



NRC Controlled Unclassified Information (CUI) Public Meeting

Thursday, March 5, 2020
NRC Three White Flint North
11601 Landsdown Street
1C03 & 1C05
2-4 pm EDT

Purpose

To continue discussions between the NRC staff and industry representatives on issues related to the NRC's plans to implement a Controlled Unclassified Information (CUI) program.

Agenda

- NRC Implementation Plan
 - Questions & Comments
- Nuclear Energy Institute (NEI) Implementation Plan
 - Questions & Comments
- Meeting Conclusion

What is CUI?

- An information security reform that standardizes the way the Federal government handles information that is not classified or Restricted Data but requires protection.
- Replaces more than one hundred different agency policies and associated markings with one shared policy (CUI) and standardized markings for Federal executive branch agencies.
- Directly applies to executive branch agencies that designate or handle CUI, and indirectly applies through written agreements or arrangements to non-executive branch recipients* of CUI.

**Non-executive branch 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 does not include foreign entities, nor does it include individuals or organizations when they receive CUI information pursuant to Federal disclosure laws, including the Freedom of Information Act (FOIA) and the Privacy Act of 1974. See § 2002.4(gg).*

CUI and Public Access to NRC Information

- The CUI program:
 - Addresses how executive branch agencies handle and share information for agency business purposes.
 - Does not affect public rights to information under the Freedom of Information Act or the Privacy Act.
 - Does not require agencies to change their policies on public release of information to the general public.

Requirements For Agencies When Sharing CUI

In summary, 32 C.F.R. § 2002.16(a)(5)(i) states that:

- Prior to disseminating or sharing CUI with non-executive branch entities, agencies should, "whenever feasible," enter into written agreements or arrangements in which the recipient agrees to protect the information in accordance with the CUI Rule; 32 CFR 2002 "Controlled Unclassified Information.
- 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.
- If an agreement with a particular non-executive branch entity is not feasible, but the agency's mission requires it to disseminate CUI to that entity, the agency must strongly encourage the recipient to protect CUI in accordance with the CUI Rule.

Non-Executive Branch Entities (Handling of CUI)

- CUI includes only information the government creates or possesses, or that an entity creates or possess on behalf of the government.
- Non-executive branch entities will only have to apply CUI controls to information received from the Federal government pursuant to a written agreement or arrangement.
 - The NRC has not yet decided the nature and type of these agreements/arrangements.
- Once the NRC transitions to CUI, “Official Use Only,” designations will no longer be used.
 - In general, the majority of sensitive unclassified information currently shared by the NRC with non-executive branch entities as “Official Use Only,” would qualify as CUI and be marked with CUI compliant markings.
- The CUI rule does not supersede or replace other Laws, Regulations, or government-wide policies, which may impose their own control requirements (e.g., 10 CFR Part 73, “Physical Protection of Plants and Materials,” controls for Safeguards Information (SGI)).
- Non-executive branch entities will continue to comply with the markings specified in NRC Regulations. Examples include:
 - 10 CFR 2.390, “Public inspections, exemptions, requests for withholding”
 - 10 CFR Part 73 "Physical Protection of Plants and Materials"

NIST Special Publication (SP) 800-171

NIST Special Publication 800-171
Revision 2

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

RON ROSS
VICTORIA PILLITTERI
KELLEY DEMPSEY
MARK RIDDLE
GARY GUISSANIE

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-171r2>

C O M P U T E R S E C U R I T Y

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

- The National Archives and Records Administration (NARA) CUI rule identifies National Institute of Standards and Technology (NIST) SP 800-171 as containing the security requirements for protecting CUI's confidentiality on non-Federal information systems.
- The primary goal of NIST SP 800-171 is to protect the confidentiality of CUI and to reduce the risk of data breaches that involve CUI that resides on a non-Federal information system.
- Agencies must prescribe, at a minimum, the requirements of NIST SP 800-171 when sharing electronic CUI with non-executive branch entities that are not operating an information system on behalf of the agency.
- In February 2020, NIST SP 800-171, Revision 2, was published.
 - It provides minor editorial changes in Chapters One and Two, and in the Glossary, Acronyms, and References appendices.
 - There are no changes to the basic and derived security requirements in Chapter Three.
 - Reference: <https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final>

NRC Transition Goals

- CUI will:
 - Replace the NRC's current Sensitive Unclassified Non-Safeguards Information (SUNSI) program.
 - Include Safeguards Information (SGI) and SGI-Modified Handling.

