material. The determination may be an original classification action or derivative classification action. Proper classification enables appropriate protection of information. Persons handling information must abide by the classification markings and also not assume an unmarked document or source does not contain classified or sensitive information. The Internet, in particular, can be a source of unmarked classified information or a combination of unclassified information that is classified in aggregate.

ORIGINAL CLASSIFICATION AUTHORITY

The authority to originally classify information may only be exercised by the President and the Vice President; agency heads and officials designated by the President; and U.S. Government officials delegated the authority pursuant to EO 13526. For NSI, the original classification authority (OCA) also serves as the declassification authority and sets the date for automatic declassification. Within DoD and DOE, only appointed government officials can serve as OCAs to classify NSI. Further, only DOE officials have OCA for RD information. The Deputy Assistant Secretary of Defense for Nuclear Matters (DASD(NM)) is the OCA for DoD determined FRD.

DERIVATIVE CLASSIFICATION AUTHORITY

According to EO 13526, those individuals who reproduce, extract, or summarize classified information, or who apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority. Individuals who apply derivative classification markings are required to observe and respect original classification decisions and carry forward the pertinent classification

markings to any newly created documents. Individuals within both DoD and DOE can use derivative classification authority on NSI, RD, and FRD information.

SECURITY CLEARANCES

Both DoD and DOE issue personnel security clearances governing the access of their employees and contractors to classified information.

DoD SECURITY CLEARANCE LEVELS

DoD defines a security clearance as an administrative determination by a competent authority that a person is eligible under the standards of DoD 5200.2-R, *Personnel Security Program*, for access to classified information. DoD clearances may be issued at the Top Secret, Secret, or Confidential level. These levels allow the individual holding the clearance, and possessing the proper need- to-know, to view information classified at those levels.¹

DOE SECURITY CLEARANCE LEVELS

Adhering to the information restrictions and guidelines of the AEA, DOE established a security clearance system that is implemented through DOE Order 472.2, *Personnel Security*, and described in DOE Order 452.8:

- *L Access Authorization* is given to an individual whose duties require access to Confidential RD, Confidential/Secret FRD, or Confidential/Secret NSI.
- *Q Access Authorization* is given to an individual whose duties require access to Secret/Top Secret RD, Top Secret FRD, Top Secret NSI, or any category or level of classified matter designated as communications security, cryptographic, or sensitive compartmented information.

DoD (Access within and between DoD components) ¹	Highest Access
Final Secret (no CNWDI)	S//RD
Final Secret (w/CNWDI)	S//RD/CNWDI
Final Top Secret (no CNWDI)*	TS//RD
Final Top Secret (w/CNWDI)*	TS//RD/CNWDI

¹ Outside DoD, follow owning agency procedure.
* Access to Sigma 14, 15, 18, & 20 requires DOE approval.

DOE	Highest Access
L	S//FRD C//RD
Q**	TS//RD

**Q includes Sigma 18 for DOE Nuclear Security Enterprise personnel. Sigma 14, 15, and 20 require additional approval.

EQUATING THE TWO CLASSIFICATION SYSTEMS

While it is not possible to directly correlate the two security clearance systems used by DoD and DOE, Figure 18.1 illustrates the clearances and highest level of access for the two Departments.

Figure 18.1

DoD and DOE Clearance Levels and Access

¹ “Need-to-know” is defined in DoD 5200.2-R as a determination made by a possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to, knowledge of, or possession of classified information in order to perform tasks or services essential to the fulfillment of an official U.S. government program. Knowledge of, possession of, or access to classified information shall not be afforded to any individual solely by virtue of the individual’s office, position, or security clearance.

ACCESSING CLASSIFIED INFORMATION

The two basic requirements to access classified information are appropriate clearance and need-to-know, and both must be present for an individual to view classified information. Need-to-know is confirmed by the agency controlling the information and helps govern access to information. Security administrators verify an individual's eligibility for a certain clearance level and then grant need-to-know caveats, as needed. An individual may have access authorization of C, S, TS, or TS/SCI (special compartmented information) clearance in DoD; an individual may have L or Q access authorization in DOE. Each of these clearance levels also has an interim status, which allows the cleared person to view but not create or control documents at that level. However, an interim Secret clearance does not allow access to RD, NATO, or COMSEC (communications security) information at the Secret level. An interim TS is valid for access to TS information and Secret and Confidential levels of RD, NATO, and COMSEC information. Once given a final clearance, an individual is able to access and control documents for that level of classification.

