

# CONTROLLED UNCLASSIFIED INFORMATION (CUI) AT THE NRC

---

Presentation to the Annual CRCPCD Meeting  
May 23, 2018

Sara Mroz, CUI Program Manager

# What is CUI?

- **C**ontrolled: required by law, regulation, or Government-wide policy to be safeguarded or have limited dissemination
- **U**nclassified: not included under Executive Order 13526 “Classified National Security Information” (December 29, 2009) or a predecessor or successor order, or Atomic Energy Act of 1954, as amended
- **I**nformation: data, reports, documents, etc.

# Why CUI?

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

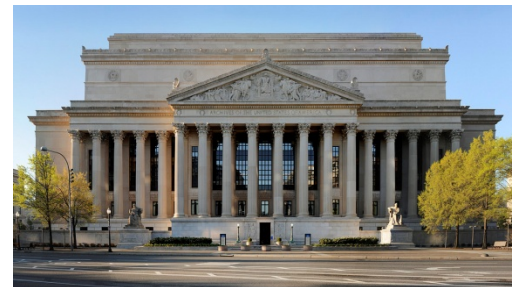
Impediments to authorized information sharing

# Executive Order 13556

- Issued November 4, 2010
- Established CUI Program
- Designated an Executive Agent to implement and oversee compliance




CONTROLLED  
UNCLASSIFIED  
INFORMATION



Source: [www.archives.gov/dc](http://www.archives.gov/dc)

# CUI Registry

- EO 13556 called for a review of the categories, subcategories, and markings used by agencies
- Information types were grouped together, legal authorities examined, and CUI Registry published



Fun Fact:  
Agencies submitted  
>2,200 authorities for  
controlling many  
types of information!

# 32 CFR 2002: The “CUI Rule”

- Published September 14, 2016
- Effective November 14, 2016
  
- Implements CUI Program
- Establishes policy for designating, handling, and decontrolling CUI
- Describes, defines, and provides guidance on the minimum protections for CUI
- Emphasizes unique protections described in law, regulation, and/or Government-wide policies (authorities)

# NIST Special Publication 800-171

- Agencies must use NIST SP 800-171 when establishing security requirements to protect CUI's confidentiality on non-Federal information systems
- Intended for use by Federal agencies in appropriate contractual vehicles or other agreements
- Established requirements for protecting CUI at Moderate Confidentiality Impact Value
- Non-tailorable requirements

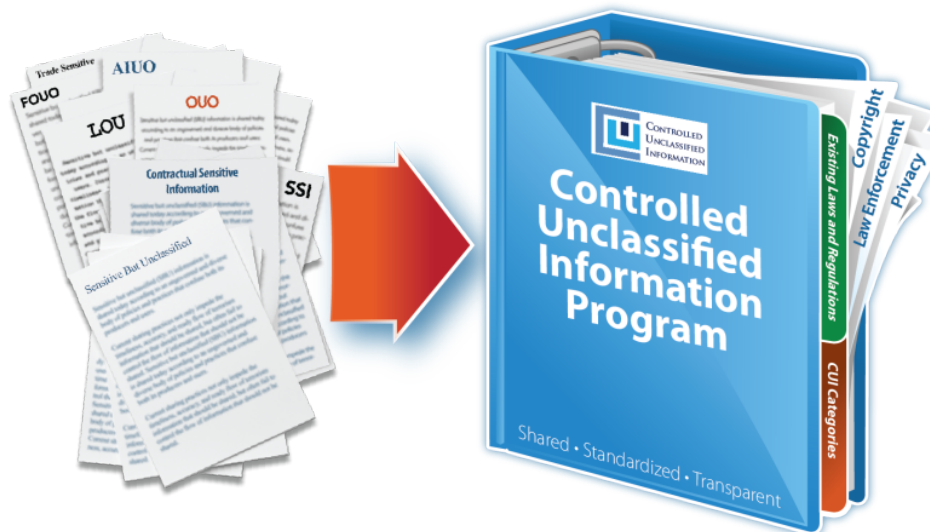
# When to Use NIST SP 800-171

- Use NIST SP 800-171 when a non-Federal entity:
  - Receives CUI incidental to providing a service or product to the Government outside of processing services (ex: producing a study, conducting research, creating a training program, etc.)
  - Government is only concerned with the confidentiality of the information ... **CUI** is regarded as the asset requiring protection
  
