LA-UR-18-21417
Approved for public release; distribution is unlimited.

Title:	A Handbook for Derivative Classifiers at Los Alamos National Laboratory
Author(s):	Sinkula, Barbara Jean
Intended for:	laboratory document
Issued:	2018-02-23

Revised February 2018

A Handbook for Derivative Classifiers at Los Alamos National Laboratory

LA-UR-18-xxxxx

Classification Office, SAFE-IP

Los Alamos National Laboratory is operated by Los Alamos National Security, LLC. (LANS), for the U.S. Department of Energy under contract No. DE-AC52-06NA25396.

Contents

Figures

Chapter 1 - Introduction

The Los Alamos Classification Office (within the SAFE-IP group) prepared this handbook as a resource for the Laboratory's derivative classifiers (DCs). It contains information about United States Government (USG) classification policy, principles, and authorities as they relate to the LANL Classification Program in general, and to the LANL DC program specifically. At a working level, DCs review Laboratory documents and material that are subject to classification review requirements, while the Classification Office provides the training and resources for DCs to perform that vital function.

Classification is the act or process by which certain USG information is determined to require a specific degree of protection against unauthorized disclosure for reasons of national security. P204-3, *Classification of Matter,* is a resource for basic information on LANL's classification program. Classification is distinct from information security, which is the mechanism for protecting classified or unclassified sensitive information once it has been identified and categorized. Classification of information is based on authorities granted to certain USG entities under the Atomic Energy Act (AEA) and under the current Classified National Security Information Executive Order (EO) (EO 13526 at the time of this revision). These authorities delineate four classification categories as indicated:

- The AEA provides the legal basis for classification of "things nuclear," i.e., nuclear weapons, nuclear reactors, and the production of uranium, plutonium, and tritium. Information classified under the Atomic Energy Act is called Restricted Data (RD), Formerly Restricted Data (FRD), or Transclassified Foreign Nuclear Information (TFNI).
- E.O 13526 provides the authority for the classification of other USG information, including certain nonnuclear fields of science and technology, and defense against transnational terrorism. Information classified under Executive Order is called National Security Information (NSI).

Three levels, Confidential (C), Secret (S), and Top Secret (TS), are applied to each classification category (RD, FRD, TFNI, and NSI) to indicate the severity of damage to national security that would result from failure to protect the information. For NSI, the classifying official, called the Original Classification Authority (OCA), is responsible for making that determination. For RD, the Director of the Department of Energy (DOE) Office of Classification makes the initial determination.

Under the aegis of the AEA, the DOE maintains unilateral ownership over RD, and shares authority with the Department of Defense (DoD) for FRD and the Office of the Director of National Intelligence (ODNI) for TFNI. In contrast to the relatively limited number of classification officials responsible for RD, FRD, and TFNI, nearly every entity in the Executive Branch (including DOE, DoD, and ODNI) has OCA over classified NSI equities within their respective jurisdictions. Every USG entity that has equity over classified information is required to issue classification guides to identify what information is classified, by both level and category.

The DOE established the elements of its classification program DOE Order 475.2B, *Identifying Classified Information,* administered by DOE Headquarters Office of Classification (DOE-OC). The contractual obligations assumed by LANL are contained in the Contractor Requirements Document (CRD) for DOE O 475.2B; the Laboratory's implementation of O 475.2B is found in P204-3,

Classification of Matter. Consistent with the CRD, LANL has a Classification Officer (CO) who is solely responsible for establishing and managing the LANL Classification Program. Training and maintaining a cadre of technically qualified DCs is a core element of the LANL Classification Program, and one of the CO's major authorities and responsibilities.

The Los Alamos National Laboratory Derivative Classification Program

The primary purpose of the Classification Program is to ensure that information, documents, and materials originating at the Los Alamos National Laboratory (LANL or the Laboratory) and our subcontractors are reviewed and derivatively classified according to approved classification guidance. The Classification Office serves all Laboratory organizations that use or may use or generate classified information.

The Laboratory's Classification Officer is responsible for appointing, training, and designating LANL DCs according to the process outlined in DOE O 475.2B. To become authorized, a qualified DC candidate must successfully complete a training program, pass a test, and be designated in writing by the LANL Classification Officer. Understanding the material in this handbook will assist DC candidates in the certification process.

The LANL CO classification analysts and staff provide LANL DCs with current classification policies and guidance. The DCs use these policies and guides to ensure that documents and materials originated by Laboratory employees or subcontractors are correctly classified and appropriately marked.

Derivative Classification

Derivative classification is the process of determining whether information classified under the Atomic Energy Act or determined to be classified by an original classifier is revealed by documents or material under review by the derivative classifier.

A *document (or matter or material)* is defined as any record of information regardless of its physical form or characteristics, including, but not limited to, the following: all handwritten, printed or typed matter; all painted, drawn, or engraved matter; all sound, magnetic, electromechanical, or optical recordings; all photographic prints, exposed or developed film, and still or motion pictures; automatic data processing input, memory, program or output information or records such as punch cards, tapes, memory drums or disks, or visual displays, or other digital or electronic format; and all reproductions of the above by any process.

Within LANL and other DOE contractor organizations, all authorized classifiers are derivative classifiers. Derivative classification determinations are based on approved guidance, that is, on explicit instructions found in DOE or other federal-agency-approved classification guides. For RD/FRD, a source document may be used in place of classification guidance in limited circumstances and then only as authorized by the Classification Officer or the Program Classification Officer (DOE O 475.2B). Complete requirements for use of source documents for making classification determinations for TFNI and NSI are found in DOE O 475.2B, Attachment 4.

Thus, derivative classification is the determination that the document or material being reviewed contains information that, in substance, is the same as information described as classified in an approved guidance document. Derivatively classified documents are marked with the appropriate classification level and category, as indicated in the guidance document. The document is marked to identify the source of the classification guidance, and, for NSI, the duration of classification is

provided according to the applicable classification guidance document as "declassify on" instructions that are part of the DC markings on the document. This discussion does not include all aspects of DC markings, such as admonishment statements and special control markings. These requirements are found in DOE O 475.2B and Executive Order 13526, and other resources available for programs with additional requirements.

Challenges to Classification

An employee may challenge a classification decision with the DC who made the determination. An informal challenge would be a discussion of the rationale for the DC's determination and consultation with another DC or subject matter expert (SME) as appropriate. Under no circumstances will the individual making the challenge be subject to retribution. If the employee or organization making the challenge to the decision is not satisfied by the DC's response, an appeal may be made to the LANL Classification Office.

A challenge becomes "formal" when it is put in writing and a written response is requested. If the employee or organization is not satisfied by the response of the Classification Office, the classification determination in question may be forwarded as a formal challenge through the Los Alamos Field Office Classification Officer to the NNSA Classification Officer who then co-ordinates the challenge with the DOE Office of Classification. The LANL Classification Office staff are available to assist the individual or organization in preparing documentation to forward to NNSA/DOE-OC.

All LANL authors, DCs, and managers should also be aware that a challenge to a derivative classification decision is not required to go through the LANL Classification Office and the DOE and NNSA routing described above. An individual can submit a challenge directly to DOE-OC. Complete information on the challenge process is found in DOE Order 475.2B, Identifying Classified Information.

Principles of Association and Compilation

Classification by association concerns:

1. Two or more different, unclassified facts that when combined in a specific way result in a classified statement, or
2. Two or more different, classified facts or unclassified and classified facts that when combined in a specific way result in a higher classification level or more restrictive category.

Associations are classified based on existing classification guide topics. If the document containing the association is portion marked, then each portion of the associated information must be marked at the level (and category if RD or FRD) of the association.

A corollary to this principle is that classified information must not be subdivided into components that are all unclassified (the "Keystone Principle").

Classification by compilation occurs at the document level when:

1. A large number of often similar, unclassified pieces of information whose selection, arrangement, or completeness in the document adds sufficient value to merit classification, or

2. A large number of often similar classified pieces of information or of unclassified and classified pieces of information whose selection, arrangement, or completeness in the document adds sufficient value to merit classifying the document at a higher classification level or more restrictive category.

