Controlled Unclassified Information

Implementation & Recommendations

Shared • Standardized • Transparent

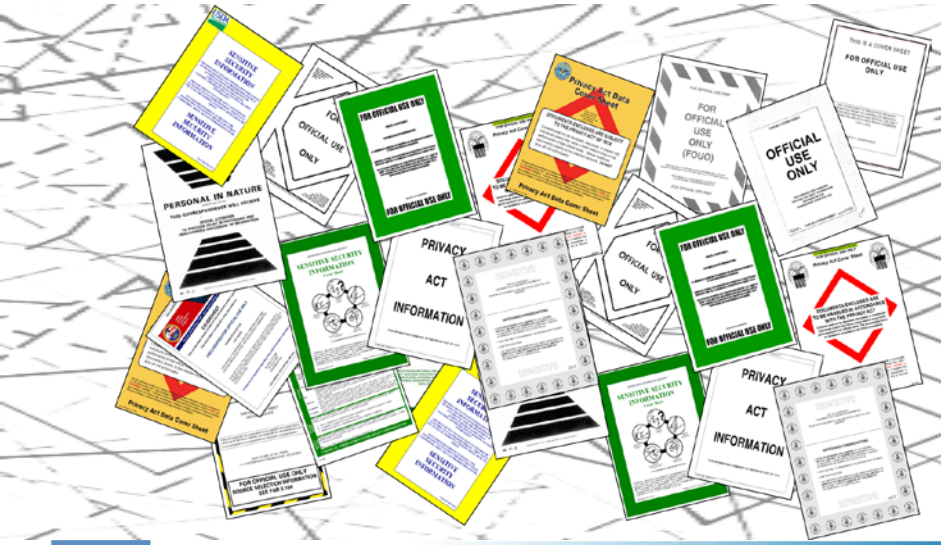
Information Security Oversight Office (ISOO)

Outline

- Information Security Reform
- CUI Registry
- Implementing Directive (32CFR2002)
- Federal Acquisition Regulation
- Phased Implementation
- Annual Report
- Recommendations for Implementation

Information Security Reform

- Clarifies and limits what to protect
- Defines safeguarding
- Promotes authorized information sharing
- Reinforces existing legislation and regulations



CUI Registry = What we protect

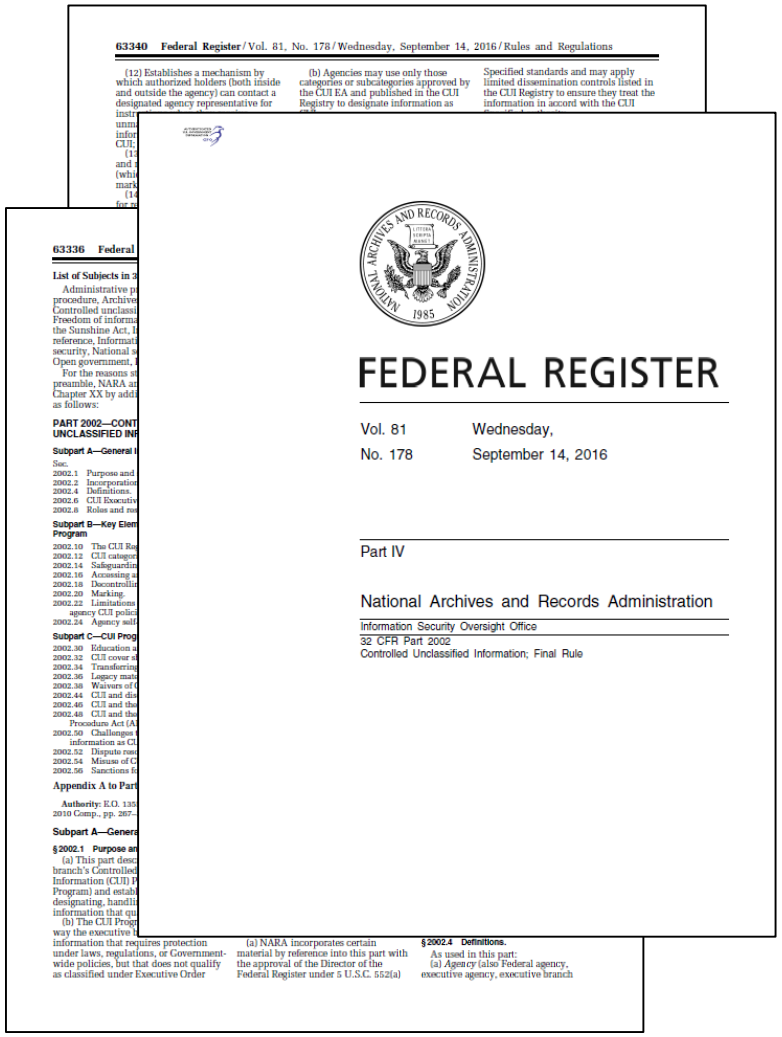
The CUI Registry is the repository for all information, guidance, policy, and requirements on handling CUI.

