U.S. NUCLEAR REGULATORY COMMISSION MANAGEMENT DIRECTIVE (MD)

MD 12.6	NRC CONTROLLED UNCLASSIFIED INFORMATION (CUI) PROGRAM	DT-21-12
Volume 12:	Security	
Approved by:	Daniel H. Dorman Executive Director for Operations	
Date Approved:	December 3, 2021	
Cert. Date:	N/A, for the latest version of any NRC directive or handbook, see the online MD Catalog.	
Issuing Office:	Office of the Chief Information Officer Governance & Enterprise Management Services Division	
Contact Name:	Tanya Mensah	

EXECUTIVE SUMMARY

Management Directive (MD) 12.6, "NRC Controlled Unclassified Information (CUI) Program," (formerly titled, "NRC Sensitive Unclassified Information Security Program" (SUNSI)) is revised to describe the agency Controlled Unclassified Information (CUI) program. The NRC CUI Program implements 32 CFR Part 2002, "Controlled Unclassified Information," (CUI rule) in order to protect NRC sensitive but unclassified information from unauthorized access, use, disclosure, disruption, modification, and destruction. The CUI rule standardizes markings across all Federal agencies; therefore, SUNSI and the associated markings, such as Official Use Only, will be discontinued once CUI is implemented at the NRC.

MD 12.6 is issued in accordance with Commission direction to ensure NRC information is appropriately protected.

TABLE OF CONTENTS

I. POLICY

A. It is the policy of the U.S. Nuclear Regulatory Commission (NRC) to implement and maintain an agencywide Controlled Unclassified Information (CUI) Program to protect information in accordance with Executive Order 13556, "Controlled Unclassified Information," Title 32 of the *Code of Federal Regulations* (CFR), Part 2002, and the CUI Registry.

B. NRC CUI protections shall be consistent with Federal guidance and commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information that qualifies as CUI.

II. OBJECTIVES

- Implement a CUI program for designating, handling, marking, storing, protecting, destroying, transmitting, reproducing, decontrolling, and receiving CUI.
- Establish a CUI self-inspection and oversight program to meet the requirements stated in 32 CFR Part 2002.

- Ensure all NRC personnel, including employees, contractors, and detailees receive training to ensure appropriate protections for CUI.

III. ORGANIZATIONAL RESPONSIBILITIES AND DELEGATIONS OF AUTHORITY

A. Executive Director for Operations (EDO)

1. Ensures agency senior leadership support for the CUI program.
2. Makes adequate resources available to implement, manage, and comply with the CUI program as administered by the CUI Executive Agent (EA). Executive Order 13556 designates National Archives and Records Administration (NARA) as EA to implement the Order and oversee Federal agency actions to ensure compliance.
3. Designates the CUI Senior Agency Official (SAO), in writing, and assigns the CUI SAO with the responsibility for overseeing the agency's CUI program implementation, compliance, and management.
4. Includes the CUI SAO in agency contact listings.
5. Ensures that the CUI SAO designates a CUI Program Manager.
6. Approves agency policies, as required, to implement the CUI program.
7. Establishes and maintains a self-inspection program to ensure the agency complies with the principles and requirements of 32 CFR Part 2002.

B. Inspector General (IG)

1. Investigates instances of misuse of CUI in violation of 32 CFR Part 2002.
2. Approves the decontrol of IG investigative records.

C. Office of the General Counsel (OGC)

1. Provides legal advice related to the CUI program.
2. Approves the decontrol of documents generated by former Commissioners.

D. Director, Office of International Programs (OIP)

Administers agency-to-agency international agreements for the sharing of CUI.

E. Controlled Unclassified Information (CUI) Senior Agency Official (SAO), Office of the Chief Information Officer (OCIO)

1. Designates a CUI Program Manager.
2. Directs and oversees the agency's CUI program.

3. Ensures NRC has implementation policies and plans for the marking, safeguarding, disseminating, and decontrolling of CUI, and provides updates on agency CUI implementation efforts to the CUI EA.
4. In coordination with the Chief Human Capital Officer (CHCO), implements and maintains a CUI education and training program in accordance with 32 CFR 2002.30.
5. Submits to the CUI EA any law, regulation, or Governmentwide policy not already incorporated into the CUI Registry that NRC proposes to include/add as a category to the CUI Registry for safeguarding or dissemination. (The CUI Registry is available electronically at https://www.archives.gov/cui.)
6. Coordinates with the CUI EA, as appropriate, any proposed law, regulation, or Governmentwide policy that would establish, eliminate, or modify an organizational index grouping or category of CUI, or change information controls applicable to CUI.
7. Develops and implements the agency's CUI self-inspection program, in coordination with office directors and regional administrators, and reviews and assesses the CUI program at least annually.
8. Provides an annual CUI program report to the NRC EDO and CUI EA that includes an analysis and conclusions from the CUI self-inspection program.
9. Establishes a corrective action program, in coordination with office directors and regional administrators, to address CUI program deficiencies and retains records of corrective actions.
10. Establishes a process, in coordination with office directors and regional administrators, to accept and manage challenges to the designation of information as CUI or challenges to the lack of such designation from internal and external stakeholders.
11. Establishes a mechanism by which authorized holders (both inside and outside the agency) can contact a designated agency representative for instructions when they receive unmarked or improperly marked information the agency designated as CUI.
12. Establishes processes and criteria, in coordination with office directors and regional administrators, for reporting and investigating instances of allegations of misuse of CUI, including adhering to sanctions for the misuse of CUI specified in laws, regulations, or policies.
13. Establishes processes, in coordination with office directors and regional administrators, for handling CUI decontrol requests.
14. Establishes a waiver process, in coordination with office directors and regional administrators, for marking waivers, and exigent circumstances waivers for any CUI

within the NRC's possession or control, unless specifically prohibited by applicable laws, regulations, or Governmentwide policies.

(a) If a waiver is granted, reinstitutes the requirements for all CUI covered by the waiver as soon as the circumstances requiring the waiver are ended.

(b) Retains a record of each waiver of CUI requirements, notifies authorized recipients and the public of the waivers, and reports the waivers to the CUI EA.

F. Controlled Unclassified Information (CUI) Program Manager (PM), OCIO

1. Manages the day-to-day operations of NRC's CUI program as directed by the CUI SAO.
2. Coordinates NRC CUI policy development and updates.
3. Organizes and oversees NRC CUI training efforts.
4. Organizes NRC's CUI self-inspection program.
5. Interfaces directly and officially with the CUI EA on CUI matters, including submission of required reports.

G. Chief Human Capital Officer (CHCO)

Jointly with the CUI SAO, provides CUI training to staff and contractors and maintains records of training completion.

H. Director, Office of Administration (ADM)

1. Ensures that all agency contracts that will involve CUI include language to ensure contractors appropriately protect CUI that is either received from the NRC or that the contractor creates or possesses for or on behalf of the NRC.
2. Establishes, reviews, approves, and provides guidance on the proper storage of CUI and on all methods for physical destruction of CUI consistent with 32 CFR Part 2002.

I. Office Directors and Regional Administrators

1. Ensure that, whenever feasible, agreements or arrangements that specify required controls for CUI are in place before sharing CUI information with a non-executive branch entity (e.g., licensee, State, or local government) that is not in a contractual arrangement with the agency.
2. Ensure that all office/regional staff, contractors, and consultant personnel under their jurisdiction complete required CUI training, acknowledge the rules of behavior, and comply with the provisions of this MD.

IV. NARA CUI EXECUTIVE AGENT (EA)

Title 32 CFR 2002.8, "Roles and responsibilities," describes the role of NARA in its capacity as the CUI EA. In summary, the CUI EA—

A. Develops and issues policy, guidance, and other materials, as needed, to implement Executive Order 13556 and the CUI Registry to establish and maintain the CUI program.

B. Consults with affected agencies, Governmentwide policy bodies, State, local, Tribal, and private sector partners, and representatives of the public on matters pertaining to CUI, as needed.