During the transition to the CUI program, all elements of the NRC's existing Sensitive Unclassified Non-Safeguards Information (SUNSI) program will remain in place. If NRC employees or contractors receive CUI before the implementation of the CUI Program at the agency, they will follow current NRC guidance to protect sensitive information.

NRC CUI Key Implementation Tasks ([SECY-18-0035](#)*)

Key Tasks

- Publish NRC's CUI policy statement ([SRM-SECY-18-0097](#)*)
- Proceed with a CUI rulemaking ([SRM-COMSECY-18-0022](#)*)
- Publish Management Directive 12.6, "NRC Controlled Unclassified Information (CUI) Program"
- Develop CUI training for NRC staff and contractors
- Update NRC internal guidance and office procedures
- Establish written agreements or arrangements
- Deploy CUI training for NRC staff and contractors
- Inform the staff and external stakeholders of the NRC's milestones to transition to CUI

NRC CUI Estimated Timeline

- The NRC is planning to transition to CUI in December of 2021 (*this date is an estimate that is subject to change*).
- Potential delays in the NRC's CUI implementation date may occur as a result of our efforts to:
 - Evaluate different options to comply with the CUI Rule requirements.
 - Minimize the impact of the transition, where feasible, on NRC staff and stakeholders.

**References are available on the NRC Public Website: <https://www.nrc.gov/reading-rm/doc-collections/commission/>*

NRC Communication with Non-Executive Branch Entities

- NRC CUI Public Meeting on July 25, 2019
 - NRC Public Meeting Summary dated September 5, 2019
 - ADAMS Accession Number: [ML19211B785](#)
- NRC Regulatory Issues Task Force Public Meetings
- NRC Monthly Status Call with the Agreement States
- CUI Public Website (<https://www.nrc.gov/reading-rm/cui.html>)
 - Provides general information on the NRC's transition plans
 - Informs NRC stakeholders of any public meetings
 - Provides contact information for the NRC CUI Senior Agency Official

Issues Under NRC CUI Working Group Evaluation

- How does the NRC plan to establish written agreements or arrangements with non-executive branch entities?
- How does the NRC plan to share CUI with non-executive branch entities?
- What type of documents does the NRC expect to share with non-executive branch entities that may contain CUI?
- Can a non-executive branch entity share CUI they've received from an agency with a third party without a written agreement?
- Will non-executive branch entities be required to handle NRC documents that contain their information as CUI?
- Does the NRC plan to inspect non-executive branch entities to ensure that they are appropriately handling CUI in accordance with the CUI Rule and NIST SP 800-171?

Establishing Written Agreements or Arrangements

- Requirement
 - 32 C.F.R. § 2002.16(a)(5)(i)
- CUI Policy and Guidance (<https://www.archives.gov/cui/registry/policy-guidance>)
 - [NARA CUI Notice 2018-01](#), “Guidance for Drafting Agreements with Non-Executive Branch Entities involving CUI”
 - Draft NARA CUI Notice 2019-0X. “Non-Disclosure Agreement Template for Controlled Unclassified Information (CUI)”
 - ADAMS Accession Number [ML20050E290](#)
- NRC CUI Working Group Path Forward
 - Review the final NARA CUI standard Non-Disclosure Agreement (NDA) once published.
 - Hold further discussions with NRC external stakeholders to gain alignment on the format, template, and timing.
 - Continue to coordinate with NARA and other agencies to focus on developing a standard multi-agency agreement with external parties.

