NRC Controlled Unclassified Information (CUI) Public Meeting

Thursday, July 25, 2019

Commissioners' Conference Room

1-4 pm EDT

Introductions & Opening Remarks

Agenda

- CUI Overview
  - Questions & Comments
- NRC Transition to CUI
  - Questions & Comments
- Meeting Conclusion

Controlled Unclassified Information (CUI) Overview

What is CUI?

- An information security reform that standardizes the way the federal government handles information that is not classified 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).

Why was the CUI Program Established?

Executive departments and agencies apply their own ad-hoc policies and markings to unclassified information that requires safeguarding or dissemination controls, resulting in:

- An inefficient patchwork system with **more than 100 different policies and markings** across the executive branch
- Inconsistent marking and safeguarding of documents
- Unclear or unnecessarily restrictive dissemination policies
- Impediments to authorized information sharing

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.

Licensee Handling of CUI

- CUI includes only information the government creates or possesses, or that an entity creates or possess on behalf of the government (e.g. a contractor).
- Licensees 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 information currently shared by the NRC with licensees 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 SGI).
- Licensees 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

Requirements For Agencies When Sharing CUI

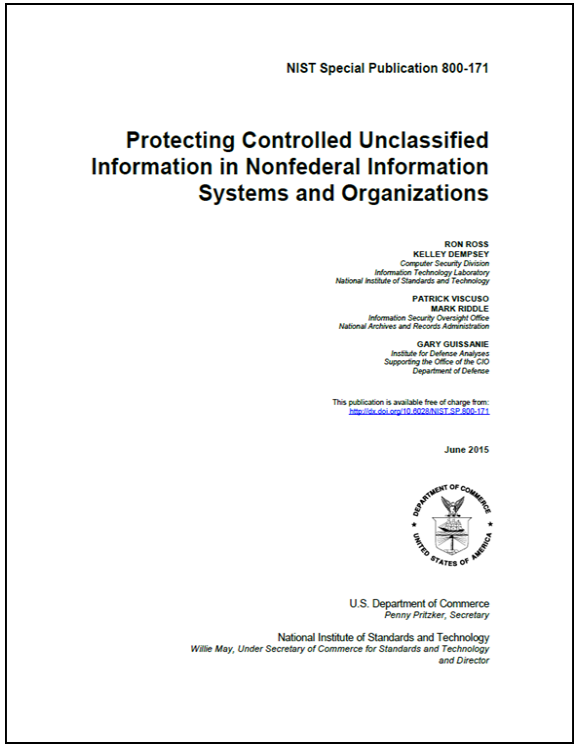
- Prior to disseminating or sharing CUI with non-executive branch entities, agencies should, "whenever feasible," enter into "written agreements or arrangements," in which the recipient agrees to protect the information in accordance with the CUI Rule.

- 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.

NIST Special Publication 800-171

- NARA's CUI rule identifies 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 information and to reduce the risk of data breaches that involve CUI that resides on a non-Federal information system.
- When non-executive branch entities are not using or operating an information system or maintaining or collecting federal information ‘‘on behalf of’’ an agency, the agency must prescribe the requirements of NIST SP 800–171 in written agreements or arrangements to protect the confidentiality of the CUI, unless the agreement establishes higher security requirements.


NIST Special Publication 800-171

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

RON ROSS
KELLEY DEMPSEY
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

PATRICK VISCUSO
MARK RIDDLE
Information Security Oversight Office
National Archives and Records Administration

GARY GUISSANIE
Institute for Defense Analyses
Supporting the Office of the CIO
Department of Defense

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-171

June 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf

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)*

Questions/
Opportunity for Comment

NRC Transition To CUI

NRC Transition Plan

- The CUI program will be implemented at the NRC through the NRC CUI Senior Agency Official (SAO).
  - The CUI SAO ensures that the agency has sufficient policies and guidance in place for NRC staff and contractors that handle unclassified information.
- CUI will eventually replace the NRC's current Sensitive Unclassified Non-Safeguards Information (SUNSI) program.
- CUI includes Safeguards Information (SGI) and SGI-Modified Handling, though all SGI controls codified in NRC regulations will remain in effect.
- As the NRC transitions through the various stages of CUI implementation, the NRC will communicate pertinent information to the NRC staff, contractors, and external stakeholders.