C. Establishes, convenes, and chairs the CUI Advisory Council (the Council) to address matters pertaining to the CUI program. The CUI EA consults with affected agencies to develop and document the Council's structure and procedures, and submits the details to OMB for approval.

D. Reviews and approves agency policies implementing 32 CFR Part 2002 to ensure their consistency with Executive Order 13556, 32 CFR Part 2002, and the CUI Registry.

E. Reviews, evaluates, and oversees an agency's actions to implement the CUI program, to ensure compliance with Executive Order 13556, 32 CFR Part 2002, and the CUI Registry.

F. Establishes a management and planning framework, including associated deadlines for phased implementation, based on agency compliance plans submitted pursuant to section 5(b) of Executive Order 13556, and in consultation with affected agencies and OMB.

G. Approves categories of CUI, as needed, and publishes them in the CUI Registry.

H. Maintains and updates the CUI Registry, as needed.

I. Prescribes standards, procedures, guidance, and instructions for oversight and agency self-inspection programs, including performing onsite inspections.

J. Standardizes forms and procedures to implement the CUI program.

K. Considers and resolves, as appropriate, disputes, complaints, and suggestions about the CUI program from entities in or outside the Government.

L. Reports to the President on implementation of Executive Order 13556 and the requirements of 32 CFR Part 2002. This includes publishing a report on the status of agency implementation at least biennially, or more frequently at the discretion of the CUI EA.

V. APPLICABILITY

The policy and guidance in this directive and handbook apply to all NRC employees, consultants, detailees, and to all NRC contractors.

VI. DIRECTIVE HANDBOOK

Handbook 12.6 facilitates implementation of the NRC CUI Program. The handbook includes guidance regarding administrative, technical, management, operational, and physical security measures appropriate for the protection of CUI.

VII. GUIDANCE DOCUMENTS

A. Information Disclosure

MD 3.1, “Freedom of Information Act,” pertains to NRC policy regarding the Freedom of Information Act.

MD 3.2, “Privacy Act,” pertains to NRC policy regarding the Privacy Act.

MD 3.4, “Release of Information to the Public,” pertains to the NRC policy regarding public release.

B. Protection of Classified Information

MD 12.2, “NRC Classified Information Security Program,” pertains to required protections for non-electronic classified information.

C. Cybersecurity

MD 12.5, “NRC Cybersecurity Program,” pertains to required protections for electronic processing of information.

D. Protection of Non-Electronic Safeguards Information (CUI//SP-SGI)

MD 12.7, “NRC Safeguards Information Security Program,” pertains to the designation of Controlled Unclassified Information//Specified (CUI//SP)-Safeguards Information (SGI), requirements for obtaining access to CUI//SP-SGI, and the safekeeping and storage requirements for non-electronic CUI//SP-SGI.

E. Glossary

MD 12.0, “Glossary of Security Terms,” is a listing of defined security terms used in the MD Volume 12, “Security,” series.

VIII. EXCEPTIONS

Exceptions to or deviations from this directive and handbook may be granted by the CUI SAO, except for those areas in which the responsibility or authority is vested solely with the

EDO or the Director, ADM and cannot be delegated, or for matters specifically required by law, Executive Order, or directive to be referred to other management officials. Nothing in this directive or handbook shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended.

IX. REFERENCES

Code of Federal Regulations

10 CFR Part 73, "Physical Protection of Plants and Materials."

32 CFR Part 2002, "Controlled Unclassified Information."

Executive Orders (EO)

EO 13526, "Classified National Security Information," December 29, 2009.

EO 13556, "Controlled Unclassified Information," November 4, 2010.

National Archives

NARA General Records Schedule:
https://www.archives.gov/records-mgmt/grs.

National Archives Controlled Unclassified Information Web Site (also the CUI Registry): https://www.archives.gov/cui.

CUI Registry: Limited Dissemination Markings:
https://www.archives.gov/cui/registry/limited-dissemination.

National Institutes of Standards and Technology

NIST Computer Security Division, Computer Security Resource Center:
https://csrc.nist.gov/publications/.

NIST Special Publications (SP):
http://csrc.nist.gov/publications/PubsSPs.html.

NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations."

NIST SP 800-88, "Guidelines for Media Sanitization."

NIST SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations."

NIST SP 800-172, "Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171."

Nuclear Regulatory Commission Documents

Management Directives (MD)—

MD 3.1, "Freedom of Information Act."

MD 3.2, "Privacy Act."

MD 3.4, "Release of Information to the Public."

MD Vol. 3, "Information Management," Part 2, "Records Management."

MD 5.13, "NRC International Activities, Practices, and Procedures."

MD 7.4, "Reporting Suspected Wrongdoing and Processing OIG Referrals."

MD 10.166, "Telework."

MD 12.0, "Glossary of Security Terms."

MD 12.1, "NRC Facility Security Program."

MD 12.2, "NRC Classified Information Security Program."

MD 12.3, "NRC Personnel Security Program."

MD 12.5, "NRC Cybersecurity Program."

MD 12.7, "NRC Safeguards Information Security Program."

NRC Agencywide Rules of Behavior for Authorized Computer Use (ML17194A704).

NRC CUI-STD-1000, "Controlled Unclassified Information Marking Standard" (ML20206K936).

NRC Internal Controlled Unclassified Information (CUI) Program Web site: http://drupal.nrc.gov/cui.

NRC Internal Web site: http://drupal.nrc.gov/.

NRC Public Controlled Unclassified Information (CUI) Program Web site: https://www.nrc.gov/reading-rm/cui.html.

NRC Report a Safety or Security Incident: http://drupal.nrc.gov/content/report-safety-or-security-incident.

NRC Records Disposition Schedule: https://www.nrc.gov/reading-rm/records-mgmt.html.

United States Code

Appointment of Administrative Law Judges (5 U.S.C. 3501).

Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 et seq.).

Energy Reorganization Act of 1974, as amended (42 U.S.C. 5801 et seq.).

Executive Agency (5 U.S.C. 105).

Federal Information Security Modernization Act of 2014 (FISMA) (44 U.S.C. 3551 et seq.).

Freedom of Information Act (5 U.S.C. 552).

Inspector General Act (5 U.S.C. App.).

Privacy Act (5 U.S.C. 552a).

DH 12.6	NRC CONTROLLED UNCLASSIFIED INFORMATION (CUI) PROGRAM	DT-21-12
Volume 12:	Security	
Approved by:	Daniel H. Dorman Executive Director for Operations	
Date Approved:	December 3, 2021	
Cert. Date:	N/A, for the latest version of any NRC directive or handbook, see the online MD Catalog.	
Issuing Office:	Office of the Chief Information Officer Governance & Enterprise Management Services Division	
Contact Name:	Tanya Mensah	

EXECUTIVE SUMMARY

Management Directive (MD) 12.6, "NRC Controlled Unclassified Information (CUI) Program," (formerly titled, "NRC Sensitive Unclassified Information Security Program" (SUNSI)) is revised to describe the agency Controlled Unclassified Information (CUI) program. The NRC CUI program implements 32 CFR Part 2002, "Controlled Unclassified Information" (CUI rule) to protect NRC sensitive but unclassified information from unauthorized access, use, disclosure, disruption, modification, and destruction. The CUI rule standardizes markings across all Federal agencies; therefore, SUNSI and the associated markings, such as Official Use Only, will be discontinued once CUI is implemented at the NRC.

MD 12.6 is issued in accordance with Commission direction to ensure NRC sensitive but unclassified information is appropriately protected.

TABLE OF CONTENTS

I. NRC CONTROLLED UNCLASSIFIED INFORMATION (CUI) PROGRAM

A. Introduction

1. In November 2010, the President issued Executive Order (EO) 13556, "Controlled Unclassified Information (CUI)," to "establish an open and uniform program for managing information that requires protection or dissemination controls." In the past, Federal executive branch agencies employed ad hoc, agency-specific policies, procedures, and markings to protect and control this information (such as the NRC's former Sensitive Unclassified Non-Safeguard Information (SUNSI) program), and there was no Governmentwide direction on what information should or should not be protected. Under the CUI program, only the categories and subcategories of information listed in the CUI Registry may be marked and handled as CUI. On September 14, 2016, the Information Security Oversight Office (ISOO) of the National Archives and Records Administration (NARA) issued Title 32 of the *Code of Federal Regulations* (CFR) Part 2002, "Controlled Unclassified Information."