Sharing CUI With Non-Executive Branch Entities

- Develop an online NRC Portal
 - The NRC's preference is for users to view the document containing CUI only, so that the user doesn't have to take possession of the document on a non-Federal information system.
 - NRC external stakeholders provided initial feedback that they would need an option to download documents.
- Incorporate a written agreement as terms and conditions that have to be accepted ("click and sign") before the recipient can access CUI documents that are disseminated by the NRC.
- NRC CUI Working Group Path Forward
 - Continue to explore options for sharing CUI with non-executive branch entities.

General Path Forward to Establish Written Agreements or Arrangements

Task	Status
Identify NRC Stakeholders (Licensees, Agreement States, Applicants, Vendors, Owners Groups, Contractors, etc.)	In progress
Awareness Communication and Gather Feedback	In progress
Develop General Agreement *	TBD
Share General Agreement with Stakeholders	TBD
Edit Agreement - Case by Case	TBD
Sign Agreement Prior to the NRC's CUI Implementation Date	TBD

**Alternative approaches may need to be considered by the NRC to establish written agreements or arrangements with specific groups of NRC external stakeholders.*

Examples of NRC Documents That May Transmit CUI

NRC documents that may contain CUI include, but are not limited to, the following:

- Non-public information shared with licensees, applicants, Agreement States, nuclear suppliers, U.S. national labs, international agencies.
- Documents pertaining to proprietary applications
 - License Amendment Requests
 - Topical Reports
 - Some Relief Requests and License Renewal
 - Requests for additional information (RAIs)
 - Draft guidance documents
- NRC-generated reports (Research/Technical Report)
- Unredacted Updated Final Safety Analysis Reports
- Inspection Reports
- Allegations
- Investigations
- Contracting and budgeting information
- Licensee financial information (e.g., RAIs, Safety Evaluations)
- Decommissioning Trust fund documents
- Reactor operator exam records, questions, medical or other internal records
- Generic Communications (Security Advisories, Information Assessment Team Advisories, and some Regulatory Issue Summaries)
- Security-Related Inspection Procedures
- Documents containing CUI shared with petitioners/intervenors, applicants, and licensees in the course of adjudicatory proceedings

Handling of NRC CUI Documents

- Potential Scenarios
 - The NRC is providing a document that qualifies as CUI to a non-executive branch entity, but the document does not include any information received from a non-executive branch entity.
 - Examples: NRC Research Reports/Technical Reports, Security Advisories, Information Assessment Team Advisories
 - The NRC is providing a document that qualifies as CUI to a non-executive branch entity, and the document includes information that was provided by the recipient.
 - Examples: NRC Safety Evaluations, Requests For Additional Information, Inspection Reports
- NRC CUI Working Group Considerations
 - Identify in the transmittal letter of the document if the recipient is required to handle the document as CUI, in accordance with their written agreement.
- NRC CUI Working Group Path Forward
 - Hold further discussions to further consider scenarios within the NRC CUI Working Group and Steering Committee.

Third-Party Sharing

- Scenario: A non-executive branch entity receives a document that's marked as CUI from the NRC and needs to share it with a third party (e.g., local emergency responders or law enforcement, other non-executive branch entities, etc.).
- Question: Does the recipient need to establish a written agreement with the third party in order to share the information?
- NRC CUI Working Group Path Forward
 - Unless the NRC applies a limited dissemination marking to the document, or otherwise restricts dissemination in the written agreement, the recipient would be able to share the CUI document with a third party who has a lawful government purpose to the information.
 - CUI markings would remain on the document when shared by the recipient to ensure that the third-party is aware of the CUI status and the need to protect the information in accordance with the CUI Rule and any applicable Laws, Regulations, and Governmentwide policies.
 - If the NRC applies a limited dissemination marking that restricts access only to the recipient, then the recipient would not be permitted to share the document with a third party.
- NARA-approved limited dissemination markings available for agency use are included in the CUI Registry: <https://www.archives.gov/cui/registry/limited-dissemination>

