



G.1 Overview

Throughout U.S. history, national defense has required certain information be maintained in confidence in order to protect citizens, democratic institutions, homeland security, and interactions with foreign nations. Protecting information critical to U.S. national security remains a priority.

The United States has devised its own classification system for safeguarding documents and other media, which includes marking and granting access and clearance to obtain or view those documents. This appendix provides a classification reference for general issues related to nuclear matters. This includes a discussion of information classification, classification authorities, security clearances, accessing classified information, marking classified documents, For Official Use Only (FOUO)/Official Use Only (OUO), and Unclassified Controlled Nuclear Information (UCNI).

G.2 Information Classification

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

G.2.1 National Security Information

NSI is protected by Executive Order (EO) 13526, *Classified National Security Information*. EO 13526 prescribes a uniform 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 reasonably could 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 reasonably could 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 reasonably could be expected to cause *damage* to the national security that the original classification authority is able to identify or describe.

G.2.2 Nuclear Information

Nuclear information is protected by the *Atomic Energy Act (AEA)* of 1954, as Amended. The DOE implements the AEA requirements for classification and declassification of nuclear information via 10 CFR 1045, *Nuclear Classification and Declassification*. The AEA categorizes classified nuclear information as *Restricted Data (RD)*. RD is not subject to EO 13526.

Restricted Data is all data concerning the design, manufacture, or utilization of nuclear weapons; production of special nuclear material (SNM); or use of SNM in the production of energy.

Classified nuclear information can be removed from the RD category pursuant to AEA sections 142d or 142e, and, after its removal, it is categorized respectively as *Formerly Restricted Data (FRD)*.

Formerly Restricted Data is jointly determined by the DoD and the DOE to relate primarily to the military utilization of nuclear weapons and can be adequately 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.

Restricted Data information that is recategorized as NSI refers to information jointly determined by the DOE and the Director of National Intelligence to be information that concerns the nuclear programs of other nations and can be adequately safeguarded as defense information (e.g., foreign weapon yields). When removed from the RD category, this information is subject to EO 13526.

The DoD and the DOE have separate systems for granting access to nuclear information.

The DoD System for Controlling Nuclear Information

DoD policy governing access to and dissemination of RD is stated in DoD Instruction (DoDI) 5210.02, *Access to and Dissemination of Restricted Data and Formerly Restricted Data*. The DoD categorizes RD information into Confidential RD, Secret RD, and Top Secret RD. Critical Nuclear Weapon Design Information (CNWDI) is a DoD access control caveat for a specific subset of Restricted Data. CNWDI information is Top Secret RD or Secret RD revealing the theory of operation or design of components of a thermonuclear or implosion-type fission bomb, warhead, demolition munition, or test device. In addition, the DoD currently recognizes the designations of Sigma 14, Sigma 15, Sigma 18, and Sigma 20, as defined by the DOE, as an additional subset of Restricted Data.

The DOE System for Controlling Nuclear Information

DOE policy of categorizing Restricted Data into defined subject areas is known as the *sigma system*. Subsets of Secret and Top Secret Nuclear Weapon Data (NWD) relating to RD and/or FRD concerning nuclear weapons, components, or explosive devices or materials has been determined to require additional protection. The categories of NWD are Sigma 14, Sigma 15, Sigma 18, and Sigma 20. This categorization system separates RD information into common work groups to enforce need-to-know limitations. Previous Sigma categories 1-13, defined by DOE Order (DOE O) 5610.2, *Control of Nuclear Weapon Data*, are no longer in use.

DOE O 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 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.¹

Because of the extremely sensitive nature of Sigma 14 and 15 information, all individuals who are granted access to Sigma 14 and 15 must receive formal authorization by a DOE element or contractor organization with responsibility for Sigma 14 or 15 NWD.

DOE O 452.8, *Control of Nuclear Weapon Data* (cancels DOE O 5610.2) sustains Sigma 14 and 15 and establishes Sigma 18.

- **Sigma 18:** Category of NWD including information that allows or significantly facilitates a proliferant nation or entity to fabricate a credible nuclear weapon or nuclear explosive 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. The DOE/NNSA determines which information is placed in the Sigma 18 category. Sigma 18 information includes complete design of a gun-assembled weapon; complete design of a primary or single stage implosion-assembled weapon; complete design of an interstage or secondary; weapon design codes with one-dimensional (1-D) hydrodynamics and radiation transport with fission and/or thermonuclear burn; and weapon design codes with two-dimensional (2-D) and three-dimensional (3-D) capabilities. DoD individuals must obtain DOE/NNSA approval to have access to Sigma 18.