2. Purpose and Scope

   The U.S. Nuclear Regulatory Commission (NRC) CUI program implements 32 CFR Part 2002 to protect CUI from unauthorized access, use, disclosure, disruption, modification, and destruction.

   (a) CUI is information that the Government creates or possesses (or that an entity creates or possesses for or on behalf of the Government) that is not classified information but that Federal law, regulation, or Governmentwide policy either requires or permits an agency to handle using safeguarding or dissemination controls. 32 CFR Part 2002 creates two subsets of CUI: "CUI Basic" and "CUI Specified." Authorized holders (as defined in Section I.A.2(b) of this handbook) of CUI must protect CUI in accordance with CUI Basic or CUI Specified controls, whichever applies to the information. The CUI Executive Agent (EA) at NARA maintains a Federal Governmentwide CUI Registry, which identifies all approved CUI categories and whether the information they cover is CUI Basic or CUI

Specified. The CUI Registry also provides general descriptions for each category of CUI, identifies the legal basis for controls, establishes CUI markings, and includes guidance on CUI handling procedures. The CUI Registry, as well as additional CUI guidance documents, are available at NARA's CUI Web site at https://www.archives.gov/cui.

(i) CUI Basic is the subset of CUI for which the authorizing law, regulation, or Governmentwide policy does not set out specific handling or dissemination controls or the required controls are met by the CUI Basic controls. Agencies handle CUI Basic per the uniform set of controls in 32 CFR Part 2002 and the CUI Registry. In electronic form, all CUI Basic categories are controlled at the "moderate" confidentiality level, at a minimum. In general, the confidentiality level indicates the potential impact resulting from a compromise of the confidentiality, integrity, or availability of information. As an example, the security requirements for information controlled at a "moderate" level are stronger than the security requirements for information that needs to be controlled at a "low" confidentiality level. At a minimum, NRC issued computers and systems are configured at a moderate confidentiality level. Federal direction regarding required controls for the moderate confidentiality level are provided by National Institute of Standards and Technology (NIST). Also, controlled environment requirements apply to CUI Basic to ensure that it is protected from access, overhearing, or observation by unauthorized persons (i.e., protecting screen visibility, ensuring that conversations involving CUI cannot be overheard by unauthorized individuals, and ensuring that unauthorized individuals don't have access to CUI).

(ii) CUI Specified is the subset of CUI for which the authorizing law, regulation, or Governmentwide policy contains specific handling controls that it requires or permits agencies to use that differ from those for CUI Basic. Safeguards Information (SGI) is one example of CUI Specified, because NRC regulations in 10 CFR Part 73, "Physical Protection of Plants and Materials," provide specified handling controls for that information. Because it is CUI Specified, authorized holders of SGI continue to apply the handling controls specified in NRC regulations. CUI Specified information in electronic form may be handled at higher confidentiality levels if the authorities establishing and governing the CUI Specified allow or require more specific or stringent controls. Unless otherwise stated by the authorizing law, regulation, or Governmentwide policy for the CUI Specified information, the CUI Basic controlled environment requirements apply.

(iii) The underlying law, regulation, or governmentwide policy that authorizes particular information to be CUI determines if CUI is CUI Basic or CUI Specified. NARA's CUI Registry indicates whether CUI is Basic or CUI Specified. However, as described in 32 CFR 2002.4(r), CUI Specified may have to be handled using a mix of both CUI Specified and CUI Basic controls

depending on the requirements in the authority that authorized it. As an illustrative example, if a Federal law or regulation requires that information be stored or handled in a certain way but is silent as to how that information may be destroyed, authorized holders must apply the specified storage and handling requirements to that information and the CUI Basic requirements for destruction.

(iv) CUI does not include any information that is classified under EO 13526, "Classified National Security Information," or any predecessor or successor order, or is classified under the Atomic Energy Act of 1954, as amended. CUI also does not include information that a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch entity.

(v) Uncontrolled Unclassified Information is information that is neither CUI nor classified information. By definition, Uncontrolled Unclassified Information is not considered sensitive information; however, it must still be handled in accordance with Management Directive (MD) 12.5, "NRC Cybersecurity Program," when it is in electronic form to ensure the integrity or availability of the information is not compromised. Uncontrolled Unclassified Information in isolation, in physical or electronic form, is not considered sensitive. However, the compilation of certain Uncontrolled Unclassified Information may, depending on the subject matter, elevate the Uncontrolled Unclassified Information to CUI or classified information (i.e. the "mosaic effect"). Staff should always consider the content of Uncontrolled Unclassified Information, and when warranted, consult a subject matter expert (SME) if a compilation of Uncontrolled Unclassified Information is believed to warrant a more stringent level of protection as CUI or classified information. A designation of Uncontrolled Unclassified Information does not in and of itself mean that the information is publicly releasable (see MD 3.4, "Release of Information to the Public," for more information).

(b) An authorized holder is an individual, agency, organization, or group of users that is permitted to designate or handle CUI, in accordance with 32 CFR Part 2002. Anyone, whether internal or external to the NRC, can be an authorized holder of CUI, provided that their access to CUI furthers a lawful Government purpose and is not otherwise restricted or prohibited by laws, regulations, or Governmentwide policy (see Section VII, "Controlled Unclassified Information (CUI) Access and Dissemination," of this handbook for more detailed information regarding access to and dissemination of CUI).

(c) A non-executive branch entity is a person or organization established, operated, and controlled by individual(s) acting outside the scope of any official capacity as officers, employees, or agents of the executive branch of the Federal Government. Such entities may include elements of the Legislative or Judicial

Branches of the Federal Government; State, interstate, Tribal, or local government elements; and private organizations. Non-executive branch entity, when used in this handbook, does not include foreign entities as defined in 32 CFR Part 2002, nor does it include individuals or organizations when they receive CUI information in accordance with Federal disclosure statutes, including the Freedom of Information Act (FOIA) and the Privacy Act of 1974. CUI requirements that may otherwise apply when sharing CUI with a non-executive branch entity do not apply when the NRC is required to provide CUI to that entity in accordance with Federal disclosure laws, such as the FOIA or Privacy Act. See Section VII of this handbook for more detailed information regarding the dissemination of CUI to non-executive branch entities.

B. Relationship to FOIA, Whistleblower Protection Laws, and the Privacy Act

1. The CUI program and the FOIA are distinct, serve different purposes, and are not interchangeable. The CUI program addresses the Government's own internal handling of sensitive unclassified information and its sharing of that information for official Government business purposes; it does not address whether information can or must be disclosed to the public. FOIA addresses disclosure of information to the public, both to individual members of the public and to the public at large; it does not address how agencies can or must control information when it is being used or shared for official government business purposes. There are many parallels between the CUI program and FOIA because information sensitive enough to require special controls under the CUI program will often qualify for protection, under FOIA's statutory exemptions, from FOIA's public disclosure requirements. Nonetheless, confusing one regime for the other could result in incorrect outcomes.

2. If the NRC receives a FOIA request that includes CUI within its scope, the decision to disclose or withhold CUI must be based solely on the applicability of any FOIA statutory exemptions at the time the FOIA request is made. CUI markings and designations may be informative in determining whether a record contains information that could, or must, be withheld in response to a FOIA request. However, decisions to withhold information in response to a FOIA request cannot be made simply based on CUI markings and designations. Further, even if a record marked as CUI that is responsive to a FOIA request does contain information exempt from disclosure under FOIA, FOIA would still require release of any reasonably segregable, non-exempt information in the record.

3. Relatedly, FOIA exemptions cannot be relied on as a basis for treating information as CUI. The CUI Registry—not FOIA—identifies the types of information that qualify as CUI.