- DO NOT use NIST SP 800-171 when a non-Federal entity:
  - Collects or maintains CUI as part of a Government function (ex: census takers or records storage)
  - Builds an information system or operates an information system for the Government (ex: an email provider or payroll system)
  - Provides processing services for the Government (ex: cloud service provider)
  - Government has a concern in the confidentiality, integrity, and availability of the information system ... the **system** is the asset requiring protection
  - Agencies may require these systems to meet additional requirements that it sets for its own internal systems

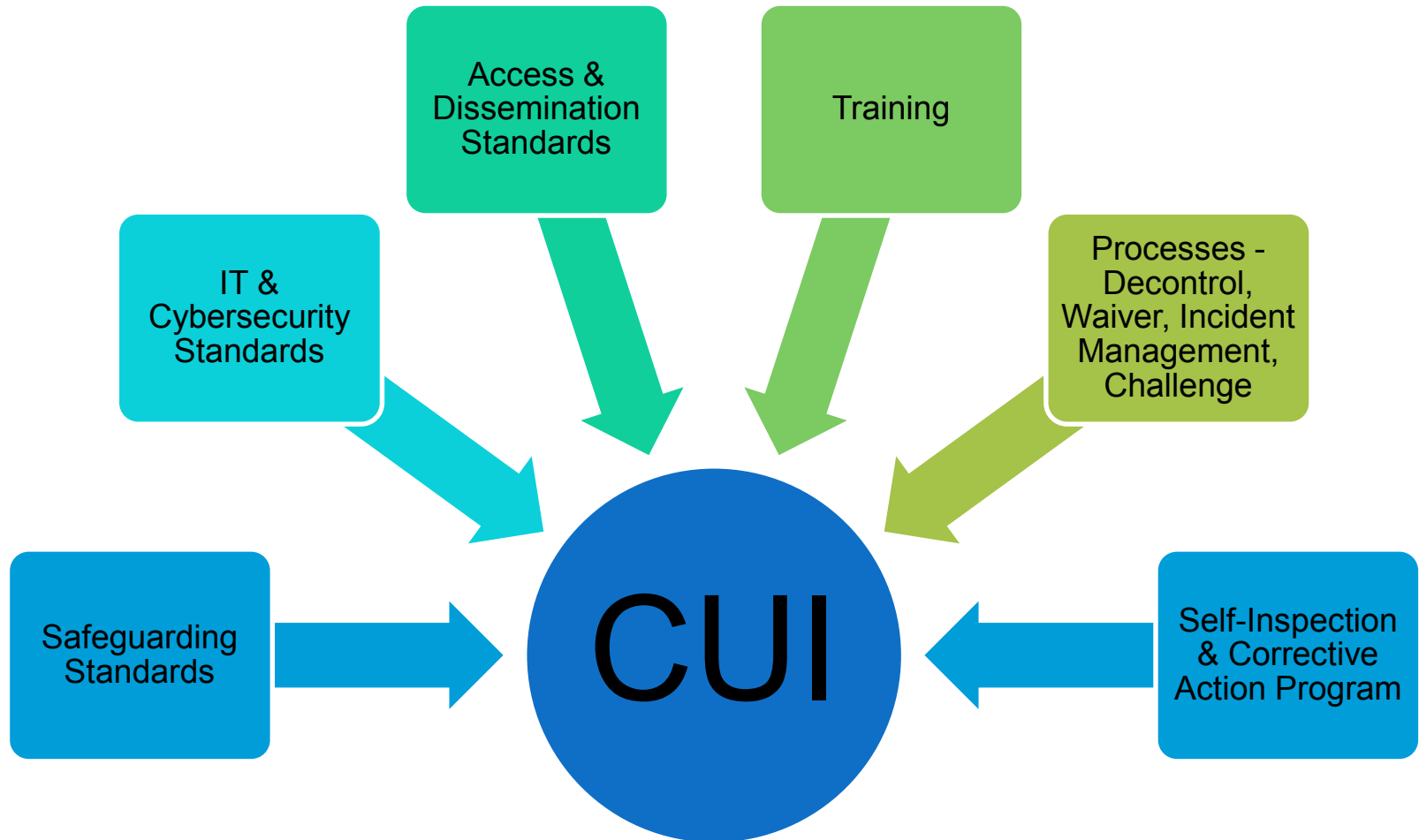


# CUI at the NRC

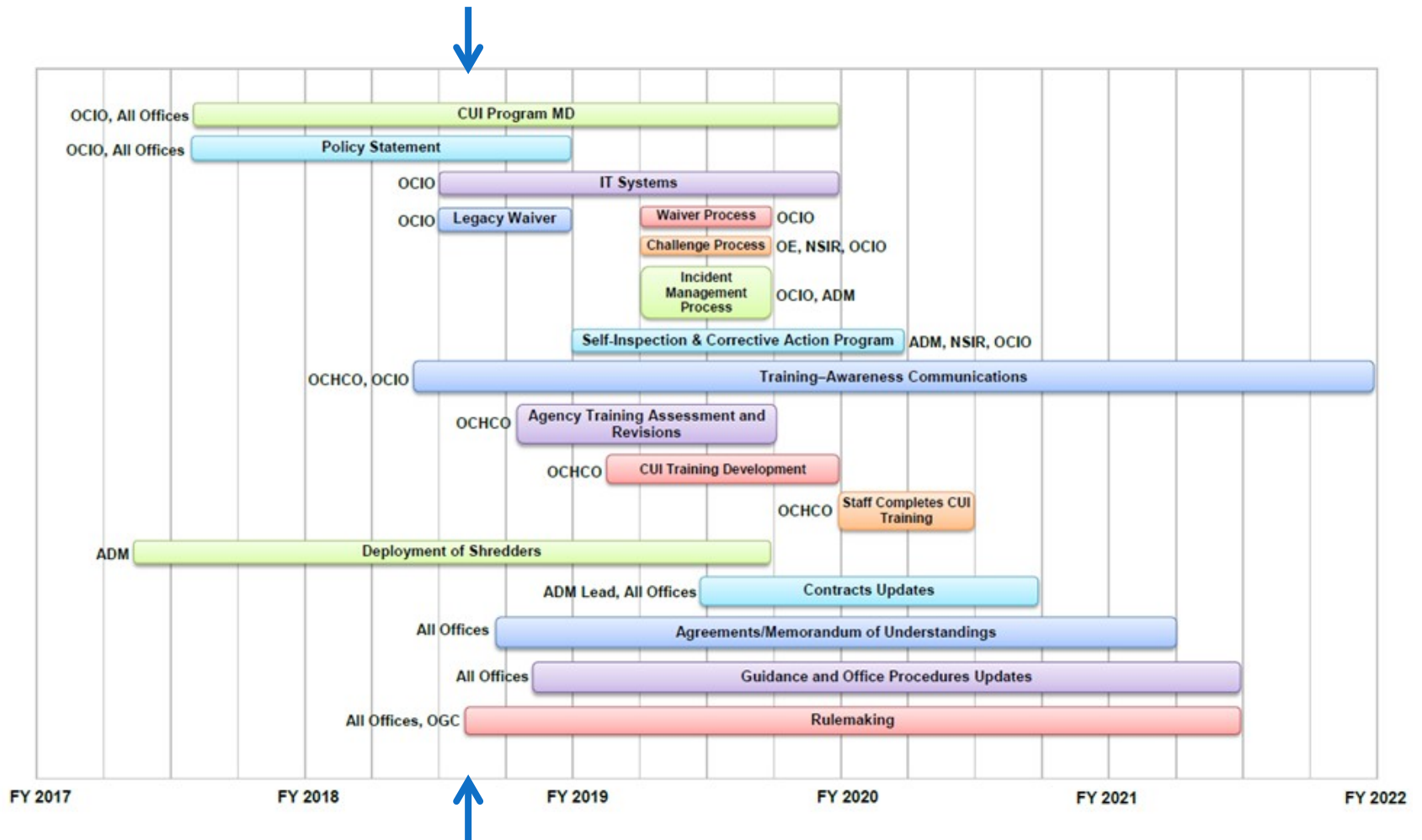
- Replace the current Sensitive Unclassified Non-Safeguards Information (SUNSI) program (i.e., proprietary information, personally identifiable information)
- Include Safeguards Information (SGI) and Safeguards Information—Modified (SGI-M) Handling