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

- **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 are Sigma 20. DoD individuals must obtain DOE/NNSA approval to have access to Sigma 20.

¹ Not all use control design information is Sigma 15.

Foreign Nuclear Information

The DOE is developing protocols to address foreign nuclear information. Foreign nuclear information begins as information on foreign nuclear programs and contains foreign design, manufacture, or utilization of nuclear weapons, the production of SNM, or the use of SNM in the production of energy and is treated as RD.

The information may be removed from RD categorization under the following conditions: no automatic declassification; DOE determines when declassified; requires special marking; access is the same as NSI; and/or is safeguarded the same as NSI at which point it is categorized as Transclassified Foreign Nuclear Information (TFNI) (DOE O 475.2A, *Identifying Classified Information*).

TFNI is information from any intelligence source concerning the nuclear energy programs of foreign governments that was removed from the RD category (by transclassification) under section 142(e) of the AEA by past joint agreements between the DOE and the Director of Central Intelligence or past and future agreements with the Director of National Intelligence.

TFNI is stored, transmitted, and destroyed the same as NSI of the same level and does not require special read on.

Information Sharing with the United Kingdom

The DoD and the DOE agreed on joint guidance for complying with each Department's requirements on 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/NNSA management may disclose transmissible RD, FRD, and unclassified information, which includes Controlled Unclassified Information (CUI) within the nuclear weapon, to the United Kingdom. This disclosure may be made without a license or authorization under the International Traffic in Arms Regulations (ITAR) and without prior coordination with the relevant U.S. Military Department. The disclosure of RD and FRD external to the nuclear weapon may be made using JAIEG-approved processes. However, the disclosure of NSI, which includes Classified Military Information (CMI), external to the nuclear weapon shall not be made without approval of the respective Military Departments.



Federal Register

**Tuesday,
January 5, 2010**

Part VII

The President

**Executive Order 13526—Classified
National Security Information
Memorandum of December 29, 2009—
Implementation of the Executive Order
“Classified National Security Information”
Order of December 29, 2009—Original
Classification Authority**

Questions on these processes should be referred to the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs and the NNSA Deputy Administrator for Defense Programs.

G.3 Classifying Documents

In order to properly classify a document, an individual must have classification authority. DoD Manual (DoDM) 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 information which may be considered classified, or the combination of several unclassified data may be classified in aggregate.

G.3.1 Original Classification Authority

The authority to classify information originally 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, section 1.3, Paragraph (c). For NSI, the original classification authority (OCA) also serves as the declassification authority and sets the date for automatic declassification. A joint DoD-DOE/NNSA determination is required to declassify FRD information. Within the DoD and the DOE/NNSA, only appointed government officials can classify NSI. Further, only DOE/NNSA officials can have original classification authority for RD information. In an exceptional case, that is when an employee or government contractor of an agency without classification authority originates information believed by that person to require classification, the information must be protected in a manner consistent with EO 13526 and the AEA. The agency must decide within 30 days whether to classify the information.

G.3.2 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 the DoD and the DOE/NNSA can use derivative classification authority on NSI, RD, and FRD information.

G.4 Security Clearances

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

G.4.1 DoD Security Clearance Levels

The DoD defines a security clearance as an administrative determination by 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, assuming they have the proper need-to-know,² to view information classified at those levels, as defined by EO 13526.

G.4.2 DOE Security Clearance Levels

Corresponding to the information restrictions and guidelines in the AEA, the DOE established a security clearance system, implemented through DOE O 472.2, *Personnel Security* and described in DOE O 452.8, where:

- **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 COMSEC, CRYPTO, or SCI.³

G.4.3 Equating the Two Classification Systems

While it is not possible to directly correlate the two security clearance systems used by the DoD and the DOE/NNSA, **Figure G.1** shows the clearances and highest level of access for the two Departments.

² 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.

³ Communications Security (COMSEC), Cryptography/Cryptographic (CRYPTO), and Sensitive Compartmented Information (SCI).

G.5 Accessing Classified Information

The two basic requirements to access classified information are appropriate clearance and need-to-know. Both must be present for an individual to view classified information. Rank, position, or clearance are not sufficient criteria from which to grant access. Personnel security clearance levels correspond to the security classifications. Need-to-know is granted 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 a C, S, TS, or TS/SCI clearance in the DoD; an individual may have L, Q, or Q with TS authority in the DOE/NNSA. 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. Once the individual is given a final clearance, he or she is able to control documents for that level of classification. Most caveats are granted after individuals review

a briefing explaining the nature of the material and sign forms. After completing this process, these individuals have the appropriate clearance to access the information. The process is commonly referred to as being “read-in” for a caveat.