4. If, in response to a FOIA request, CUI is released and placed as a publicly available record into an NRC official recordkeeping system, the information released no longer requires protection as CUI (see Handbook Section VI.D, "Decontrolling Controlled

Unclassified Information"). However, depending on the nature and sensitivity of the information, not all information that is provided to an individual FOIA requester is placed in an NRC official recordkeeping system as a publicly available record. The NRC may still control such information as CUI internally. For further information on NRC policy and procedures regarding FOIA, please see MD 3.1, "Freedom of Information Act."

5. Outside the context of FOIA, the presence or lack of CUI markings does not determine whether a document may be withheld from the public. Details are provided in MD 3.4, "Release of Information to the Public."

6. The CUI program does not change or affect existing legal protections for whistleblowers. The fact that information is designated or marked as CUI does not determine whether an individual may lawfully disclose that information under a law or other authority and does not pre-empt or otherwise affect whistleblower legal protections provided by law, regulation, EO, or directive.

7. The CUI rule does not override any of the Privacy Act's requirements. Privacy Act information, even if designated as CUI, shall still be handled in accordance with MD 3.2, "Privacy Act." When determining whether certain information must be protected under the Privacy Act, or whether the Privacy Act allows release of the information to an individual, the decision must be based on the content of the information and the Privacy Act's criteria, regardless of whether the information is designated or marked as CUI.

C. Controlled Unclassified Information (CUI) Registry

1. The CUI Registry serves as the central repository for all guidance, policy, and requirements on handling CUI, including authorized organizational index groupings and CUI categories. The CUI EA at NARA maintains the CUI Registry and the associated Web site, http://archives.gov/cui.

2. The CUI categories within the CUI Registry shall serve as exclusive designations for the CUI framework. Items can only be marked according to the categories in the CUI Registry.

3. New CUI authorities can be added to the CUI Registry, whether to expand the scope of an existing CUI category or to support establishment of a new CUI category, when an agency identifies a new or pre-existing law, regulation, or Governmentwide policy that requires or permits safeguarding or dissemination controls for an information type. NRC staff who believe that a new CUI authority should be added must contact the NRC CUI Program Manager for assistance in determining whether the information type is eligible for inclusion in the CUI Registry. Only the NRC CUI SAO may submit a request to NARA for creation of a new CUI category or the addition of a new authority to an existing CUI category. NARA is also authorized to grant, upon request of the CUI SAO, provisional approval of CUI categories for agency use

before the enactment of regulation or Governmentwide policy, if certain criteria are met. NRC staff should contact the NRC CUI Program Manager if they have questions about the need for new CUI categories or authorities for the designation of CUI.

D. Controlled Unclassified Information (CUI) Description

1. All CUI must be handled in accordance with the CUI program.
2. The CUI Registry includes citations to laws, regulations, or Governmentwide policies that form the basis for each category and notes any sanctions or penalties for misuse of each category.
3. No uncontrolled information may be labeled as CUI.
4. No classified information may be controlled within the CUI program, but some information may be both CUI and classified.

II. PERSONNEL

MD 12.6 provides the management framework for personnel associated with the NRC CUI program.

A. Management Commitment to the CUI Program

NRC management at all levels must ensure that staff and contractors understand and abide by the CUI requirements.

B. Users

All agency employees and contractors who encounter CUI are responsible for protecting and properly securing CUI, following the CUI requirements, and reporting all suspected or actual compromise of CUI (including unauthorized access to CUI) and all cases where information is inappropriately marked as CUI. This may include intentional violations or unintentional errors in safeguarding or disseminating CUI. This may also include designating or marking information as CUI when it does not qualify as CUI or inappropriately restricting access to, or dissemination of, CUI. Employees and contractors who have good faith disagreements over whether information qualifies as CUI should refer Section VIII.A, “Challenges to Designation of Information as Controlled Unclassified Information (CUI),” for additional guidance. See Section IX, “Misuse and Inadvertent Release of Information,” of this handbook, for additional guidance on reporting incidents involving CUI.

C. Personnel Screening

1. In accordance with the Federal Information Security Modernization Act of 2014 (FISMA) (44 United States Code (U.S.C.) 3551 et seq.), all NRC personnel, including

NRC employees and contractors, must successfully complete appropriate screening before being provided access to sensitive NRC information or electronic systems that contain sensitive information. This includes individuals being granted general building access, access to NRC IT systems (IT Level I or II), and/or security clearance. MD 12.3, "NRC Personnel Security Program," provides detailed information on pre-employment screening requirements for NRC job applicants and contractors, national security clearance processing, and individual information and facility/system access authorizations, as well as requirements related to visitors and foreign nationals. Because CUI is a type of sensitive information, appropriate screening, consistent with MD 12.3, must occur before NRC employees and contractors may access CUI in their capacity as NRC employees or contractors.

2. MD 12.1, "NRC Facility Security Program," provides information on the various foreign national programs at the NRC.

3. MD 5.13, "NRC International Activities, Practices, and Procedures," provides information on the foreign national program and process to be followed by the NRC to accept foreign assignees.

D. Controlled Unclassified Information (CUI) Awareness and Training

1. All NRC personnel, including employees, contractors, and detailees—

   (a) Are required to complete the CUI awareness and training sessions commensurate with their duties.

   (b) Must take initial CUI awareness training and biennial CUI training thereafter.

   (c) Who create and/or handle CUI on a regular basis must have a deeper knowledge and understanding of relevant CUI categories, the CUI Registry, associated markings, and applicable protections, dissemination, and decontrol policies and procedures, as described in this MD. These individuals must complete more indepth CUI training.

2. NRC individuals who are subject matter experts (SME) on specific information categories shall identify appropriate in-depth training content and consult with OCHCO Training and Development for the creation and maintenance of an indepth training program that provides designated staff members with an enhanced level of CUI awareness.

3. NRC organizations will identify SME who serve to ensure the organization's information is categorized appropriately.

E. Improper Release of Controlled Unclassified Information (CUI)

Any suspected or known unauthorized CUI release must be reported by the responsible office or the individual that suspects or knows of the unauthorized release, in accordance with MD 3.4, "Release of Information to the Public," and within 1 hour as a

security incident by clicking on the “Report a Safety/Security Incident” button on the NRC Internal Web site or contacting the hotline at (301) 415-6666.

III. CONTROLLED UNCLASSIFIED INFORMATION (CUI) MARKING

The NRC’s Internal CUI program Web site provides more detailed checklists, guidance, procedures, processes, standards, and templates to support the implementation of the NRC’s CUI program. CUI-STD-1000, “Controlled Unclassified Information Marking Standard,” located on the NRC’s Internal CUI program Web site is the NRC’s CUI marking standard and provides examples of how CUI marking appears within NRC documents.

A. CUI Banner Marking

1. Any document that contains CUI must include the CUI banner marking at the top of each page. The banner identifies the CUI content of the document in accordance with the CUI marking standard provided on the NRC’s Internal CUI program Web site. The marking must be the same on each page, be in bold, capitalized text, and centered on the page, when feasible. Markings must be uniformly and conspicuously applied throughout the document.

2. When a law, regulation, or Governmentwide policy requires that a specific marking be placed at the top of a document, the CUI banner may be placed directly below the other required marking. Examples at the NRC include 10 CFR 2.390, which provides specific marking instructions for persons who submit proprietary information to the NRC, and 10 CFR Part 73, which provides specific marking requirements for SGI. NRC employees applying CUI banner markings should not remove non-CUI markings that are required by law, regulation, or Governmentwide policy and must keep CUI banner markings separate from these other required markings.

3. The CUI controlled marking must be “CUI.” However, staff may encounter CUI documents that are marked by other agencies with the word “Controlled” instead of the acronym “CUI.” The use of “Controlled” in a CUI marking by another agency is permissible under the CUI rule and does not indicate improper marking. If the NRC receives a document marked by another agency with the word “Controlled” instead of the acronym “CUI,” the NRC does not need to remark the document to replace “Controlled” with “CUI.”