NIST SP 800-171 Compliance & Inspections

- Agencies must:
 - Prescribe, at a minimum, the requirements of NIST SP 800–171 when sharing electronic CUI with non-executive branch entities that are not operating an information system on behalf of the agency.
 - Reference: <https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final>
 - Use NIST SP 800-171A, “Assessing Security Requirements for Controlled Unclassified Information,” to assess non-executive branch entities for compliance.
 - Reference: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171a.pdf>
- As contracts and written agreements are established and/or modified to reflect the CUI requirements, it would be appropriate for agencies to establish a reasonable deadline for non-executive branch entities to comply with NIST SP 800-171.
- Agencies have flexibility in determining the frequency of inspections for non-executive branch entities.
 - [NARA CUI Notice 2019-04](#), “Oversight of the Controlled Unclassified Information (CUI) Program within Private Sector Entities,” provides guidance to agencies.
 - Agencies should look to perform selective validation based on the type of CUI, quantity, or mission related to the CUI that’s handled by the non-executive branch entity.
- NRC CUI Working Group Path Forward
 - Hold further discussions on NIST SP 800-171 within the NRC CUI Working Group and Steering Committee.
 - Hold a future public meeting(s) to discuss this topic.

Summary

The NRC plans to:

- Establish a path forward on written agreements between the NRC and non-executive branch entities.
- Continue to coordinate with NARA and other federal agencies as the NRC develops its CUI program.
- Continue to engage and seek feedback from NRC external stakeholders on a routine basis.

How Can You Obtain Additional Information?

- NARA CUI Website (<https://www.archives.gov/cui>)
 - CUI Registry
 - Policy & Guidance
 - Training (NARA CUI videos)
 - CUI Blog
 - CUI Program Update To Stakeholders Meeting
- NRC CUI Public Meetings
- NRC CUI Public Website (<https://www.nrc.gov/reading-rm/cui.html>)
- Send an email to “CUI@nrc.gov”
 - John Moses, NRC CUI Senior Agency Official
 - Tanya Mensah, NRC CUI Program Manager