Compilations are classified based on:

- Classification guide topics, only when an applicable topic exists, or
- A determination by the Director, Office of Classification (for RD/FRD), or by an OCA (for NSI).

A document that is classified based on compilation is never portion marked and must bear the following statement:

> *This document has been classified as a compilation and must not be used as a source document for a derivative classification decision*.

"No-Comment" Policy

It is DOE policy to not comment to uncleared persons on the accuracy or classification of classified information that has not been officially released by the DOE or another USG agency, because to do so weakens the protection provided by classification. This policy applies to information in the open literature suspected of or confirmed to contain classified information. No comment may be made either confirming or denying the accuracy, technical merit, or classification status of classified information that appears in the open.

"GEN-16" refers to the Classification Bulletin titled *No Comment Policy on Classified Information in the Open Literature* (GEN-16, R2, 9/2014). Reference to the current version of GEN-16 can be found in the Index of DOE Classification Guidance, issued by the DOE Office of Classification twice a year. The current version is posted on the LANL Classification Office website.

The "No Comment" policy applies to documents in the open literature that contain classification markings as well as unmarked documents. In many cases, the classification markings on documents in the open literature do not accurately convey the current classification status of the document. In cases where the current classification status of marked documents in the open literature is unknown, only an appropriate authority from the originating agency may determine the current classification status of the document.

Derivative Classifiers need to determine when the "No Comment" policy applies in order to make appropriate classification determinations. All cleared persons need to know how to participate in discussions in classified subject areas with uncleared persons and how to deal with questions about classified information. Researchers must be aware of when and how they may cite sources from the open literature containing classified information. In order to use information in an unclassified document that comes from the open literature and concerns a classified subject area, the review requirements in DOE Order 475.2B, *Identifying Classified Information,* must be followed. This applies even if information contained in the document is taken from internet sites or another open literature source.

All DCs should read and be thoroughly familiar with GEN-16. It provides detailed information on viewing publications; collecting publications or internet web pages in a general subject area of interest; possessing, printing, saving, or sending such documents; and citing documents that

contain “No Comment” information. Further training on GEN-16, with examples of specific situations, is available on DOE's Classification website.

Chapter 2 - Classification Review Responsibilities

Employee/Author Responsibilities

Any employee, which includes subcontractor employees, students, managers, etc., who originates a document or other matter in a potentially classified subject area must ensure that a classification review is obtained by referring it to a DC for evaluation. Employees must complete information security training and understand their responsibilities regarding access to and handling of classified information, as well review requirements for various work products and publications. P204-3-Classification of Matter, P 204-2-Classified Matter Protection and Control Handbook, and PD1022- Review and Release of Scientific and Technical Information (STI) are several relevant LANL Policy documents that provide further information. DOE requirements are found in DOE O 475.2B-Identifying Classification Information, and a list of all applicable statutes, regulations, and directives for the Classification Program is available from DOE's Classification webpage.

Identifying and marking Official Use Only (OUO) information and Unclassified Controlled Nuclear Information (UCNI) also are responsibilities of the DOE Office of Classification. All employees who may work with unclassified controlled information must be briefed on review and security requirements. The LANL Procedure P204-1-Controlled Unclassified Information provides an overview of OUO and UCNI requirements, which are covered in DOE O 471.3 Admin Chg 1, and DOE M 471.3-1 Admin Chg 1, *Identification and Protection of Official Use Only Information*, and DOE Order 471.1B, *Identification and Protection of Unclassified Controlled Nuclear Information*.

All cleared employees should review the DOE *No Comment Policy.* Classification Bulletin GEN-16, REVISION 2, *"No Comment" Policy on Classified Information in the Open Literature,* provides guidance to employees with access to classified information on appropriate actions when classified information, including RD, FRD, TFNI, and NSI, appear in the open literature, and clarifies the circumstances or actions that constitute comment.

Management Responsibilities

Line management is responsible for ensuring that all employees are informed of the classified aspects, if any, of the work they perform, and well as aspects concerning OUO or UCNI. Management is also responsible for ensuring their organizations have sufficient DCs and UCNI Reviewing Officials (RO) and for requesting that the Classification Office train and designate individual DC/ROs. Requests for new DC/ROs are made by submitting "Request for Derivative Classification Authority," online Form 1901, to the LANL Classification Office, SAFE-IP.

Classification Office Responsibilities

The LANL Classification Office is responsible for:

- Review of all technical information in potentially classified subject areas intended for public release from the Laboratory or for widespread distribution
- Administering the Derivative Classifier program
- Disseminating approved classification guidance applicable to laboratory programs
- Conducting classification and controlled information awareness and training

- Adjudicating classification disputes and providing classification, UCNI and OUO guidance to Laboratory workers
- Developing policies and procedures for implementing applicable DOE orders

Derivative Classifier (DC) Responsibilities

DCs May

- ***Review LANL-generated documents or materials that may contain classified information, provided the subject matter is within their programmatic area and assigned DC authorities***.
  For a LANL email message or document on an unclassified computer system that is suspected to contain classified information, the DC should derivatively classify the document if it is within the DC's subject area authorities. If the DC is not qualified to make the determination, the document must be marked as a working paper at the highest suspected level and category (e.g., Secret Restricted Data Working Paper) and referred to an appropriate DC or the Classification Office. The receiver of the information is responsible for notifying the Security Incident Team (SIT), as appropriate, in accordance with LANL P214, Information Security Incident Management.

  If asked to review an email message or other document from a non-LANL organization that contains classified information but has not been marked and protected appropriately, the DC should handle it in accordance with the "No Comment" Policy. DCs should advise the receiver of the email or document to take it to the Classification Office for confirmation and resolution of the issue with the originating organization.

- ***Assign the proper classification level and category based on classification review and approved guidance.***
  As a rule, DC determinations shall be based on approved classification guides authorized for the DC's use. For NSI, source documents may also be used under certain circumstances.

  For derivative classification of NSI, current classification guidance must be used as the basis for determining whether a document or material contains NSI and, if so, its classification level. A source document may be used to classify any email or to classify any other document that contains NSI outside the Derivative Classifier's jurisdiction or authorized subject areas, or when the Classification Officer has specifically approved its use. Additional requirements for using source documents as the basis for a classification determination are found in DOE O 475.2B Attachment 4, 1(b)(3).

  When conducting a classification review, DCs should consider the following:

  - How is the information or item used?
  - What inferences can be derived from the information and context under consideration?
  - What association does the information under review have with other unclassified information, and can one form a classified association?

- ***Upgrade the classification level and/or category*** of LANL documents or material in accordance with approved classification guides or notices as necessary.

- ***Determine that information is unclassified*** when it does not contain technical or programmatic content, or is identical to information officially released as unclassified by the DOE or DoD, or other government agencies. (Note: Congressional records and hearings do not necessarily constitute official release.)

The detailed process for making a classification decision is shown in Figure 2 of Chapter 7.

Specifically, DCs are expected to:

- Be familiar with applicable guidance in their areas of authority.
- Have relevant classification guides readily available. Guides are available from the Classification Office (SAFE-IP), 667-5011. Updates and new versions are announced periodically via email from the Classification Office. The DC is responsible for requesting, by email to dchelp@lanl.gov, updates and new versions of their guides.
- Review and correctly classify documents and materials for which they are responsible.
- Read classification bulletins issued by the Classification Office and retain those that are relevant to their programs.
- Be aware of classification resources available from the Classification web page.
- Consult the Classification Office when uncertain about any classification issue.
- Act as liaison between their organization and the Classification Office, and discuss applicable classification guidance with members of the DC's organization.