4. The category markings for information contained within the document are provided in alphabetized order after “CUI//” in the banner. Each category is separated from other categories using a single forward slash (/), and each category that is CUI Specified must be preceded by “SP-.” When both CUI Basic and CUI Specified are present in the document, the CUI Specified categories must appear in alphabetized order and then the CUI Basic categories should appear in alphabetized order.

5. Limited dissemination markings are provided last in the banner and are separated from the other markings using a double slash (//).

6. All documents containing CUI and generated by the NRC, must reflect the NRC as the designator of the information, and identify a point of contact, branch name, or division name within the NRC. If this designation information is not readily apparent on the face of the document (such as the presence of agency letterhead or an e-mail accompanying the document), NRC staff should place this designation information at the bottom of the first page of the document

B. Limited Dissemination Markings

1. The CUI rule allows agencies to place additional limits on the dissemination of CUI through approved limited dissemination markings. Agencies may only use limited dissemination markings that are approved by NARA and published in the CUI Registry.

2. NRC staff may use any of the limited dissemination markings that are approved and published in the CUI Registry, found at https://www.archives.gov/cui/registry/limited-dissemination. However, NRC staff may use limited dissemination controls to restrict access to CUI only if the designation serves a lawful Government purpose. NRC staff who are unsure whether a limited dissemination control is appropriate for a specific document should refer to the appropriate NRC CUI Standard, available at the NRC's Internal CUI program Web site. The appropriate NRC CUI Standard provides additional guidance to staff on the use of limited dissemination markings for specific CUI categories that NRC staff may typically encounter. Staff should direct questions to the CUI Program Manager.

3. When the NRC marks documents as CUI, the control marking must be "CUI." Staff may, however, encounter CUI documents that are marked by other agencies with the word "Controlled" instead of the acronym "CUI." The use of "Controlled" in a CUI marking by another agency is permissible under the CUI rule and does not indicate improper marking. If the NRC receives a document marked by another agency with the word "Controlled" instead of the acronym "CUI," the NRC does not need to remark the document to replace "Controlled" with "CUI."

C. Portion Marking

Portion marking specifics are provided in the CUI marking standard located on the NRC's Internal CUI program Web site.

1. Portion marking is required for any document that contains both classified national security information and CUI. Additional information regarding portion marking requirements for documents containing both classified information and CUI can be found in Section IV, "Commingled Information," of this handbook.

2. Portion marking for documents that do not contain classified information is required only for documents containing the CUI categories identified in CUI-STD-1000,

"Controlled Unclassified Information Marking Standard," on the NRC's Internal CUI program Web site.

3. CUI portion markings must be placed at the beginning of the portion (i.e., in front of the CUI paragraph) to which they apply and must be used throughout the entire document.

4. CUI portion markings must be contained within parentheses and include the following three elements:

   (a) "CUI."

   (b) CUI category markings separated from CUI control marking by a double forward slash (//) and separated from each other by a single forward slash (/). Category markings must be alphabetized with all CUI Specified categories in the portion listed in alphabetic order before all CUI Basic categories in the portion listed in alphabetic order.

   (c) Limited dissemination control markings, where appropriate, are separated from preceding CUI markings by a double forward slash (//). When including multiple limited dissemination control markings, they must be alphabetized and separated from each other by a single forward slash (/).

   Example: An NRC staff member is preparing a document that contains CUI. At the beginning of the portion (i.e., paragraph) that contains CUI, the marking would appear as:

   (CUI//CUI CATEGORY MARKING//LIMITED DISSEMINATION CONTROL)

5. When CUI portion markings are used, and a portion (i.e., paragraph) does not contain CUI or classified national security information, a "U" is placed in parentheses in front of the paragraph to indicate that the portion contains only Uncontrolled Unclassified Information.

D. Supplemental Administrative Markings

1. The CUI rule allows agencies to authorize the use of supplemental administrative markings. These markings are intended to inform the recipient of the status of a document in the agency's decisionmaking process. Specifically, supplemental administrative markings are intended to help avoid confusion over the final or non-final status of a document and maintain the integrity of an agency's decisionmaking process. Placing a supplemental administrative marking on a document does not make the document CUI, nor can a supplemental administrative marking be used as the basis for placing a safeguarding or dissemination restriction on the document. Documents containing CUI, that also warrant supplemental administrative markings, must be protected as CUI until the CUI within the document is removed or the qualifying information within the document no longer warrants the CUI designation.

2. NRC staff may use the following supplemental administrative markings, either alone or in combination, in documents that contain CUI. These are the only supplemental administrative markings permitted for use in combination with CUI markings. These markings may be included in a watermark, or in a header below the CUI banner marking. Supplemental administrative markings may never occupy the same line as the CUI banner marking.

   (a) **Draft**: This marking may be used in a document that is non-final, meaning that the document is still in the process of being developed and may be further revised before finalization.

   (b) **Predecisional/Deliberative**: This marking may be used in a document, either final or non-final, if the document is intended for the purpose of consultation, consideration, discussion, or otherwise expresses opinions, advice, or recommendations on legal or policy decisions that have not yet been made.

   Example: A member of the NRC staff is preparing a document that contains Nuclear Security-Related Information. The document will be signed by the office director and presents various options to the Commission on a matter of agency policy. Before final signature, the document may be marked "Draft" or "Pre-decisional/Deliberative" (or both), either with a watermark or in a header beneath the CUI marking (CUI//SRI). Once the document has been finalized and signed by the office director, "Draft" markings should be removed from the final document but "Predecisional/Deliberative" markings may remain. However, "Draft" markings need not be removed from draft versions of the final document that are still retained.

3. NRC employees still may place any markings, including "Draft" or "Predecisional/Deliberative," on documents that do not contain CUI, provided that—

   (a) The document is not marked as CUI on the basis of the administrative marking. Examples of prohibited markings would be "CUI – Draft" or "CUI – Predecisional."

   (b) The administrative marking does not otherwise purport to place safeguarding or dissemination controls on the document (examples of prohibited markings would be "Predecisional/Deliberative – Do Not Disseminate" or "Agency Use Only").

4. Employees are encouraged to use "Draft" and "Predecisional/Deliberative" administrative markings on all documents whenever applicable. These markings provide the holder of the document with the status of the document in the agency's decisionmaking process. The presence of such markings can alert the holder that the document may be eligible to be withheld from release in the event of a FOIA request, although placing a "Draft" or "Predecisional/Deliberative" marking on a document will not automatically make the document eligible for withholding.

E. Electronic Media Marking

1. Electronic media must be marked to alert holders to the presence of CUI stored on the device.
2. Where there is space, the CUI banner must be used to mark the electronic media.
3. Where there is not space, the electronic media must be marked using “CUI” and “NRC” or the identifier of the agency that designated the information as CUI. Some CUI Specified categories have marking requirements that exceed the minimal "CUI" marking.
4. Refer to MD 12.5 for additional information on electronic media marking.

F. Cover Sheets

CUI cover sheet GSA Standard Form (SF) 901 shall be used for documents identified in CUI-STD-1000, located on the NRC’s Internal CUI program Web site, as requiring a cover sheet. This form is available in the NRC supply room and available electronically on the NRC’s Internal CUI program Web site.

G. Form Marking

Forms that will contain CUI when filled in must include “When Filled In” under the CUI banner.

H. Transmittal Documents

1. When a transmittal document (e.g., cover memorandum) accompanies CUI, it must indicate that CUI is enclosed or attached. Staff should not include CUI within the body of the transmittal document, unless necessary. The notice on the transmittal document must be conspicuous, on its face, with the following message: “When enclosure is removed, this document becomes Uncontrolled Unclassified Information.”
2. If CUI is contained within the body of the transmittal document, the transmittal document must be marked as a CUI document. CUI marking requirements are located on the NRC’s Internal CUI program Web site.

I. Packing, Shipping, and Mailing

1. Envelopes or packages that contain CUI should be marked to indicate that they are intended for the recipient only and should not be forwarded. Envelope and packing requirements may differ for CUI Specified and those requirements are provided in the protection standard associated with the CUI Specified information type, as described in Section VI of this handbook.
2. No CUI markings shall be placed on the outside of an envelope or package.