NRC CUI Implementation Estimated Timeline*

Fiscal Year (FY) 2021

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

**The current milestones shown above are estimates and are subject to change.*

Areas For Future Engagement

- Establishing written agreements or arrangements
- NIST SP 800-171

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

BACKGROUND SLIDES

Executive Order 13556


Presidential Documents

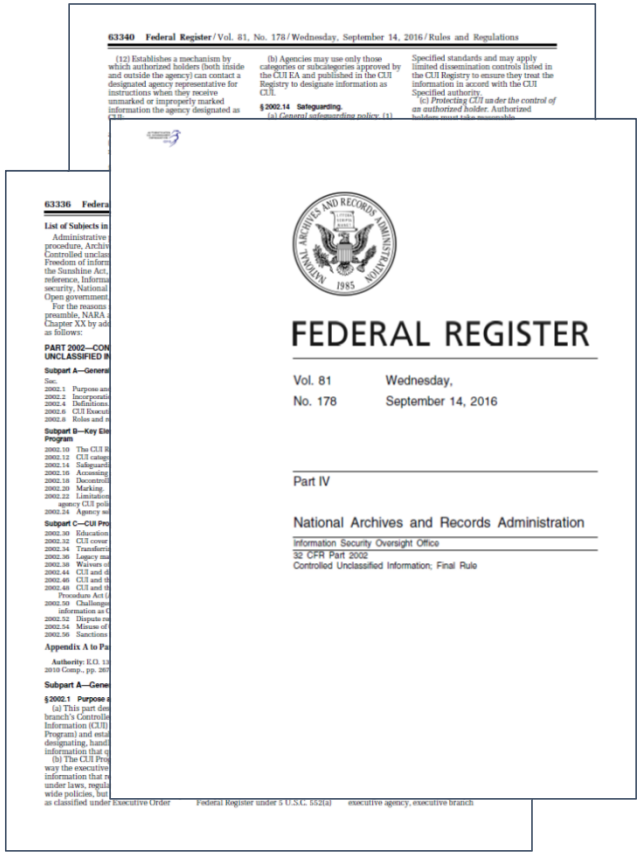
Executive Order 13556 of November 4, 2010

Controlled Unclassified Information

- 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

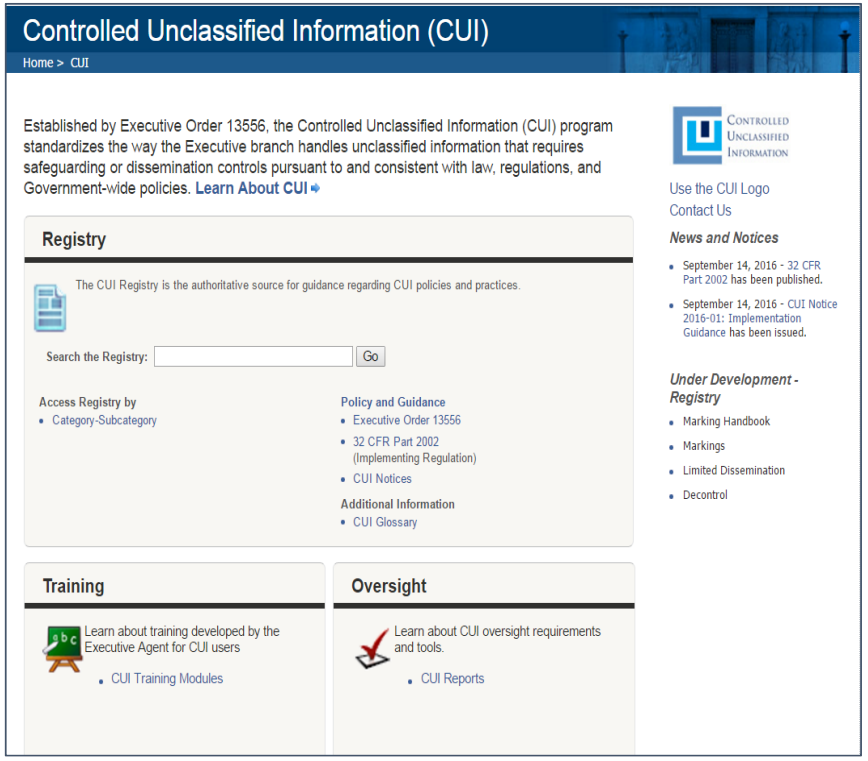
CUI Registry = What we protect

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

www.archives.gov/cui



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: Security-Related Information, Safeguards Information
  - Agencies protect the information at the CUI Basic Level, except where laws, regulations, or government-wide specify something different.