DCs May NOT

- Assign levels and categories to information not covered by guidance
- Make classification decisions that are not supported by reasonable interpretation of guidance
- Classify documents containing information outside his/her areas of expertise or authority
- Downgrade or declassify documents or other matter (See Chapter 9)
- Make OUO determinations that are not based on approved classification guidance. Such determinations *must* be made by the author, programmatic owner, or the line manager of the author or owner.
- Perform other types of reviews, such as those for Export Controlled Information (ECI) or Personally Identifiable Information (PII). A DC's authority is limited to making classification, UCNI (if also an UCNI Reviewing Official), and OUO determinations covered by classification guidance.

Requirements to Become a DC

1. Nomination by line management in writing (see "Request for Derivative Classification Authority," Form 1901)
2. Possession of DOE Q-clearance

3. Demonstrated competence in the subject area(s) in which the authority will be used. The designated subject area(s) will be specified by the supervisor who nominates the DC. DCs at Los Alamos are almost always senior, full-time regular LANS employees with expertise in a physical science or engineering specialty relevant to classified programs.
4. Knowledge of DOE classification procedures and familiarity with classification guidance in the subject area in which the authority will be used
5. Successful completion of a training program including passing a test on basic classification principles, and designation in writing by the Classification Office

Requirements to Maintain DC Authority

1. Attend the annual refresher training or one of the make-up sessions provided by the Classification Office
2. Recertification by testing every two years
3. Reliably exercise DC authority
4. Continued need for DC authority

Consequences for Misclassification

Derivative Classifiers avoid misclassification by exercising *due diligence*, including:

1. Only review documents or materials within *jurisdiction* and *subject areas* authorized in writing by the LANL Classification Officer.
2. Maintain and use current approved classification guidance by verifying guides with the current DOE Index of Classification Guidance (or with the appropriate programmatic authority for non-DOE/NNSA-sponsored work) and requesting new or updated guidance when notified that it is available from the Classification Office.
3. Consult with other DCs or the Classification Office if unsure about a determination.
4. Do not review information unless you feel you have sufficient technical expertise in the specific subject, even if it is within your authorized subject areas.

DCs that intentionally or negligently misclassify information, documents, or material may be subject to criminal, civil, and/or administrative penalties. Security infractions can be issued for classifying without authority or outside of granted authority. The classification authority of any individual who demonstrates gross negligence or carelessness that results in misclassification will be cancelled. Note that misclassifying information includes *over classifying* information (e.g. declaring a document to be S//RD when it is really C//RD).

When a DC misclassifies unintentionally, a security infraction is rarely issued. Broadly worded topics may lead to differences in interpretation of classification category or level and the differences must be resolved by a higher authority. One of the Classification Office's functions is to provide interpretation of such topics. If a DC has made an incorrect decision based on his or her interpretation of the classification guidance, the Classification Office may overrule the decision, but a security infraction will not be given to the DC since proper procedures were followed.

Chapter 3 – Publication Review Requirements

Within DOE, classification guidance is the foundation for the classification program. Classification guidance must be used as the basis for determining whether a document or material contains RD, FRD, TFNI, or NSI unless use of a source document is permitted by the Classification Officer. A document or material potentially containing classified or controlled, unclassified information must be reviewed for classification by the appropriate review official to ensure that such information is identified for protection. Specific review requirements are as follows:

- A newly generated document or material in a classified or otherwise sensitive subject area that potentially contains classified or controlled, unclassified information (e.g., UCNI) must receive a classification review by a DC and/or UCNI reviewing Official (RO), as appropriate.
- An existing, unmarked document or material that an employee believes may contain classified or controlled, unclassified information must receive a classification review by a DC and/or RO, as appropriate.
- An existing, marked document or material that an employee believes may contain information classified at a higher level or more restrictive category must receive a classification review by a DC.
- A document or material generated in a classified subject area and *intended for public release* (e.g., for a publicly available webpage, for news organizations) must be reviewed by the Classification Officer or Classification Analyst in the Classification Office; this includes documents provided to or testimony given to Congress.

The only documents regarding LANL activities and intended for public dissemination that do not require review by LANL Classification Office prior to publication are those within the scope of a Designated Unclassified Subject Area (DUSA) and processed for publication through the Laboratory's Review and Approval System for Scientific and Technical Information (RASSTI). Additional information can be found in the DUSA Manual.

Web Pages

Web pages are considered "publications" and are subject to the same review requirements as other documents. For material posted on the "yellow network", i.e., unclassified servers with access limited to Laboratory personnel, only one DC review is required and is sufficient. Content for web pages intended for public release, that is, posting on a "green" server, may be submitted through RASSTI. Web pages with many links or audio visual content can also be reviewed by contacting the Classification Office directly.

E-Mail

E-mail review is not required for strictly administrative information, or for technical information that has already been reviewed or is within the scope of a DUSA. However, caution is advised since classified associations may be created in an e-mail, particularly when a recipient adds comments to an original message.

DC review of e-mail may be required for scientific or technical information, R&D information, programmatic information, etc. The mechanics and requirements for e-mail review are

determined by the Responsible Line Managers in accordance with the principles of ISSM. As with document reviews, it is the responsibility of the sender to obtain a review.

Computer Codes

Computer Codes and other computer software are subject to special DOE requirements before public released. Codes are assigned an LA-CC number. For more information on the process, refer to the Intellectual Property website.

Chapter 4 - Classification Level and Categories

Classification Levels

The three classification levels are Top Secret (TS), Secret (S), and Confidential (C). These three levels apply to the three categories of classified information.

Top Secret (TS)

The "Top Secret" designation requires special handling and special measures of protection. This designation is reserved for information that requires the highest degree of protection. "Top Secret" is assigned only to information, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security. It is current DOE policy to keep the number of TS documents to a minimum, both to limit the quantity of extremely sensitive documents and to minimize the administrative burden of handling TS material.

Secret (S)

"Secret" applies to information that requires a substantial degree of protection. The justification for assigning a "Secret" classification shall be whether its unauthorized disclosure could reasonably be expected to cause serious damage to the national security.

Confidential (C)

"Confidential" is the lowest level of classified information. The damage tests for RD/FRD and NSI are different as noted below:

- Confidential//Restricted Data/Formerly Restricted Data. The Confidential level is applied to information whose unauthorized disclosure could reasonably be expected to cause undue risk to the common defense and security.
- Confidential National Security Information. The Confidential level is applied to information whose unauthorized disclosure could reasonably be expected to damage the national security.

Unclassified (U)

"Unclassified" is the designation for information, a document, or material that is not classified under a statute or executive order, or that has been declassified by proper authority.

The designation, "Unclassified," does not necessarily mean that the information is also uncontrolled, depending on the context.

Classification Categories

Classified information falls into one of four categories. The categories are "Restricted Data," "Formerly Restricted Data," "National Security Information," and "Transclassified Foreign Nuclear Information." They are abbreviated "RD," "FRD," "NSI," and "TFNI."

Restricted Data and Formerly Restricted Data

The devastating power of the atomic bomb, its dramatic role in ending the war with Japan, and the secrecy surrounding its development led to Congress deciding that statutory control over atomic weapons and atomic energy was necessary. To that end, the Atomic Energy Act of 1946 was enacted by Congress. It transferred control of all aspects of atomic energy from the Army to a civilian Atomic Energy Commission (AEC) but continued the Manhattan Project's comprehensive, rigid controls on U.S. information about atomic bombs (later generally known as nuclear weapons) and some aspects of atomic or nuclear energy. The Act established a special category of information called "Restricted Data," which essentially included all nuclear energy-related scientific and technical information.

The Atomic Energy Act of 1946 was replaced by the Atomic Energy Act of 1954. The 1954 act neither significantly changed the definition of RD nor relinquished the AEC's statutory control of RD. However, it placed increased emphasis on wider dissemination of atomic energy information to U.S. industry and to the world. This was a change in philosophy from the 1946 act, which was based on the assumption that helping countries build nuclear reactors also helped them build atomic weapons. The 1954 act was predicated on the belief that access to more atomic energy information by U.S. industry was necessary for the development of nuclear reactors for commercial production of electric power.