3. Use in-transit automated tracking and accountability tools where possible when shipping or mailing CUI.

J. Electronic Controlled Unclassified Information (CUI)

Electronic processing of CUI must comply with MD 12.5.

IV. COMMINGLED INFORMATION

When CUI is included in a document that contains any type of National Security Information (NSI), that document is referred to as "commingled." MD 12.2, "NRC Classified Information Security Program," provides marking and protection requirements for non-electronic classified information and MD 12.5 provides protection requirements for electronic classified information.

A. Commingled Documents

1. Commingled documents are subject to the requirements of both the CUI and NSI Programs.
2. CUI and NSI must be placed in separate portions of the document to the greatest extent possible to allow for maximum information sharing.
3. All portions must be marked to ensure that authorized holders can distinguish CUI portions from those containing just NSI and/or Uncontrolled Unclassified Information. Documents containing Restricted Data (RD) and/or Formerly Restricted Data (FRD) are not portion marked under any circumstance, unless directed in writing by the designating agency (e.g., Department of Energy, etc.) to be portion marked.
4. The decontrolling provisions for CUI apply only to portions marked as CUI. NSI portions remain subject to their own downgrading or declassification requirements.
5. Any applicable limited dissemination control markings must appear in the CUI banner.
6. When used, banner line elements must appear in the following order:
   (a) U.S. Classification,
   (b) Non-U.S. Classification,
   (c) Joint Classification,
   (d) Sensitive Compartmented Information (SCI) Control System,
   (e) Special Access Program (SAP),
   (f) Atomic Energy Act Information (i.e., Restricted Data (RD) or Formerly Restricted Data (FRD)),

(g) Foreign Government Information,

(h) CUI Control Marking,

(i) CUI Category Marking, and

(j) Dissemination Control Marking.

B. Commingled Document Portion Marking

1. Commingling in the same paragraph is not recommended.
2. Where paragraphs contain CUI and NSI commingled, portion marking elements follow the same order as the banner marking.
3. Every portion must be appropriately marked; with the exception of documents that are marked as containing RD and/or FRD. (See Section IV.A.3 of this handbook for details).
4. Limited dissemination control markings must appear in all portions to which they apply.

V. LEGACY DOCUMENTS

A. Legacy information is unclassified information that an agency marked or restricted from access or dissemination in some way, or otherwise controlled, before the CUI program. Any NRC documents that were marked or restricted from access in some way, or otherwise controlled before the implementation of the NRC's CUI program are legacy documents. Specifically, NRC documents controlled in accordance with the NRC's SUNSI policy would be considered legacy documents.

B. In accordance with the CUI Rule and current NARA guidance, the NRC CUI Senior Agency Official (SAO) determined that it would be excessively burdensome for the agency to re-mark NRC legacy information. Therefore, the NRC will not re-mark legacy documents that qualify as CUI unless a legacy document is re-used for an agency purpose or shared with others outside of the agency. If the legacy document containing CUI is re-used, or if it is being sent outside the agency, the document must first be appropriately marked as CUI. In addition, if portions of a legacy document that contain CUI are reused in some way (e.g., incorporated into a new document), or if a legacy document is revised and the revised version contains CUI, the new/revised document must be appropriately marked as CUI.

C. The NRC CUI SAO will provide written notification in an NRC agency announcement to communicate the implementation date of the NRC's CUI program.

D. The NRC CUI SAO will also report in its annual reports to ISOO that the SAO has issued a legacy markings waiver.

VI. PROTECTING CONTROLLED UNCLASSIFIED INFORMATION (CUI)

NRC CUI standards provide specific information associated with protecting CUI categories. The standards on the NRC's Internal CUI program Web site provide detailed protection requirements for all CUI at the basic level. NRC protection standards for each type of CUI designated in the CUI Registry as CUI Specified that NRC typically encounters also are provided on the NRC's Internal CUI program Web site. Staff encountering a type of CUI Specified information for which a protection standard has not been provided on the NRC's Internal CUI program Web site should contact the CUI Program Manager for direction.

A. General Protection

1. CUI, regardless of its form, shall be protected at all times in a manner that minimizes the risk of unauthorized disclosure while allowing for access by authorized holders.
2. Authorized holders of CUI must comply with applicable protection requirements in accordance with 32 *Code of Federal Regulations* (CFR) Part 2002, applicable laws, regulations, Governmentwide policies, all applicable guidance published in the CUI Registry, and this MD.
3. NRC internal use of protection measures that are more stringent than those required by the CUI Registry (such as those for classified information) are also acceptable for CUI. If the information is being shared or disseminated outside the NRC, such additional measures may not be required of the receiving organization. The only exception is that agencies may enter into agreements or arrangements with external parties that require those parties to protect CUI Basic information shared by the agency at above the moderate confidentiality impact level.
4. When it is impractical to individually mark CUI due to quantity or nature of the information, materials that would otherwise have an identical CUI marking may be marked in the aggregate using that CUI marking instead of marking each individual item of information.
5. Employees and contractors must maintain a clean desk whenever CUI is unattended (i.e., not in use or under observation) by storing CUI in a desk drawer, cabinet, or container, except as authorized in an area approved by DFS, ADM. Individuals would consider CUI to be unattended any time they are not in the same cubicle or office as the CUI. The requirements to store CUI in either a locked or unlocked drawer, cabinet, or container vary based upon the standards of protection associated with each CUI category. The majority of CUI expected to be handled at the NRC requires storage in **locked** drawers, cabinets, or another ADM-approved storage location or area. Refer to the NRC CUI Internal Web site to determine if the CUI you are handling requires locked or unlocked storage.
6. If an authorized holder is outside of the office environment (e.g., teleworking, traveling), extra care must be taken to ensure that CUI is not accessible to

individuals who are not authorized holders. Authorized holders must protect CUI from visual inspection by unauthorized persons while it is being used and must secure the CUI in a locked location that is not accessible by individuals who are not authorized holders when not in use. For additional guidance on the NRC's telework policy, refer to MD 10.166, "Telework."

B. Protection Standards

1. Users must protect CUI using one of two types of standards, CUI Basic or CUI Specified.
2. CUI Basic standards are the default set of controls for CUI.
3. CUI Specified refers to CUI for which the supporting law, regulation, and/or Governmentwide policy requires specific protection measures that are more stringent than, or otherwise differ from, those required for CUI Basic. Agencies are not permitted to mark a CUI Basic document as CUI Specified to impose more stringent protection measures. Only CUI designated in the CUI Registry as CUI Specified may have these more stringent protection measures applied.

C. Protection Practices

1. Only authorized holders shall have access to CUI.
2. All CUI must be protected from access, overhearing, or observation by unauthorized persons. In open office environments, CUI holders must be careful, with respect to persons not authorized to access the information, to protect—
   (a) CUI documents from view,
   (b) CUI-related discussions from being overheard, and
   (c) CUI displayed on a computer screen from being seen.
3. Authorized holders of CUI are encouraged to find a private area for discussions involving CUI.
4. CUI in hardcopy must be kept under direct control of an authorized holder or stored in a desk drawer, cabinet, or ADM-approved storage container or area to protect the CUI from unauthorized access or observation when not in use. Refer to the NRC CUI Internal Web site to determine if the CUI you are handling requires locked or unlocked storage when left unattended.
5. CUI documents must not be unattended in an open environment, such as on a shared printer or fax machine where unauthorized people can have access to the information. Staff may use a secure method of printing (e.g., Secure Print, etc.) to ensure that CUI documents are only printed after they insert their PIV card into the

machine. When security incidents involve unprotected CUI, the person or persons that discover the information should—

(a) Immediately take possession of it and not read the material,

(b) Notify their immediate supervisor or guard force member,

(c) Take steps to protect it from unauthorized disclosure, and

(d) Report the discovery of that information as described in Section II.E of this handbook.

6. If a CUI document is discovered on a public Web site or other media that is publicly available, personnel should report the discovery of that information using one of the methods described in Section II.E of this handbook.