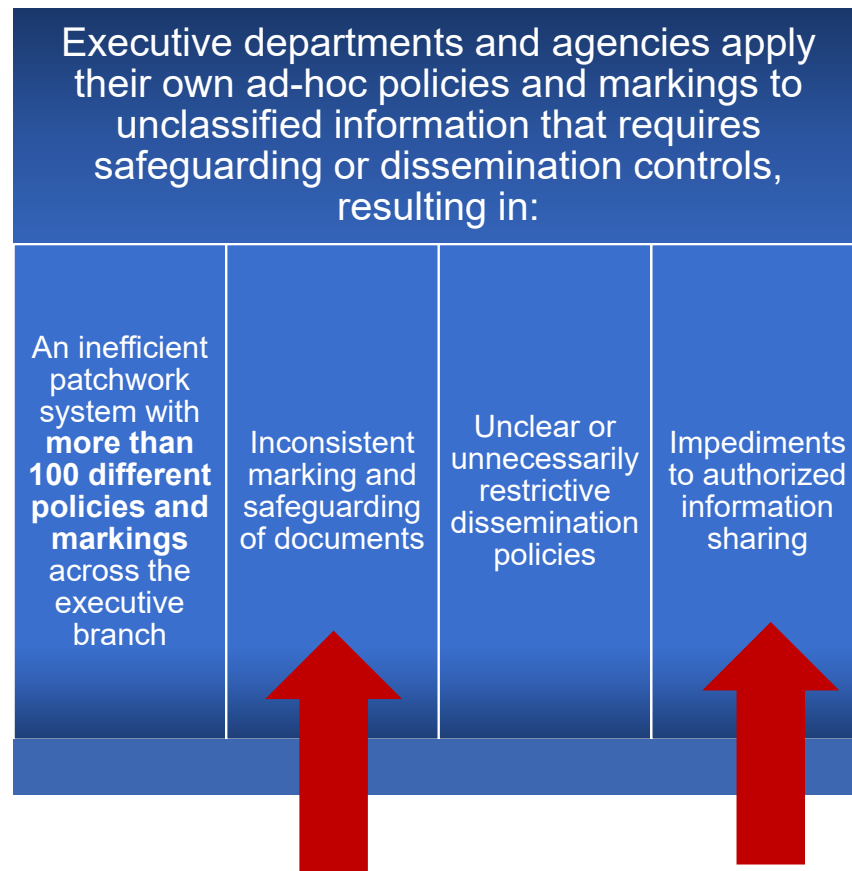
Questions/Opportunity for Comment

CUI BACKGROUND SLIDES

NRC Sensitive Unclassified Non-Safeguards Information (SUNSI) Program

- SUNSI is:
 - The NRC's current program to protect information that is generally not publicly available and encompasses a wide variety of categories (e.g., personnel privacy, attorney-client privilege, confidential source, etc.).
 - Any information where the loss, misuse, modification, or unauthorized access can reasonably be foreseen to harm the public interest, the commercial or financial interests of the entity or individual to whom the information pertains, the conduct of NRC and Federal programs, or the personal privacy of individuals.

Why was the CUI Program Established?

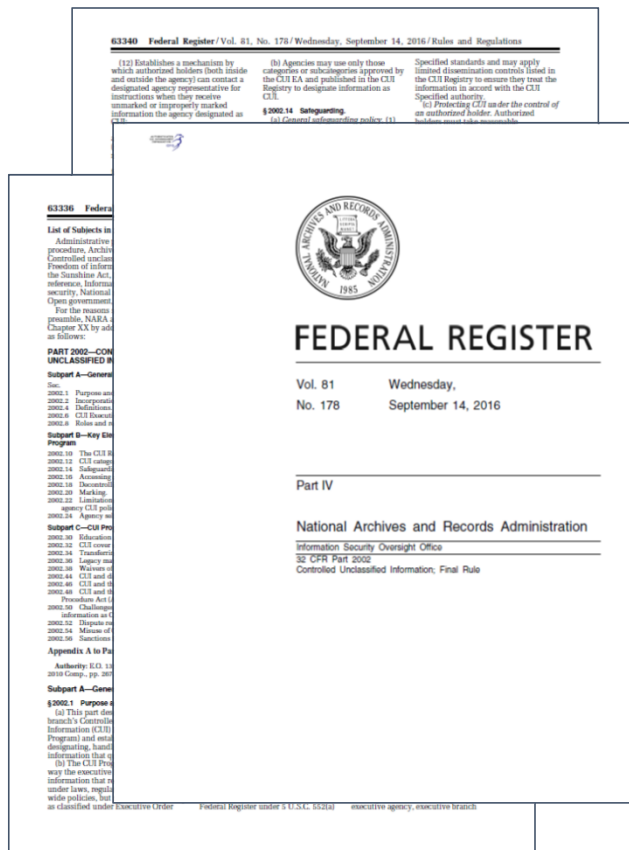


Executive Order 13556



- Established CUI Program (**November 4, 2010**)
 - Required agencies to review and identify categories of unclassified information requiring safeguarding or dissemination controls by existing Law, Regulation, or Government-wide policy.
 - Promoted information sharing with Federal partners (e.g., industry, academia, licensees, vendors, States).
- Designated an Executive Agent (EA) to implement Executive Order 13556 and oversee Department and Agency actions to ensure compliance.
 - National Archives and Records Administration (NARA)
 - Information Security Oversight Office (ISOO)

CUI Rule



- **32 CFR 2002 (September 14, 2016) [CUI rule]**
- Implements the CUI Program
 - Establishes policy for designating, handling, and decontrolling information that qualifies as CUI
 - **Effective: November 14, 2016 (Day 0)**
- Describes the minimum protections (derived from existing agency practices) for CUI
 - Physical and Electronic Environments
 - Marking
 - Sharing
 - Destruction
 - Decontrol