The 1954 act also allowed (by joint determination of the AEC and the DoD) the removal of certain weapons-related information from the RD category and specified that it be placed in a new category designated "Formerly Restricted Data." This process is called "transclassification." Such information relates primarily to the military utilization of atomic weapons, and modification of the 1946 act was needed because of the expanding transfer of weapons to the DoD. The deployment of weapons to operational military units created a need for training the military in handling, safeguarding, and other operational aspects of nuclear weapons.

Restricted Data and FRD are under the purview of the Atomic Energy Act and were classified at their inception by the Act. New defense-related nuclear information is handled as SRD and submitted for review to the Director, DOE Office of Classification, who makes the initial determination as to whether it is RD. Restricted Data and FRD information (FRD in coordination with the Department of Defense) may be declassified by the Secretary of the Department of Energy, but cannot be reclassified after being properly declassified.

Restricted Data (RD) is the classification category which consists of information defined as RD by the Atomic Energy Act. Material classified as RD remains classified unless officially declassified by the DOE. It may also be *transclassified*, or removed from the RD category pursuant to Section 142 of the Atomic Energy Act then categorized as FRD.

RD includes data concerning one or more of the following:

- Design, manufacture, or utilization of atomic weapons
- Production of special nuclear material
- The use of special nuclear material in the production of energy

By its very nature, RD information requires strict access limitations. Only individuals granted an appropriate clearance or having special DoD authorization, along with a verified "need to know" for the specific information may have access to RD.

Formerly Restricted Data (FRD) is information related primarily to the military use of atomic weapons. By joint DOE and DoD determination, RD information has been transclassified to FRD. Within the United States, FRD is safeguarded by protections equivalent to that provided for NSI.

RD and FRD are excluded from foreign dissemination except under special agreements.

If you feel that you have information which fits the general definition of RD but is not addressed by a classification topic, contact the LANL Classification Office immediately. The need to identify such information and have it reviewed by the DOE Headquarters Office of Classification is also identified by classification guide topics, which instruct that certain new developments in some subject areas that are beyond the scope of existing topics must be protected at the highest level and category, and referred to the DOE Office of Classification for review and classification determination.

In addition to DOE Order O 475.2B, DOE has codified the administrative policies and procedures for classification in Title 10 of the Code of Federal Regulations, Part 1045(10 CFR 1045), "Nuclear Classification and Declassification."

National Security Information (NSI)

In addition to congressional statutes, several United States presidents have issued executive orders (EOs) concerned with the classification of information. The first EO dealing with classification was issued in 1940 by President Franklin Roosevelt and concerned the protection of "certain vital military and naval installations and equipment." EO 13526, *Classified National Security Information*, issued in 2009, remains in effect at this time. Earlier EOs on this subject have been superseded by subsequent EOs. EO 13526, prescribes a uniform system for classifying, declassifying, and safeguarding information that is not covered under the Atomic Energy Act.

The classification of NSI pertains to information associated with government policy, defense, conventional weapons, intelligence, weapons of mass destruction, and other national security matters. In contrast to RD and FRD, NSI is not automatically classified by law at its inception but must be specifically classified by an authorized original classifier acting under the authority of the EO 13526.

Information may be classified under the terms of EO 13526 only if

- The information is owned by, produced by or for, or is under the control of the United States Government.
- The original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to national security.
- The information falls within one or more of the following categories of information:
  - military plans, conventional weapon systems, or operations
  - foreign government information
  - intelligence activities, 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 national security
  - United States Government programs for safeguarding nuclear materials or facilities

- vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to national security
- the development, production, or use of weapons of mass destruction.

The EO as amended also imposes the following limitations on classification of NSI:

- In no case shall information be classified in order to
  - conceal violations of law, inefficiency, or administrative error
  - prevent embarrassment to a person, organization, or agency
  - restrain competition, or
  - prevent or delay the release of information that does not require protection in the interest of national security.
- Basic scientific research information not clearly related to national security may not be classified.
- Information that has been declassified and released to the public may be reclassified only under certain specific limited conditions and authorities.

Transclassified Foreign Nuclear Information (TFNI)

Transclassified Foreign Nuclear Information is intelligence-related information concerning foreign nuclear programs (e.g. foreign nations, organizations, and may include non-state actors) for which comparable U.S. information would be RD or design-related FRD. Examples of U.S. RD or design-related FRD for which the comparable foreign nuclear information has the potential to be TFNI are nuclear weapon yields and design of non-nuclear components (e.g. safing, arming, fuzing and firing components). While U.S. nuclear stockpile numbers and storage locations are FRD, they are not design-related; therefore comparable foreign information is not TFNI. Intelligence information on foreign stockpile numbers and storage locations does, however, have the potential to be NSI.

TFNI does not include

- Information concerning the nuclear programs of the United Kingdom or Canada
- Information generated under the Tripartate Agreement concerning the development of gas centrifuges, and
- Information exchanged pursuant to an official agreement for cooperation between nations or national-level agencies.

The RD and design-related FRD topics in classification guides may be used to make TFNI determinations for collected intelligence on foreign nuclear programs, except for those noted above. Any technical evaluation of foreign nuclear program information by a U.S./U.K./Canadian government asset that confirms or impugns its credibility, uses RD or design-related FRD in evaluating the foreign nuclear program information, gives insight to the U.S. nuclear weapons program, or reveals U.S. RD information is RD. This will occur when foreign nuclear program information is compared to U.S. RD technology or if U.S. RD technology is used as a basis for analysis of the foreign information.

If you think you have a document that contains TFNI, consult DOE O 475.2B, DOE marking resources, or the Classification Office for detailed instructions on marking and protection.

Classification Level and Category of a Document

The classification *level* is determined by its ranking in terms of sensitivity and potential damage to national security if disclosed to unauthorized persons. Thus, damage from unauthorized disclosure of TS information is the greatest, and TS is ranked higher than S, which is ranked higher than C. The classification *category* assigned to a document containing more than one category of classified information is determined according to the ranking of the categories: RD is ranked higher than FRD, which is ranked higher than NSI. A document is marked and protected at the highest level and highest category, which are combined as shown in Figure 1. For example, a document containing both SNSI and CRD information would be given the overall classification level and category of SRD (because S is the highest level and RD is the highest category of information found in the document). The document is marked SRD, even though it contains no specific SRD information.

The ranking and combining of classification levels and categories depicted in Figure 1 also identifies combinations of information access permitted for Q- and L-clearance holders. The combinations highlighted in yellow are those that L-cleared individuals may access, and the blue level-category combinations may be accessed by Q-cleared individuals in addition to those shown in yellow.

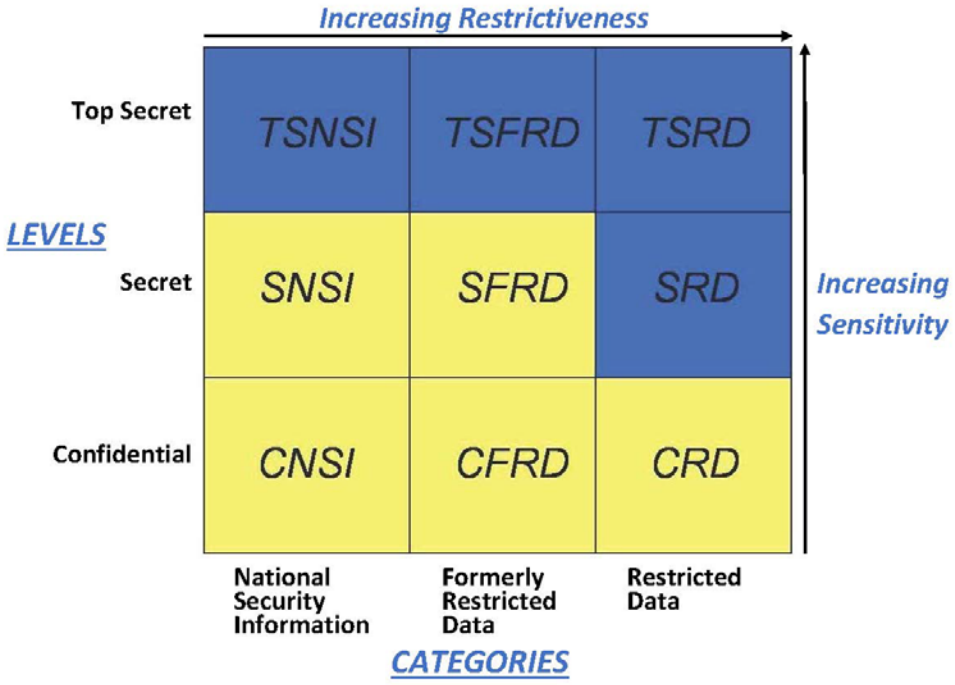


Figure 1. Combinations and rankings of classification levels and categories

Chapter 5 - Classification Guides

Classification guides are the basic tools of the DC. Most classification decisions a DC makes will have a basis in classification guidance. A DC may only use guides in their authorized subject area(s) for derivative classification.