Only DoD, DOE, the Nuclear Regulatory Commission, and the National Aeronautics and Space Administration have the authority to grant RD and FRD access. The DoD does not require a 'read-in' for access to RD or FRD in the possession of DoD with the exception of access to CNWDI. To access CNWDI information, individuals require authorization and a read-in briefing.

MARKING CLASSIFIED DOCUMENTS CONTAINING INFORMATION PROTECTED BY THE ATOMIC ENERGY ACT

MARKING RESTRICTED DATA, FORMERLY RESTRICTED DATA, AND CNWDI DOCUMENTS

There is a special requirement for marking RD, FRD, and CNWDI documents. The front page of documents containing RD must include the following statement:

RESTRICTED DATA

This document contains Restricted Data, as defined in the Atomic Energy Act of 1954. Unauthorized disclosure is subject to administrative and criminal sanctions.

This may appear on the first page of the document and on a second cover page, placed immediately after the initial classified cover sheet.

FRD material must contain the following statement on the front page of the document:

FORMERLY RESTRICTED DATA

Unauthorized disclosure is subject to administrative and criminal sanctions. Handle as Restricted Data in foreign dissemination, per section 144b, Atomic Energy Act of 1954.

Additionally, documents containing RD and FRD should have abbreviated markings included with the classification portion marking (e.g., S//RD or S//FRD). Documents containing RD and CNWDI material must also contain the following statement, in addition to the RD statement on the front page of the document:

CNWDI

Critical Nuclear Weapon Design Information. DoD Instruction 5210.02 applies.

In addition, CNWDI is marked with an “N” in separate parentheses following the portion marking (e.g., (S//RD)(N)).

Finally, when a document contains RD, FRD, and CNWDI, only the RD and CNWDI warning notices are affixed. No declassification instructions are used.

ATOMAL

ATOMAL is a NATO term used to identify and protect Restricted Data or Formerly Restricted Data provided to NATO by the U.S. government. Because materials marked RD or FRD are not cleared for release to NATO or NATO countries, organizations wanting to transmit RD or FRD materials to NATO must clear the materials through the JAIEG. RD or FRD materials cleared by the JAIEG for release will be assigned a JAIEG reference number (JRN). Once a JAIEG cleared document is marked as ATOMAL and handed over to a NATO registry and assigned a NATO control number, it becomes a controlled NATO ATOMAL document.

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

CUI replaces the terms *For Official Use Only (FOUO)* and *Official Use Only (OUO)* that were applied by DoD and DOE, respectively, to certain unclassified information that may be exempt from mandatory disclosure under the Freedom of Information Act (FOIA).

The CUI program developed a common marking system across Federal Agencies and created categories to capture many types of unclassified information requiring safeguarding based on existing laws, regulations, and government-wide policies. CUI is based on Executive Order 13556, *Controlled Unclassified Information*, November 4, 2010; 32 Code of Federal Regulations, part 2002, September 14, 2016 and DoDI 5200.48, *Controlled Unclassified Information (CUI)*, March 6, 2020.

One of the CUI categories used by DoD and DOE is Unclassified Controlled Nuclear Information. DoD defines UCNI as unclassified information pertaining to security measures, including plans, procedures, and equipment, for the physical protection of DoD SNM, weapons, equipment, or facilities. While this information is not formally classified, it is restricted in its distribution. DoD UCNI policy is provided in DoD Instruction 5210.83, *DoD Unclassified Controlled Nuclear Information*.

DOE uses the term UCNI in a broader manner than DoD. Designating DoD information as UCNI is governed by Title 10 USC §128, whereas designating DOE information as UCNI is governed by Title 42 USC §2168.