7. Reproduction of CUI (copying, scanning, printing, electronic duplication) is allowed if in the furtherance of a lawful Government purpose. See MD 12.5, "NRC Cybersecurity Program," for electronic processing requirements.

8. Authorized interoffice or interagency hardcopy mail systems and electronic systems may be used to transport/transmit CUI. Section VII of this handbook provides CUI dissemination methods, and MD 12.5 provides electronic processing requirements.

9. CUI holders must have a reasonable expectation that all persons involved in discussions that include CUI are authorized to receive the CUI (i.e., that they all have a lawful Government purpose for receiving the CUI and no law, regulation, or government-wide policy governing the CUI prohibits it) before discussing the information with them. Information regarding appropriate protection of discussions using electronic methods (e.g., using voicemail systems, virtual meeting rooms, telepresence systems, video conferencing, or other electronic means of sharing of sharing) is provided in MD 12.5.

10. CUI holders must properly restrict access to CUI information, including within agency systems such as ADAMS, to the appropriate individuals with a lawful Government purpose.

11. Electronic processing of CUI shall be performed in accordance with MD 12.5.

D. Decontrolling Controlled Unclassified Information (CUI)

1. Decontrolling CUI relieves authorized holders from requirements to handle the information under the CUI program but does not constitute authorization for public release.

2. CUI may be decontrolled as soon as practicable when—

(a) Laws, regulations, or Governmentwide policies no longer require CUI controls;

(b) A determination to decontrol the information is made by the designating agency in response to a request for decontrol by an authorized holder;

(c) The information has been properly placed into an NRC official recordkeeping system as a publicly available record in accordance with agency policy governing release of information (see MD 3.1 and MD 3.4);

(d) Any declassification action occurs under EO 13526, “Classified National Security Information,” or any predecessor or successor order, as long as the information appropriately qualifies for decontrol as CUI; or

(e) When the designating agency has included with the CUI a specific predetermined decontrolling date or event and the authorized holder has verified that the predetermined event or date has occurred.

3. Only authorized holders may decontrol CUI, in conjunction with the designating agency.

4. If CUI markings still remain on decontrolled CUI, the authorized holder must clearly indicate, when restating, paraphrasing, re-using, or releasing it to the public, that the information is no longer controlled as CUI (e.g., strike-through of CUI markings).

5. Once decontrolled, any public release of information that was formerly CUI must be in accordance with applicable laws and NRC policies on the public release of information. MD 3.4 provides details on public release.

6. Authorized holders may request that a designating agency decontrol certain CUI. If an authorized holder publicly releases CUI in accordance with the designating agency’s authorized procedures, the release constitutes decontrol of the information.

7. Unauthorized disclosure of CUI does not constitute decontrol. CUI must not be decontrolled solely due to an instance of unauthorized disclosure. Proper procedures must still be followed for decontrolling and reporting possible misuse.

8. When laws, regulations, or Governmentwide policies require specific decontrol procedures, authorized holders must follow such requirements.

E. Destroying CUI

CUI destruction must render the information, including in electronic form, unreadable, indecipherable, and irrecoverable.

1. CUI may be destroyed when—

(a) The information is no longer needed and

(b) NRC records disposition schedules no longer require retention of the records. For more information, refer to the NRC Records Disposition Schedule

(https://www.nrc.gov/reading-rm/records-mgmt.html) and NARA General Records Schedule (https://www.archives.gov/records-mgmt/grs).

2. An ADM-approved destruction method must be used to destroy non-electronic CUI (i.e., shredder or disintegrator approved or provided by ADM for use by NRC employees, contractors, and detailees).

3. MD 12.5 provides information on electronic information destruction.

4. To minimize the challenges associated with the destruction of CUI for employees who telework, all NRC employees are encouraged to work electronically while teleworking. Electronic access must be through a Government-furnished computer authorized to process the specific type of CUI, within an application authorized to remotely process the information (e.g., the NRC CITRIX application, Government laptop using Virtual Private Networking), or NRC-authorized BYOD device container. ADM-approved shedders are not available by request for employees who telework. Employees approved for telework need to make arrangements in advance to ensure that any hard copy CUI that needs to be destroyed is shredded using ADM-approved shredders located within NRC headquarters complex, NRC regional offices, and resident offices. Employees who work remotely full-time will need to have an approved telework plan that covers the procedures for the proper storage and destruction of CUI material. If the employee needs to shred CUI while teleworking, the employee shall secure a personal shredder to reduce paper documents to shards measuring 1 millimeter by 5 millimeters, or less, per the requirements of NIST 800-88, “Guidelines for Media Sanitization.” Questions about specific shredders can be directed to ADM/DFS/SMOB.

F. Transferring records

1. When feasible, users must decontrol records containing CUI before transferring them to NARA. When records cannot be decontrolled before transferring them to NARA, users should work with the local Records Management representative for proper handling. NARA regulations (32 CFR 2002.34) require the use of a specific transfer request form in the event the NRC transfers records that are to remain controlled as CUI after transfer.

2. Records transfer must be performed in accordance with MDs in Vol. 3, “Information Management,” Part 2, “Records Management.”

VII. CONTROLLED UNCLASSIFIED INFORMATION (CUI) ACCESS AND DISSEMINATION

A. Access and Dissemination

The NRC and all agencies in the executive branch are encouraged to disseminate and permit access to CUI when doing so is consistent with all applicable CUI requirements

and policies, and the authorized holder reasonably expects that the intended recipients are authorized to receive the CUI and have a basic understanding of how to handle it. The CUI Rule states that agencies should enter into written agreements or arrangements, whenever feasible, before disseminating CUI to any non-executive branch entity. Such an agreement or arrangement may take any form, including, but not limited to, contracts, grants, licenses, certificates, memoranda of agreement/arrangement or understanding, and information-sharing agreements or arrangements. Whatever vehicle is used to establish it, the agreement or arrangement must, at a minimum, require compliance with CUI EO requirements, 32 CFR Part 2002, and the CUI Registry. General principles regarding CUI access and dissemination controls include the following:

1. The NRC may not impose controls that unlawfully or improperly restrict access to CUI.
2. When CUI Specified access and dissemination controls apply to particular CUI (for example, in the case of SGI, or personally identifiable information), any access to and dissemination of the CUI must comply with those specified requirements. As discussed previously, the CUI program does not override any more stringent information controls specified in laws, regulations, or Governmentwide policies.
3. Unclassified sensitive information shall only be controlled through the CUI Program.
4. Individuals may disseminate and permit access to CUI in accordance with the specific laws shown in the CUI Registry if it furthers a lawful Government purpose and is not otherwise prohibited by law.
5. Before disseminating CUI, authorized holders must appropriately mark CUI according to this MD.
6. When the NRC intends to share CUI with a non-executive branch entity, the NRC should enter into a written agreement or arrangement with that entity whenever feasible. At a minimum, such agreements or arrangements must specify that—
   (a) The non-executive branch entity must handle CUI received from the NRC in accordance with EO 13556, 32 CFR Part 2002, and the CUI Registry.
   (b) Non-executive branch entities with electronic CUI received from the NRC must protect that CUI in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171, “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations,” at a minimum on non-Federal information systems. This NIST publication is accessible through the NIST Computer Security Division, Computer Security Resource Center Web site, at https://csrc.nist.gov/publications/.
   (c) Misuse of CUI is subject to penalties established in applicable laws, regulations, or Governmentwide policies. The non-executive branch entity must report any

non-compliance with handling requirements to the appropriate person specified in Section IX, "Misuse and Inadvertent Release of Information," of this handbook.

7. When a written agreement is not feasible but the NRC's mission requires that it disseminate CUI to the non-executive branch entity, an NRC authorized holder may disseminate CUI even in the absence of a written agreement, but the authorized holder must communicate to the recipient that the Government strongly encourages the non-executive branch entity to protect CUI in accordance with EO 13556, 32 CFR Part 2002, and the CUI Registry, and that such protection should accompany the CUI if the entity disseminates it further.