The introduction to each DOE guide explains its purpose, scope, basic policy, use, and limitations (with cautions). These introductory statements and warnings are mandatory reading.

Use of these guides often entails difficult judgments and interpretations of topics. The lack of an explicit statement in a guide classifying specific information does not mean that the information is unclassified. If a DC cannot determine the proper classification of an element of information using classification guidance, or if guidance does not appear to exist, he/she contacts the local classification officer for assistance. If the problem cannot be resolved, the local Classification Officer will refer the issue to the Field Office Federal Classification Officer. For these reasons, only DCs may possess and use classification guides. There are extracts of certain guides containing only the reasons for classification and broad guidance sections available for use by non-DCs as classification awareness tools.

Classification decisions can be difficult when inconsistent guidance is used. Three possible causes for inconsistencies are that guidance is ambiguous, outdated, or conflicting. When information is described equally well by more than one topic with different classification levels, use the most restrictive guidance until clarification is obtained. To prevent problems using outdated guidance, always keep guides updated, and use the guidance with the most current date. *DCs are not to keep superseded or outdated guides, even for reference*. Only the Classification Officer may have these guides for reference. The Classification Office should be consulted to help with resolution of any of these problems.

The DOE Classification Guidance System

As a DOE National Laboratory, LANL plays a major role in both the development and the use of DOE classification guides. The DOE classification policy is established on the basis of the Atomic Energy Act of 1954, as amended, and 10 CFR 1045 for RD and FRD information, and 32 CFR 2001 and EO 13526 as the bases for NSI.

From these laws and directives the DOE has developed classification policy guidelines, which become the basis for a hierarchy of classification guides used to identify classified and unclassified information related to nuclear weapons and other classified programs. The DoD and other federal agencies often use classification guides developed jointly by DOE and the agency. The Nuclear Weapon Classification Policy Guide and other weapon classification guides are jointly approved for use by both the DOE and the DoD.

A listing of the DOE Headquarters (DOE HQ) classification publications, except those relating to special access programs, is provided in the *Index of DOE Classification Guidance*.

Classification Bulletins

Bulletins are issued by DOE Headquarters Office of Classification to implement classification policy. Classification bulletins are used to address a specific issue or concepts, and issued by DOE to

interpret, clarify, or expand on guidance contained in a program guide. Classification bulletins may also be used by DOE to implement changes in classification procedures. DOE HQ bulletins are also listed in the *Index of DOE Classification Guidance*.

Classification Guides for Non-DOE Work

The Laboratory does a significant amount of work for non-DOE sponsors. If that work will use or generate classified information, the Classification Officer must review the work request and proposed classification guidance and certify in writing that the guidance does not contradict DOE classification guidance, *prior to commencement of the work*.

For unclassified work conducted for non-DOE sponsors, the funding organization is required to provide a written statement that classified activities are not part of the project. Much of this work may fall within the scope of a DUSA and thus not require DC support.

Chapter 6 - Access Limitations

Access limiters are not classification levels or categories but are used on certain classified documents to indicate that the information has additional access or handling requirements. At LANL the line organizations and programs are responsible for assignment of access limitations. Access to such information is limited to those personnel who are properly cleared and require access to the classified information in the performance of their duties. The DCs concerned provide a double check to assure that the appropriate access control level has been assigned in conjunction with the classification level and category of the reports or documents. Definitions and descriptions of some of these access limiters are provided in the following sections.

Nuclear Weapon Data (NWD)

Nuclear Weapon Data is a category of information that was created by DOE's former Military Applications Program Office and is described in detail in DOE Order 452.8, *Control of Weapon Data.* NWD comprises RD/FRD information concerning the design, manufacture, or utilization (including theory, development, storage, characteristics, performance, and effects) of atomic weapons or atomic weapon components. It includes information incorporated in or relating to nuclear explosive devices. There are two types of NWD: non-Sigma NWD and Sigma NWD. NWD Sigma categories were established to provide additional need-to-know protection of specific types of NWD. This Order provides for:

Sigma NWD

The Sigma categories were created by DOE to further restrict access to certain NWD information requiring a certified "need to know" and an appropriate clearance. All documents containing Sigma NWD require designation of the Sigma category of access control on the first page of the document. Definitions of the Sigma categories currently in effect, as given in DOE Order 452.8, are as follows:

> *Sigma 14*. The category of sensitive information concerning the vulnerability of nuclear weapons to deliberate, unauthorized nuclear detonation.
>
> *Sigma 15.* The category of sensitive information concerning the design and function of nuclear weapons use-control systems, features, and their components. This includes use-control information for passive and active systems.
>
> Sigmas 14 and 15 are discussed in detail in DOE Order DOE O 452.7*, Protection of Use Control Vulnerabilities and Designs.*
>
> *Sigma 18* includes information that would allow or significantly facilitate 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 NNSA or successor organization determines which information is placed in the Sigma 18 category.

The list of Sigma 18 information is found in DOE O 452.8, *Control of Nuclear Weapon Data.*

Sigma 20. A specific category of nuclear weapon data that pertains to "crude, simple or innovative" improvised nuclear device designs, concepts, and related manufacturing or processing pathways. Sigma 20 is discussed in DOE O 457.1A, *Nuclear Counterterrorism.*

Access to Sigma Categories

Sigmas 14, 15, and 20 require access to be granted through a site control coordinator.

All Q-cleared DOE/NNSA Nuclear Security Enterprise employees automatically have Sigma 18 access authority.

Non-Sigma NWD

Non-Sigma weapon data is a large category that comprises all RD and FRD weapon data that does not fit into one of the Sigma categories. Access to non-Sigma weapon data is granted based solely on the employee's clearance level and need-to-know.

Critical Nuclear Weapon Design Information (CNWDI)

CNWDI was established to strengthen classified information controls within the DoD. CNWDI markings are not required for communications within the DOE complex. This category of control includes TS//RD and S//RD revealing the theory of operation or design of the components of a thermonuclear or fission bomb, warhead, demolition munitions, or test device. Specifically excluded from CNWDI is information concerning arming, fusing, and firing systems; limited-life components; and total quantities of fissionable, fusionable, and high-explosive materials by type. Also among the excluded items are the components that military personnel set, maintain, operate, test, or replace. Unlike DOE's comparable sigma access designation, CNWDI does not apply to C//RD or any level of FRD.

In classification guides, CNWDI is indicated by the designator (N), placed adjacent to the classification level and category for a specific classification topic. It is the responsibility of Laboratory employees to insure that DoD and DoD contractor personnel with whom they have discussions or meetings have been certified by their headquarters as being authorized for access to CNWDI. All TS//RD or S//RD reports, or other documents transmitted to DoD require a special CNWDI marking if they contain CNWDI information.

UK Atomic Information

The LANL UK Program Office is responsible for the management of LANL's technical exchanges with the United Kingdom in association with the 1958 US-UK Mutual Defense Agreement (MDA). The UK Program Office provides **training** on identifying, marking, and transmitting documents to the UK.