CUI CATEGORIES

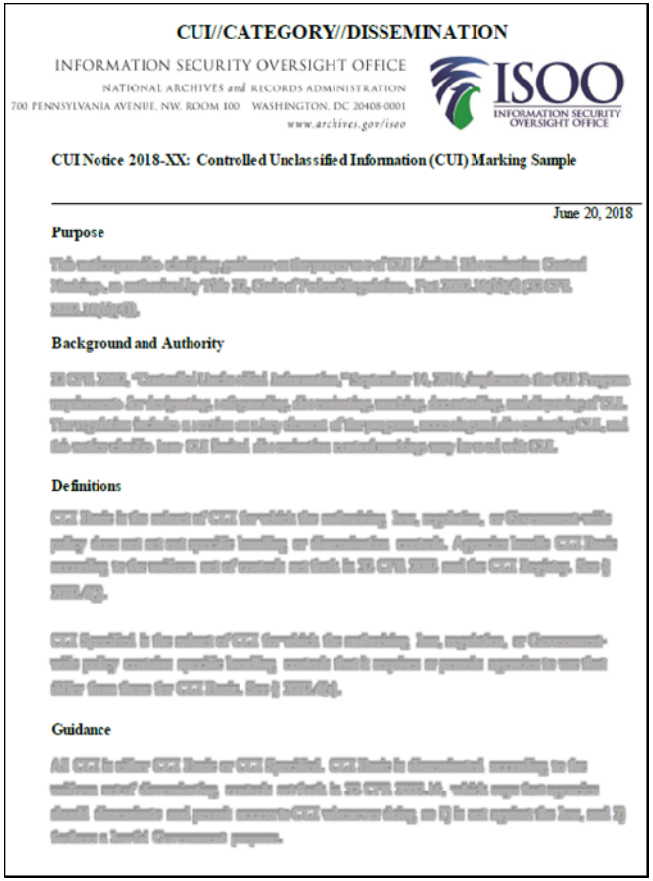
A list of the information categories maintained by NARA that qualify as CUI is available at the CUI Registry: https://www.archives.gov/cui/registry/category-list

Organizational Index Grouping in the CUI Registry

Agriculture	**Law Enforcement**
Controlled Technical Information	**Legal**
Critical Electric Infrastructure Information	**North Atlantic Treaty Organization (NATO)**
Emergency Management	**Nuclear**
Export Control	**Patent**
Financial	**Privacy**
Geodetic Product Information	**Procurement and Acquisition**
Immigration	**Proprietary Business Information**
Information Systems Vulnerability	**SAFETY Act Information**
Information	**Statistical**
Intelligence	**Tax**
International Agreements	**Transportation**

CUI Markings

- CUI Banner Marking Format
  - CUI//CATEGORY//DISSEMINATION
    - Bold, capitalized black text, and centered.
  - Category markings:
    - Listed in the CUI Registry: https://www.archives.gov/cui/registry/category-marking-list
    - Arranged in alphabetical order after the "CUI//" in the banner.
  - CUI Specified categories are preceded by "SP".



CUI//CATEGORY//DISSEMINATION

INFORMATION SECURITY OVERSIGHT OFFICE
NATIONAL ARCHIVES and RECORDS ADMINISTRATION
700 PENNSYLVANIA AVENUE, NW, ROOM 100 WASHINGTON, DC 20408-0001
www.archives.gov/isoo

ISOO INFORMATION SECURITY OVERSIGHT OFFICE

CUI Notice 2018-XX: Controlled Unclassified Information (CUI) Marking Sample

June 20, 2018

Purpose

Background and Authority

Definitions

Guidance

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

Controlled Environments

Any area or space an authorized holder* deems to have adequate physical or procedural controls (e.g., barriers and managed access controls) for protecting CUI from unauthorized access or disclosure.

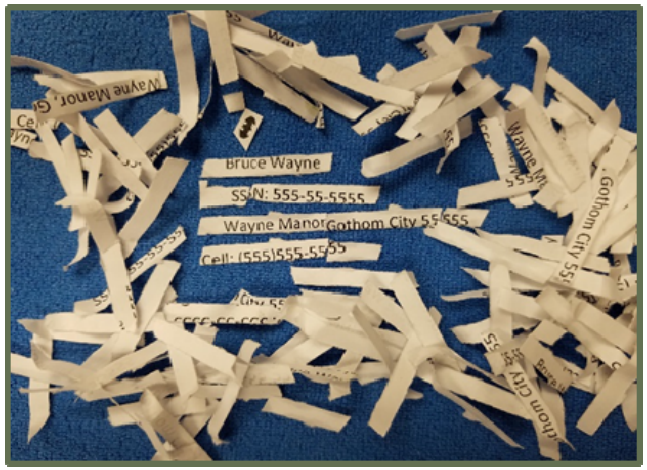
- Requirements:
  - Establish controlled environments in which to protect CUI from unauthorized disclosure.
  - Reasonably ensure that unauthorized individuals cannot access or observe CUI, or overhear conversations discussing CUI.
  - Keep CUI under the authorized holder's direct control or protect it with at least one physical barrier.

Authorized Holder: An individual, agency, organization, or group of users permitted to designate or handle CUI, in accordance with the CUI rule. See§ 2002.4(d).

Destruction

When destroying CUI, including in electronic form, agencies must do so in a manner that makes it unreadable, indecipherable, and irrecoverable.

Unacceptable



Acceptable

Destroy paper using cross cut shredders that produce particles that are no more than 1mm by 5 mm.

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.

Safeguards Information (SGI)

- SGI:
  - 10 CFR Part 73, “Physical Protection of Plants and Materials,” provides specific requirements for the protection of Safeguards Information.
  - A special category of sensitive unclassified information authorized by Section 147 of the Atomic Energy Act to be protected.
  - Concerns the physical protection of operating power reactors, spent fuel shipments, strategic special nuclear material, or other radioactive material.