# NRC's CUI Program Elements



# Schedule



# Transition to CUI Program

- During transition, all elements and controls of the SUNSI program will remain in place
- Until directed by the NRC's CUI policy, guidance, and training, NRC employees and contractors must not use CUI markings or follow other requirements specific to CUI
- During transition period, information received at the agency that is marked as CUI must be protected accordingly

# Impact on External Stakeholders

- Recognize changes will have impacts on external stakeholders – including Agreement States, licensees, tribes, intervenors, contractors, and others
- Requirements will likely vary between stakeholder groups based on types of information shared and how that information is created
- Want input from stakeholders on best approaches

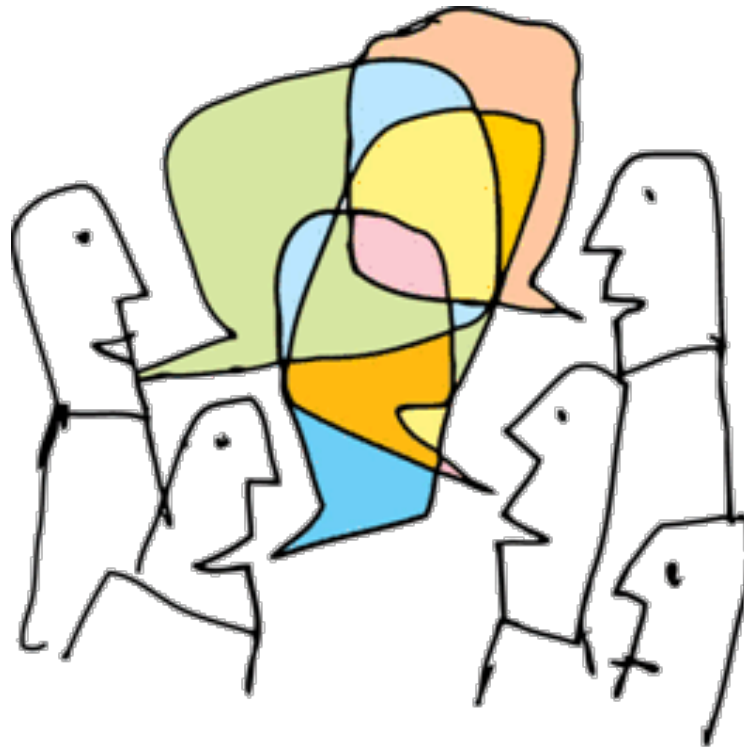
# Information Sharing Agreements

- Agencies should, when feasible, enter into or modify existing agreements with non-Executive branch entities before sharing CUI
  - Agreements must include provisions that require handling CUI in accordance with the CUI Rule
- Existing laws, regulations and Government policies that govern CUI-Specified, must be followed whether or not an Agreement is in place with the non-Executive branch entity taking receipt of the sensitive information (ex: SGI)

# Intention to Reduce Burden

- Looking at potential new solutions / services for secure information sharing and collaboration
- Legal interpretation of what must be protected and how
- Seeking input on best approaches

# Discussion





# Contacts and Resources

- Sara Mroz, CUI Program Manager
  - [Sara.Mroz@nrc.gov](mailto:Sara.Mroz@nrc.gov)
- John Moses, Senior Agency Official for CUI
  - [John.Moses@nrc.gov](mailto:John.Moses@nrc.gov)
- SECY-18-0035: Update on Development of the Controlled Unclassified Information Program
  - ML18065B107
  - <https://www.nrc.gov/docs/ML1806/ML18065B107.pdf>
- NARA CUI website
  - [www.archives.gov/cui](http://www.archives.gov/cui)