To be given access to Top Secret or Q-level information a DoD individual must have a favorable single scope background investigation (SSBI). Access to Confidential RD/FRD or L-level information requires a favorable national agency check with local agency and credit check (NACLC). In both instances, only the DoD, DOE/NNSA, Nuclear Regulatory Commission (NRC), and National Aeronautics and Space Administration (NASA) have the authority to grant RD and FRD access. To access CNWDI information, individuals require authorization and a briefing.

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*	TS-RD

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

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

** Access to Sigma 14, 15, & 20 requires additional approval

Figure G.1 DoD and DOE Clearance Levels and Access

G.6 Marking Classified Documents

Two types of documents that require classification markings are originally classified documents and derivatively classified documents.

G.6.1 Originally Classified Documents

EO 13526 requires certain essential markings on originally classified documents. DoDM 5200.01-V2 stipulates marking requirements for classified documents. The marking elements are portion marking, banner line, “classified by” line, reason for classification, and “declassify on” line.

Portions can be paragraphs, charts, tables, pictures, illustrations, subjects, and titles. Before each portion a marking is placed in parentheses: (U) for Unclassified, (C) for Confidential, (S) for Secret, and (TS) for Top Secret and include additional control markings, as appropriate. The subsequent paragraph underneath also has its own classification marking. The classification of the portion is not affected by any of the information or markings of other portions within the same document.

The banner line must specify the highest level of classification of the document and include the most restrictive control marking applicable. The classification is centered in both the header and footer of the document. It is typed in all capital letters and in a font size large enough to be readily visible to the reader. This marking is noted on the front cover, the title page, the first page, and the outside of the back cover. Internal pages may be marked with the overall document classification or the highest classification level of the information contained on that page.

In the lower left-hand corner of the title page, the original classification authority is identified. Authority must be identified by name, or personal identifier, and position. If the agency of the original classifier is not readily apparent, then it must be placed below the “classified by” line.

The reason for classification designation is placed immediately below the “classified by” line. This line should contain a brief reference to the classification category and/or classification guidance. The number 1.4 may appear with corresponding letters, representing section 1.4 of EO 13526 and the classification categories it defines. The information being classified must relate to one or more of the following:

- military plans, weapons systems, or operations;

- foreign government information;
- intelligence activities (including covert action), intelligence sources or methods, or cryptology;
- foreign relations or foreign activities of the United States, including confidential sources;
- scientific, technological, or economic matters relating to the national security;
- U.S. Government programs for safeguarding nuclear materials or facilities;
- vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or
- the development, production, or use of weapons of mass destruction.

The final essential marking is the “declassify on” line. One of three rules listed below is used in determining how long material is to stay classified. All documents must have a declassification date or event entered onto the “declassify on” line. The original classifying authority determines the “declassify on” date of the document using the following guidelines:

- When possible, identify the date or event for declassification that corresponds to the lapse of the information’s national security sensitivity. The date or event shall not exceed 10 years from the date of the original classification.
- When a specific date or event cannot be determined, identify the date that is 10 years from the date of the original classification.
- If the sensitivity of the information warrants protection beyond 10 years, then the original classification authority may assign a declassification date up to, but no more than, 25 years from the date of original classification.

For dates 25 years and beyond, DoDM 5200.01-V2 serves as a reference.

G.6.2 Derivatively Classified Documents

Derivative classification is the act of incorporating, paraphrasing, restating, or generating in new form information already classified and marking the newly developed material consistent with the markings of the source information. The source information ordinarily consists of a classified document(s) or a classification guide issued by an OCA. It is important to note that the DoD can only derivatively classify documents containing RD.

Single Source Document or Multiple Source Documents

When using a classified source document as the basis for derivative classification, the markings on the source document determine the markings to be applied to the derivative document. As with documents created by original classifiers, each derivative document must have portion markings and overall classification markings.

Derivatively classified documents are handled in much the same manner as originally classified documents except for two markings. In a document derived from a single source, portion markings, overall markings, and “declassify on” lines all remain the same as the original document. In a document derived from multiple sources, before marking the document with the “declassify on” line, it is necessary to determine which source document requires the longest period of classification. Once that has been determined, the derivative document should reflect the longest period of classification in the source documents.