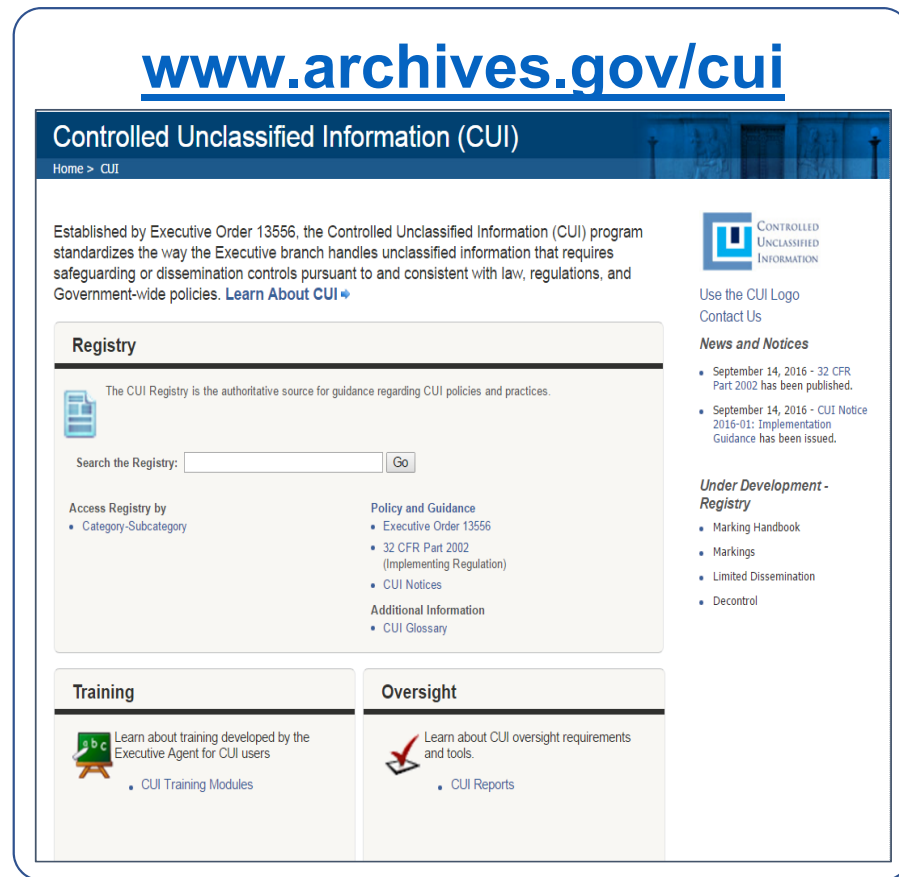
CUI Registry

CUI Registry = What we protect

It is a “living” catalogue of what the Executive branch protects.

The CUI Registry identifies all approved CUI categories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures.

- Categories
- Limited Dissemination Controls
- Marking Guidance
- CUI Notices
- Training and awareness
- Annual Reports to the President



Types of CUI

- CUI Basic
 - Information type for which Laws, Regulations, or Government-wide policies require or permit protection, but do not set out specific handling or dissemination controls.
 - Agencies protect CUI Basic per the uniform controls established in 32 CFR 2002 and the CUI Registry.
- CUI Specified
 - Information type for which Laws, Regulations, or Government-wide policies require or permit protection and also include one or more specific handling standards for that information (e.g., unique markings, enhanced physical safeguards, limits on who can access the information).
 - Examples: Export Controlled, Safeguards Information
 - Agencies protect the information at the CUI Basic Level, except where Laws, Regulations, or Government-wide specify something different.

NRC Banner Marking Examples

“OFFICAL USE ONLY” markings will no longer be used after the NRC transitions from SUNSI to CUI.

(SUNSI)

- OFFICIAL USE ONLY– SECURITY-RELATED INFORMATION
- OFFICIAL USE ONLY – PROPRIETARY INFORMATION
- OFFICIAL USE ONLY – PRIVACY ACT/PERSONALLY IDENTIFIABLE INFORMATION

(CUI)

- CUI//SP-SRI
- CUI//PROPIN
- CUI//PRVCY

Federal Acquisition Regulation (FAR)*

The FAR rule ensures uniform implementation of the requirements of the CUI program in **contracts across the government**.



**Federal Acquisition Regulation: Controlled Unclassified Information (FAR case 2017-016)*