8. When entering into agreements with a foreign entity, including individual foreign assignees, the CUI Rule requires that the NRC encourage the entity to protect CUI in accordance with EO 13556, 32 CFR Part 2002, and the CUI Registry, but the CUI Rule allows agencies to use their judgment regarding what and how much to communicate to foreign entities, keeping in mind the ultimate goal of safeguarding CUI.

9. A written agreement is not needed when sharing CUI with the following entities:

   (a) Congress, or any committee, subcommittee, joint committee, joint subcommittee, or office thereof;

   (b) The Comptroller General, while performing duties of the Government Accountability Office;

   (c) Individuals or entities when releasing information in accordance with a FOIA or Privacy Act request;

   (d) A court of competent jurisdiction, or any individual or entity when directed by an order of a court of competent jurisdiction or a Federal administrative law judge (ALJ) appointed under 5 U.S.C. 3501; or

   (e) The originator of the CUI.

10. CUI agreements/arrangements will not be used in NRC adjudicatory proceedings because decisions on litigant access to CUI are made by the proceeding's presiding officer and the terms are established by protective order.

11. Authorized holders of CUI Specified may disseminate and allow access as permitted by the authorizing laws, regulations, or Governmentwide policies applicable to the information. The NRC CUI standard associated with the information provides specific requirements.

12. In the absence of specific dissemination restrictions in the applicable laws, regulations, or Governmentwide policies, CUI Specified may be disseminated the same as CUI Basic.

13. Only the approved controls that limit to whom CUI may be disseminated may be used and only if they serve a lawful Government purpose, or are required by law, regulation, or Governmentwide policy. If there is significant doubt about whether it is appropriate to use a limited dissemination control, contact the NRC CUI Program Manager for guidance.

B. CUI Dissemination Methods

1. Access to CUI should be limited to only those individuals authorized to handle it.
2. When sending CUI by courier, mark "signature required" on the documents to create a paper trail in the event items are misplaced or lost. The U.S. Postal Service or any commercial delivery service may be used to transport CUI to another organization.
3. Electronic dissemination must be in accordance with MD 12.5.

VIII. OTHER CONSIDERATIONS

A. Challenges to Designation of Information as Controlled Unclassified Information (CUI)

1. Authorized holders of CUI who, in good faith, believe that its designation as CUI is improper or incorrect, or who believe they have received unmarked CUI, should submit a CUI Challenge Request form to the NRC CUI SAO. The form is available on the NRC's CUI public Web site: https://www.nrc.gov/reading-rm/cui.html.
2. The CUI challenge process is not used for determining the CUI status of information associated with ongoing Government litigation.
3. The CUI SAO accepts and manages challenges to CUI status.
   (a) The CUI SAO ensures that both internal and external challengers have the option of bringing the challenge anonymously, and that challengers are not subject to retaliation.
   (b) Until the challenge is resolved, all authorized holders must continue to protect and disseminate the challenged CUI at the control level indicated in the markings. The control level indicates the protection and dissemination requirements associated with the information.
   (c) If a challenging party disagrees with the response to a challenge, that party may use the dispute resolution procedures described in 32 CFR Part 2002.
   (d) Additional guidance on the NRC's challenge process is provided on the NRC's Internal CUI program Web site.

B. Waivers of CUI Requirements

In urgent circumstances, the CUI SAO may waive the requirements of the CUI policy or the CUI Registry for any CUI within NRC's possession or control, unless specifically prohibited by applicable laws, regulations, or Governmentwide policies. Waivers are requested by contacting the CUI SAO at cui@nrc.gov and using the template provided on the NRC's Internal CUI Program Web site. Additional guidance on the NRC's Waiver Process is on the NRC's Internal CUI program Web site.

IX. MISUSE AND INADVERTENT RELEASE OF INFORMATION

The CUI SAO is the contact point for the CUI EA when the EA receives reports of misuse of CUI by the NRC or from within the NRC.

A. Reporting Misuse or Inadvertent Release of Information

All employees and contractors shall report suspected or confirmed misuse of CUI, including marking information as CUI that is not authorized to be CUI, inadvertent release, mishandling, improper storage, or improper access, to the CUI SAO (through the NRC Report a Safety or Security Incident process) within 1 hour. As described in Section II.B, of this handbook, this may include intentional violations or unintentional errors in safeguarding or disseminating CUI. This may also include designating or marking information as CUI when it does not qualify as CUI or inappropriately restricting access to, or dissemination of CUI. Employees and contractors who have good faith disagreements over whether information qualifies as CUI should refer Section VIII.A, "Challenges to Designation of Information as Controlled Unclassified information (CUI)," for additional guidance.

B. Consequences of Non-Compliance

1. Misuse or failure to comply with CUI requirements may result in administrative action, or may result in sanctions that are established by the governing law, regulation, or Governmentwide policies for the CUI at issue, including but not limited to the following:

   (a) Removal of CUI access for a specific period of time,

   (b) Discipline up to and including removal from the Federal service, and

   (c) Prosecution under applicable law.

2. Allegations of violation/misconduct must be reported to the Office of the Inspector General (OIG) in accordance with MD 7.4, "Reporting Suspected Wrongdoing and Processing OIG Referrals."

X. SELF INSPECTION PROGRAM

The self-inspection program must include a periodic review and assessment of the CUI program, at least annually. CUI self-inspections are conducted under the authority of the CUI SAO. Additional guidance on the NRC's Self-Inspection Program is on the NRC's Internal CUI program Web site.

A. Purpose

1. The purpose of the self-inspection program is to evaluate program effectiveness, measure the level of compliance, monitor the progress of the CUI program implementation, and incorporate lessons learned to improve the program.
2. The CUI SAO implements a CUI self-inspection program that includes—
   (a) Self-inspection methods, reviews, and assessments that serve to evaluate program effectiveness, measure the level of compliance, and monitor the progress of CUI implementation;
   (b) Templates for documenting self-inspections and recording findings;
   (c) Procedures for integrating lessons learned and best practices arising from reviews and assessments into operational policies, procedures, and training;
   (d) A process for resolving deficiencies and taking corrective actions in an accountable manner; and
   (e) Analysis and conclusions from the self-inspection program, documented on an annual basis and as requested by the CUI EA.

B. Frequency

CUI self-inspections are conducted at least annually.

C. Inspection Process

1. CUI program self-inspections are performed and reported in accordance with guidance provided on the NRC's Internal CUI program Web site.
2. The self-inspection results and any recommendations are discussed with management personnel of the inspected organization and alignment between the CUI SAO and the inspected organization is sought before the final report is completed.
3. The findings and recommendations from the self-inspection are furnished to the appropriate office no later than 30 calendar days after a self-inspection is completed.

D. Corrective Action Program

1. NRC offices must take prompt action to ensure that necessary corrective measures are implemented based on recommendations contained in the report.
2. NRC offices must provide the CUI SAO with written confirmation, by a memo, that the necessary corrective measures have been taken within 30 calendar days after receiving the self-inspection report or, in the event corrective measures have not been implemented within 30 calendar days, a written explanation for the delay.

XI. ACRONYMS

ADM	Office of Administration
ALJs	Administrative Law Judges
CFR	*Code of Federal Regulations*
CIO	Chief Information Officer
CNSI	Classified National Security Information
CUI	Controlled Unclassified Information
CUI EA	CUI Executive Agent NARA
CUI//SP	The category marking to indicate the category is CUI Specified
DH	Directive Handbook
EA	Executive Agent
EDO	Executive Director for Operations
EO	Executive Order
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
ISOO	Information Security Oversight Office
MD	Management Directive
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OCHCO	Office of the Chief Human Capital Officer

OCIO	Office of the Chief Information Officer
OGC	Office of the General Counsel
OIG	Office of the Inspector General
SAO	Senior Agency Official for CUI
SAP	Special Access Program
SCI	Sensitive Compartmented Information
SGI	Safeguards Information
SP when not part of the banner marking or portion marking	Special Publication
SME	Subject Matter Expert
SUNSI	Sensitive Unclassified Non-Safeguards Information
USC	United States Code