Other Access Limitation Markings

Documents containing certain types of classified information must also be specially marked to control access to the information. Examples of these special markings that are sometimes found in DOE programs include but are not limited to the following:

- NNPI Naval Nuclear Propulsion Information
- NOFORN Not Releasable to Foreign Nationals

- ORCON Dissemination and Extraction of Information Controlled by Originator (ORCON is used exclusively on classified intelligence information)

Foreign Government Information (FGI)

The legal basis for protecting foreign government classified information and *unclassified information provided in confidence* is Executive Order 13526, which is implemented by 32 CFR Part 2001, Classified National Security Information Final Rule.

A cover sheet for "Confidential Foreign Government Information – Modified Handling Authorized (C/FGI-MOD)" can be found on the LANL Classification Web Page. DOE O 471.6, *Information Security*, provides requirements for marking and handling C/FGI-MOD.

For additional information, please contact the LANL Classification Office.

Chapter 7 - Making a Derivative Classification Decision

The process of derivatively classifying a document is graphically shown in Figure 2.

The DC verifies that the document's subject matter lies within the DC's technical expertise and assigned area(s) of authority. If not, the document should be referred to another DC or the Classification Office for review. If it is within the DC's purview, he or she determines if there is information in the document that might be classified by other U.S. government agencies such as the DoD or State Department, or a foreign country. If so, it is the DC's responsibility to determine if there is a joint, interagency, or other-agency classification guide that would apply to the information. The Classification Office will assist the DC if approved guidance is not available.

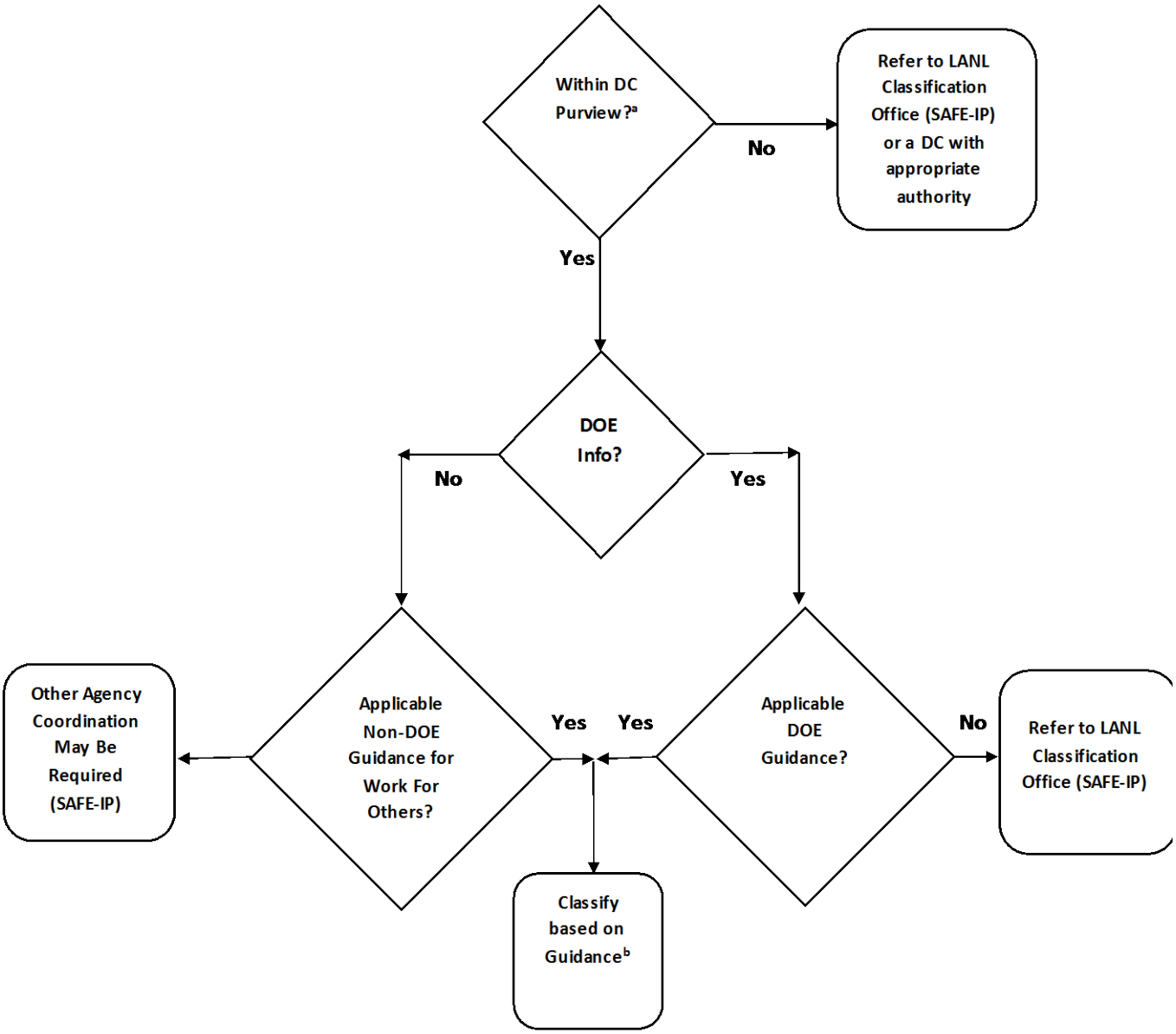
If the document includes only DOE information, it is reviewed by the DC using DOE-approved classification guidance. If the document is found to include classified information, the DC determines the appropriate classification *level* and *category* for the complete document, its abstract (if any), and its title. If it is not possible for the DC to determine the classification based on approved DOE guidance, the DC refers the document to the Classification Office for assistance in assigning the correct classification level and categories for the information under review.

If the information in the document is determined to be unclassified, the DC should consider whether the document contains Unclassified Controlled Nuclear Information (UCNI). To make an UCNI determination, the DC must also be a Reviewing Official (RO). The document may also contain Official Use Only (OUO) information. Some classification guides specify certain information as OUO (see Chapter 11). Further discussion of OUO and UCNI, as well as other types of controlled unclassified is found in LANL Policy 204-1, *Controlled Unclassified Information.* If the DC determines that the document does not include either classified or controlled unclassified information, the DC informs the author that the document is unclassified, and no DC marking is required. DCs are encouraged to keep records about documents that he or she has reviewed.

When making a derivative classification determination, DCs must be aware importance of avoiding over-classification and of considering information sharing needs, i.e., the need to share both unclassified and classified information with other government agencies so that agencies can work together effectively to protect national security. Because classification and security clearance requirements are not uniform across government agencies concerned with national security, over-classification can result in the inability to share information effectively.

There are sanctions for improper use of derivative classification authority. However, as discussed in Chapter 2, as long as a DC does classification reviews within his or her jurisdiction and subject area authorities, and exercises due diligence in using and interpreting classification guidance, unintentional errors are not subject to sanctions.

Derivative Classification Procedure



[a] Is the information in the DC's assigned area of authority?

[b] For NSI documents, source documents may be used under certain circumstances.

Figure 2. Derivative classification decision flow chart

Chapter 8 - Marking Documents

DCs ensure that the required classifier markings are placed on the documents they have reviewed. Laboratory implementation requirements relating to marking documents are found in P 204-2, "Classified Matter Protection and Control Handbook." DCs are responsible for the front page markings, including the classification authority block, page markings, and any admonishment statements or caveats. DCs may personally mark the document or provide all relevant information to the individual that will mark the document. DCs are encouraged to allow Classified Matter Custodians (CMCs) in their organizations, or others specifically trained in marking classified documents, to apply proper classification markings to documents the DC has reviewed.

For marking requirements and examples, refer to P204-2 and marking resources provided by the DOE Office of Classification. DC training materials and the introductory chapter of DOE classification guides are also resources for applicable marking requirements.