The CUI Registry is a catalogue of what the Executive branch should be protecting.

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

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

32 CFR 2002 = How we protect



- Effective: November 14, 2016
- Started implementation efforts within the Executive branch
- Establishes a protection baseline
  - Designation
  - Physical and Electronic Environments
  - Marking
  - Sharing
  - Destruction
  - Decontrol
- Emphasizes unique protections described in law, regulation, and/or Government-wide policies (authorities)

Federal Acquisition Regulation (FY18)

Will standardize the way the Executive branch conveys safeguarding guidance

Phased Implementation

- **CUI practices and Legacy practices will exist at the same time.**
  - Legacy practices will be phased out as agencies implement
- Resources
  - Plan and Budget
- Annual Reporting
  - November 1
- Sequencing
  - Policy
  - Training
  - Self Inspection

3 to 4 years

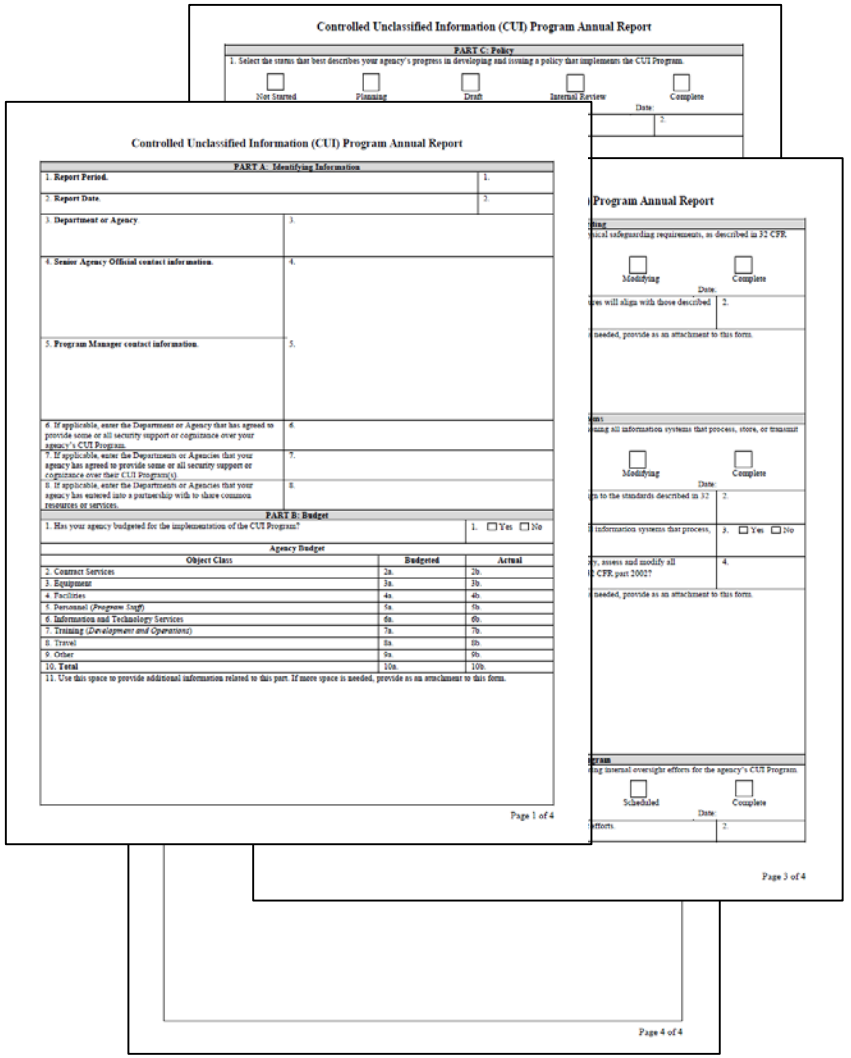
What goes in the Annual Report?