In a derivatively classified document, the “classified by” line identifies the name and position of the individual classifying the document. The name and position should be followed by the derivative classifier’s agency and office of origin. In addition, a derivatively classified document includes a “derived from” line. In a document derived from a single source, a brief description of the source document is used to determine the classification of the material.

Documents where classifications are derived from multiple sources are created in the same manner as documents derived from a single classified source. Enter “multiple sources” on the “derived from” line. On a separate sheet of paper, a list of all classification sources must be maintained and included as an attachment to the document. When classifying a document from a source document marked “multiple sources,” do not mark the derived document with “multiple sources.” Instead, in the “derived from” line, identify the source document. In both cases, the “reason” line, as reflected in a source document or classification guide, is not required to be transferred to a derivatively classified document.

Derivative Classification Using a Classification Guide

A classification guide is a document issued by an OCA that provides classification instructions. A classification guide describes the elements of information that must be protected and the level, reason, and duration of classification. When using a classification guide to determine classification, insert the name of the classification guide on the

“derived from” line. Portion markings are determined by the level of classification of the information as listed in the classification guide and the overall marking is determined by the highest level of the portion markings contained within the document. Finally, the “declassified on” line is determined by the classification duration instruction in the guide.

G.6.3 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 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 subject to Administrative and Criminal Sanctions. Handle as Restricted Data in Foreign Dissemination 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.
.....

Additionally, 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.

G.6.4 ATOMAL

RD and FRD marked materials are not cleared for release to the North Atlantic Treaty Organization (NATO) or NATO countries. Organizations that wish to transmit RD or FRD materials to NATO must clear the materials through the JAEIG. RD or FRD materials cleared by the JAEIG for release will be assigned a JAEIG reference number (JRN). If the document is modified after a JRN has been assigned, it will require an additional JAEIG review.

The originating organization, or JAEIG in limited situations, will convert the U.S. classification markings to NATO ATOMAL as required by paragraph 19 and in accordance with paragraphs 38-42 of the *Administrative Arrangements to Implement the Agreement Between the Parties to the North Atlantic Treaty for Co-operation Regarding ATOMAL Information* (C-M(68)41 (7th revise)). These materials, although marked as ATOMAL, have not been assigned a NATO Registry control number and, therefore, not considered NATO materials and can still be disseminated between DoD components via secure email (SIPRNET) in the same manner as FRD materials. Once the material is formally handed over to a NATO Registry and assigned a NATO control number, it becomes a controlled NATO ATOMAL document.

G.7 For Official Use Only and Unclassified Controlled Nuclear Information

FOUO and OUO are terms used by the DoD and the DOE/NNSA, respectively, that can be applied to certain unclassified information. FOUO and OUO designations indicate the potential to damage governmental, commercial, or private interests if disseminated to persons who do not need-to-know the information to perform their jobs or other agency-authorized activities and may be exempt from mandatory release under one of eight applicable *Freedom of Information Act* (FOIA) exemptions.

- Those properly and currently classified in the interest of national defense or foreign policy.
- Information specifically exempted by a statute establishing particular criteria for withholding. The language of the statute must clearly state the information will not be disclosed.
- Information, such as trade secrets and commercial or financial information, obtained from a company on a privileged or confidential basis that, if released,

would result in competitive harm to the company, impair the government's ability to obtain similar information in the future, or protect the government's interest in compliance with program effectiveness.

- Interagency memoranda that are deliberative in nature. This exemption is appropriate for internal documents part of the decision-making process and contain subjective evaluations, opinions, and recommendations.
- Information, the release of which could reasonably be expected to constitute a clearly unwarranted invasion of the personal privacy of individuals.
- Records or information compiled for law enforcement purposes that could reasonably be expected to interfere with law enforcement proceedings; would deprive an individual of a right to a fair trial or impartial adjudication; could reasonably be expected to constitute an unwarranted invasion of the personal privacy of others; disclose the identity of a confidential source; disclose investigative techniques and procedures; or could reasonably be expected to endanger the life or physical safety of any individual.
- Certain records of agencies responsible for supervision of financial institutions.
- Geological and geophysical information concerning wells.

The DoD and the DOE/NNSA also use the term Unclassified Controlled Nuclear Information. The 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 stated in DoDI 5210.83, *DoD Unclassified Controlled Nuclear Information*. The DOE/NNSA uses the term UCNI in a broader manner than the DoD. Designating DoD information as UCNI is governed by 10 USC 128 whereas designating DOE/NNSA information as UCNI is governed by 42 USC 2168 et seq.