Marking Titles and Subject Lines

Except in extraordinary circumstances, titles of classified documents and subject lines on classified correspondence must be unclassified and not OUO or UCNI, since they are frequently used for reference purposes on mail logs, databases, document receipts, file cards, etc. If it is necessary to include classified information in the title or subject line of a classified document, the abbreviation for the classification level and category must be indicated in parentheses, e.g., "(SRD)" for Secret Restricted Data, *before* the title or subject line. If the title or subject line is unclassified, "(U)" is required.

Portion Marking

32 CFR 2001 requires that each NSI document be marked to indicate which portions are classified (with the applicable classification level) and which portions are not classified. This requirement is known as "portion marking." Each paragraph, figure, bullet, etc. of a report is marked to indicate its classification. It is the DC's responsibility to portion mark an NSI document.

There is no requirement to portion-mark LANL documents generated before October 14, 1995. Portion marking is required only for documents that contain *only* classified National Security Information, or contain TFNI and NSI. Documents that contain Restricted Data and/or Formerly Restricted Data are not required to be portion-marked, even if they contain NSI or TFNI.

When a document is portion marked, the DC must always be careful to consider the possibility of classified associations. DCs must look at a document in its entirety. If two unclassified paragraphs within a document reveal a classified association, the two paragraphs must both be marked with the appropriate classification level.

Although RD and FRD documents are not required to be portion-marked, the classification level and category for RD and FRD document titles as well as the subject lines for classified correspondence must be indicated in parenthesis *before* the information. If the title or subject line is unclassified, "(U)" is required.

When multiple topics, guides, and/or source documents are used to derivatively classify NSI, the ''Declassify On'' line shall reflect the longest duration of any of its sources. See 32 CFR 2001, Classified National Security Information, Subpart C—Identification and Markings, for complete requirements.

Working Papers and Draft Documents

Working papers and draft documents must be properly marked and protected at the highest potential level and category of the information in the document, or marked and protected at the highest level and category of information resident on the computer system. Printed output must be handled in the same manner, which is sometimes called marking the output at "system high" until it is reviewed by the derivative classifier.

Working papers must be:

- Marked with the date created
- Protected and marked in accordance with the highest potential classification level, category (if RD, FRD, or TFNI), and caveats if applicable
- Annotated with "Working Paper" or "Draft" on the first page of the text
- Protected by the approved classified cover sheet
- Destroyed when no longer needed
- Accounted for (if required) and controlled and marked in the manner prescribed for a finished document of the same classification when the working papers are retained for more than 180 days from the date of origin or filed permanently.

The marking requirements for working papers and draft documents are explained in detail in LANL P204-2, Classified Matter Protection and Control (CMPC) Handbook. They can also be found in DOE's CMPC Marking Resource. Comprehensive requirements for working papers are found in DOE O 471.6, Information Security, and DOE O 475.2B and 32 CFR 2001, as applicable.

Chapter 9 - Declassification, Downgrading, and Upgrading

Declassification

The term “declassification” has two different, but related, meanings:

- ***Declassification of Information***

Declassification of information is the determination by appropriate authority that information no longer requires classification. This determination is made by DOE for RD, by DOE and DoD for FRD, and by the official who authorized the original classification for NSI. Incorporation of this determination into classification guidance allows Derivative Declassifiers (DDs) to declassify documents or material.

- ***Declassification of Documents or Material***

Declassification of documents or material is the act of removing classification markings that no longer apply. Classified documents may only be declassified after two independent reviews. One review may be by a DC, and the second must be by a DD. The only DDs at Los Alamos are classification analysts in the Classification Office. A document to be declassified must be protected as classified until both reviews have been completed.

Sanitization (or Redaction)

Sanitization is the process of rendering classified documents unclassified by physically removing or obliterating the classified information. This process requires two separate reviews just as for declassification and special declassification markings.

Document Review Requirements

1. Newly Created Documents

   An unclassified version of a classified document may be produced by the author only during the initial creation of the document. This may be done by deleting (e.g. on a word processor), all classified information to create a “new” document that does not carry any classification or declassification markings. A DC must review this “new” document to confirm that it is unclassified. The unclassified version must carry the identifier “Unclassified Version” in the title to differentiate it from the classified version.

   Once a classified version of a document is finalized, reviewed by a DC, and properly marked, any sanitization/redaction to produce an unclassified version requires both a DC and DD review. Note that both electronic and paper documents with the potential for classification must be marked as a working paper and reviewed by a DC (and marked) within 180 days of creation.

   Since most word processors retain information about deleted material, the electronic file of a redacted classified document is considered classified at the original level and category until it has been processed by a DOE approved file scrubbing program.

2. Existing Documents

   Sanitization/Redaction of existing classified, properly marked documents to produce an unclassified document requires two signatures; DC and DD. Such redacted documents must be marked "Redacted Version" on the first page.

3. Extracts of Classified Documents

Sometimes a portion of a classified document (a table, chapter, figure, etc.) may be extracted as a stand-alone document or included in a new document. If the extract is intended to be a stand-alone, unclassified document, it must be reviewed by a DC and DD. This is true regardless of the method of transfer; e.g. cut-and-paste vs. retyping the material. If the extract is included in a new document, the new document must be reviewed by a DC.

4. Documents Marked "System High"

   Many classified systems are set up to automatically mark printed output "system high", which means at the highest level and category of the information resident on the system (usually S//RD working paper). This is considered to be the electronic equivalent of marking a paper document at the highest level and category until a DC review can be obtained. Only a DC review of the printed document is required. *DC review of all printed output from classified systems is required.*

   Note: This includes the output from nuclear material inventory software, regardless of how it is marked by the system.

   Complete requirements for output from classified information systems is found in DOE O 475.2B, Identifying Classified Information, Attachment 4, paragraph 1a(6).

5. Unmarked Documents

Unmarked documents, electronic or paper, suspected of containing classified information must be reviewed by DC.

Downgrading

The term "downgrading," like "declassification," also has two meanings:

- ***Downgrading Information***

Downgrading information is the determination by appropriate authority that information may be protected at a classification level lower than the initial level, but not lower than Confidential/NSI (i.e., not declassified).

- ***Downgrading Documents or Material***

Downgrading documents or material is the act of changing classification markings to reflect a lower classification level or category. Downgrading requires only a single review by a DD. DCs may not downgrade documents or material.

Automatic Declassification of NSI Documents

DOE documents marked as containing NSI that do not specify a date or event for declassification are never automatically declassified.

Documents classified as NSI have the schedule of classification marked on the classification stamp, as explained in "Duration of Classification," in Chapter 8. However, Public Law 104-106 (1996 National Defense Authorization Act) requires that prior to automatic declassification of a DOE/NNSA NSI document upon passage of the declassification date or event, the document must be reviewed by a DD to confirm that it does not inadvertently contain any RD or FRD information or that the classification duration has not changed. An NSI document marked as exempt from declassification within 25 years is not automatically declassified. Holders of "expired" NSI documents (those having passed the schedule of classification indicated on the document, for example, a date or event has passed) must have them reviewed by a DD for declassification.

Classified Information Improperly Released

Information classified in accordance with official DOE guidance is not declassified automatically as a result of any unofficial publication or inadvertent or unauthorized disclosure of identical or similar information, either in the United States or abroad. See the "No-Comment" Policy in Chapter 1.

Declassification and Downgrading Notices

A DD who declassifies a document that is less than 25 years old notifies the originator or document custodian, if possible, and provides him or her with enough information to identify the specific document. Similarly, a DD authorizing the downgrading of a document notifies the originator or document custodian with a sufficient description to identify the specific document. Declassification and downgrading notices are unclassified unless the notices themselves contain classified information.

Upgrading Notices

When a DC determines that a Los Alamos document requires higher classification than it originally had, or when a document previously issued as unclassified is determined to be classified, the DC shall notify the originator or document custodian (if he or she has the proper security clearance for the upgraded document) with enough information to identify the document, and the new level, category, and classifier information. A DC who believes that a non-LANL document is not correctly classified should protect the document at the highest potential level and category and consult the Classification Office.

Some documents may require upgrading because of new or revised classification guidance or classification bulletin from DOE Office of Classification.

If the document was sent to a recipient who does not have the proper security clearance, do not contact that person. Notify the SIT immediately.

For comprehensive requirements on upgrading, see DOE O 475.2B, Attachment 4, paragraph 3b.

Chapter 10 - Unclassified Controlled Nuclear Information (UCNI)

In 1981, Congress added provisions to Section 148 to the Atomic Energy Act of 1954 at the request of DOE. It established UCNI as an additional means of controlling certain information associated with nuclear weapons. It recognized the existence of information relating to nuclear material production, use, and safeguarding that should be protected, but that cannot be classified and protected under the Atomic Energy Act or by Executive Order. 10 CFR 1017-Identification and Protection of Unclassified Controlled Nuclear Information established the requirements for UCNI. The requirements and responsibilities for DOE's UCNI program are provided in DOE O 471.1B, "Identification and Protection of Unclassified Controlled Nuclear Information."

Laboratory implementation requirements for UCNI are found in P 204-1, Controlled Unclassified Information.

UCNI Review Requirement

Any document that may contain UCNI must be reviewed by an UCNI Reviewing Official in accordance with § 1017.15(a). When a document must be transmitted outside of the originating organization prior to review by an RO, it must be marked "Protect as UCNI Pending Review" in accordance with § 1017.15(a) and transmitted in accordance with § 1017.27.

Determinations

UCNI determinations are made by Reviewing Officials (ROs) and are based on DOE-approved classification guidance. At Los Alamos, all ROs are DCs.

UCNI at Los Alamos National Laboratory

At Los Alamos, SAFE-IP appoints ROs who are authorized to determine whether information in documents they review is UCNI. These ROs must base their decisions on topical or internal guidelines.

UCNI topics are found in TCGs, CGs, and Unclassified Controlled Nuclear Information Guidelines as listed in the Index of DOE Classification Guidance. The DOE Classification Guide, CG-SS-5, *Classification and UCNI Guide for Safeguards and Security Information*, contains many UCNI topics that are applicable at LANL. Guidance is also provided in Classification Office memos.

Any DC who reviews material that may contain UCNI must have UCNI RO authority. Follow process to request appointment by SAFE-IP as an RO. SAFE-IP provides the necessary training.

Chapter 11 - Official Use Only (OUO) Information

The Department of Energy (DOE) established a program within the DOE and NNSA to identify certain controlled unclassified information as Official Use Only in 2003 and released DOE Order (O) 471.3, Identifying and Protecting Official Use Only Information and DOE M 471.3, Manual for Identifying and Protecting Official Use Only Information.

The Laboratory's OUO program is described in P204-1, Controlled Unclassified Information.

Complete requirements for review, identification and protection of documents or material containing OUO are in DOE O 471.3 and DOE M 471.3 1. Derivative Classifiers are only responsible for making determinations and marking OUO that is designated by topic in approved DOE classification guidance. The DC completes the OUO marking block, cites the appropriate exemption provided in the classification guidance, and lists the guide's short title.

A DC has no authority to identify or mark OUO documents when the OUO information is not identified in classification guidance. Other information may designated as OUO because it meets certain criteria that may make it eligible for denial of release under the Freedom of Information Act (FOIA). The author, manager, or program office responsible for the material being considered for OUO protection determines whether the material meets the OUO criteria and completes the OUO marking block. These determinations include those based on laws or regulations and those based on programmatic considerations. See P204-1 for further discussion.

Acronym List

AEC	Atomic Energy Commission
C	Confidential
C/FGI-MOD	Confidential/Foreign Government Information-Modified Handling Authorized
CFR	Code of Federal Regulations
CG	Classification Guide
CMC	Classified Matter Custodian
CNWDI	Critical Nuclear Weapon Design Information
CRADA	Cooperative Research and Development Agreement
DC	Derivative Classifier
DD	Derivative Declassifier
DoD	Department of Defense
DOE	Department of Energy
DUSA	Designated Unclassified Subject Area
ECI	Export Controlled Information
EO	Executive Order
FGI	Foreign Government Information
FOIA	Freedom of Information Act
FRD	Formerly Restricted Data
GEN-16	"No Comment" Policy on Classified Information in the Public Domain
LANL	Los Alamos National Laboratory
NNPI	Naval Nuclear Propulsion Information
NNSA	National Nuclear Security Administration
NOFORN	Information may NOt be released to FOReign Nationals
NSI	National Security Information
NWD	Nuclear Weapon Data
ORCON	Distribution controlled by the originating organization
OUO	Official Use Only
RD	Restricted Data
RO	Reviewing Official
S	Secret
SAFE-IP	Classification Office
SIT	Security Incident Team
SME	Subject Matter Expert
TCG	Topical Classification Guide
TFNI	Transclassified Foreign Nuclear Information
TS	Top Secret
U	Unclassified
UCNI	Unclassified Controlled Nuclear Information

References

32 CFR §2001.54, National Defense, PART 2001—CLASSIFIED NATIONAL SECURITY INFORMATION, Subpart E—Safeguarding, Foreign government information (FGI).

32 CFR Parts 2001 and 2003 Classified National Security Information, Final Rule, June 25, 2010.

The Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA), published this Directive as a final rule and pursuant to Executive Order 13526 (hereafter the Order), relating to classified national security information. The Executive order prescribes a uniform system for classifying, safeguarding, and declassifying national security information. It also establishes a monitoring system to enhance its effectiveness. This Directive sets forth guidance to agencies on original and derivative classification, downgrading, declassification, and safeguarding of classified national security information.

Atomic Energy Act of 1954, as amended, 10 CFR part 1045.

Classification Bulletin GEN-16, REVISION 2, "No Comment" Policy on Classified Information in the Open Literature, September 23, 2014.

Classified Matter Protection and Control (CMPC) Marking Resource: Examples of Acceptably Marked Classified Matter, U.S. DOE, January 2015.

DOE Manual 471.3, Manual for Identifying and Protecting Official Use Only Information.

DOE Order 452.7, Protection of Use Control Vulnerabilities and Designs, May 14, 2010.

The order establishes the policy, process and procedures for control of sensitive use control information in nuclear weapon data (NWD) categories Sigma 14 and Sigma 15 to ensure that dissemination of the information must be restricted to individuals with valid need to know.

DOE Order 452.8, Control of Nuclear Weapon Data.

DOE Order 457.1A, Nuclear Counterterrorism

The Order defines requirements for the protection of sensitive improvised nuclear device information and provides a framework to support DOE activities related to nuclear counterterrorism. A supplemental DOE Manual, C*ontrol of and Access to Improvised Nuclear Device Information*, provides requirements and procedures for protecting Sigma 20 information.

DOE Order 471.3, Identifying and Protecting Official Use Only Information.

DOE Order 471.6, Information Security.

DOE Order 475.2B, Identifying Classified Information.

Establishes the program to identify information classified under the Atomic Energy Act [Restricted Data (RD), Formerly Restricted Data (FRD), and Transclassified Foreign Nuclear Information (TFNI)] or Executive Order (EO) 13526 [National Security Information (NSI)], so that it can be protected against unauthorized dissemination.

Executive Order (EO) 13526, Classified National Security Information, Issued by the White House, December 29, 2009. EO 13526 is implemented by 32 CFR Parts 2001 and 2003.

INDEX 16-2, Index of DOE Classification Guidance, July 2016.

ISOO Directive No. 1, Classified National Security Information Directive Number 1 (also referred to as the Information Security Oversight Office Directive Number 1), September 22, 2003. National Archives and Records Administration Information Security Oversight Office, 32 CFR Parts 2001 and 2004 Classified National Security Information (Directive No. 1); Final Rule.

P204-1, Controlled Unclassified Information.

P204-2, Classified Matter Protection and Control Handbook.

P204-3, Classification of Matter.

Protecting the Nation's Nuclear Information: An Overview of the Restricted Data and Formerly Restricted Data Classification System, DOE Office of Classification, available from the DOE Office of Scientific and Technical Information (OSTI).