1. Where you are….

   - Planning
   - Draft
   - Internal Coordination
   - Complete

2. When you expect to be there….

   - Dates (projections)



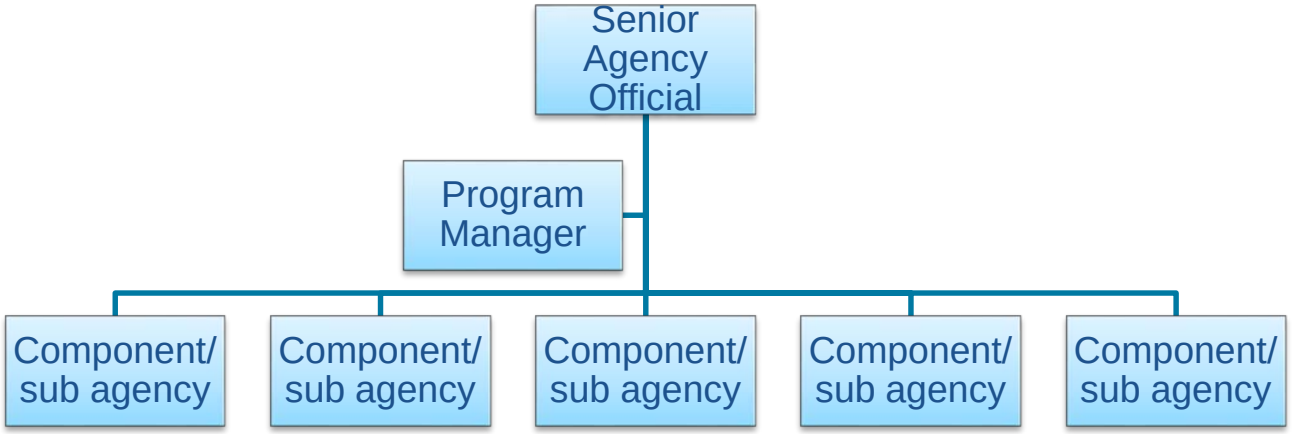
Recommendations

- Program Management
- Policy
- Training and Awareness
- Physical Safeguarding
- Information Systems
- Destruction
- Self-Inspections

See CUI Notice 2017-01

Program Management

- Senior Agency Official
- Program Manager
- Agency Working Groups



Policy

- Agency regulations will provide the foundation for effective management, oversight, and sustainment of program activities. Agencies may implement the CUI Program through a single policy or through multiple policies that address specific elements of the CUI Program.

  - The CUI Registry;
  - CUI categories and subcategories;
  - Safeguarding CUI in the physical environment;
  - Safeguarding CUI in the electronic environment;
  - Access and dissemination;
  - Marking and identification;
  - Limitations on the applicability of agency policy;
  - Contracts and agreements;
  - Agency self-inspection program;
  - Education, training, and awareness;
  - Transferring records;
  - Legacy materials;
  - Waivers of CUI requirements;
  - CUI and disclosure statutes;
  - CUI and the Privacy Act;
  - Challenges to the designation of CUI; and
  - Misuse of CUI;

Training and Awareness

- Personnel who handle and/or create sensitive information must maintain a satisfactory knowledge and understanding of the protective measures that prevent or deter disclosures to unauthorized persons.

- Four types of training:

1. **Awareness training.** Awareness training or efforts will acquaint their workforce with the coming transition to the CUI Program within their agency and throughout the executive branch.
2. **Orientation training.** Orientation training will acquaint the workforce with the agency's CUI policy and program.
3. **Specified training.** Specified training will acquaint the workforce or a portion of the workforce with the special or unique handling requirements for CUI Specified categories or subcategories.
4. **Refresher training.** Refresher training reacquaints the workforce with safeguarding principles addressed in the initial orientation training.

Physical Safeguarding

- Agencies must safeguard CUI at all times in a manner that minimizes the risk of unauthorized disclosure while allowing for access by authorized holders.
- The 32 CFR part 2002 allows for considerable flexibility when it comes to ensuring that CUI is adequately protected in the physical environment. Agencies can leverage or utilize existing policies and practices when implementing the CUI Program.
- Evaluate the protective measures, policies, and procedures currently used within and across the agency to protect facilities, assets, and working environments.

Information Systems

- Information systems that used to store, process, or transmit CUI must be configured at no less than the **Moderate Confidentiality** impact value. The majority of the systems throughout the Executive branch are already configured to this standard.

1. Identify all information systems used to store, process, or transmit CUI;
2. Assess or determine their current configuration; and
3. Develop a plan or strategy to transition all information systems found to be configured lower than Moderate Confidentiality.

Destruction

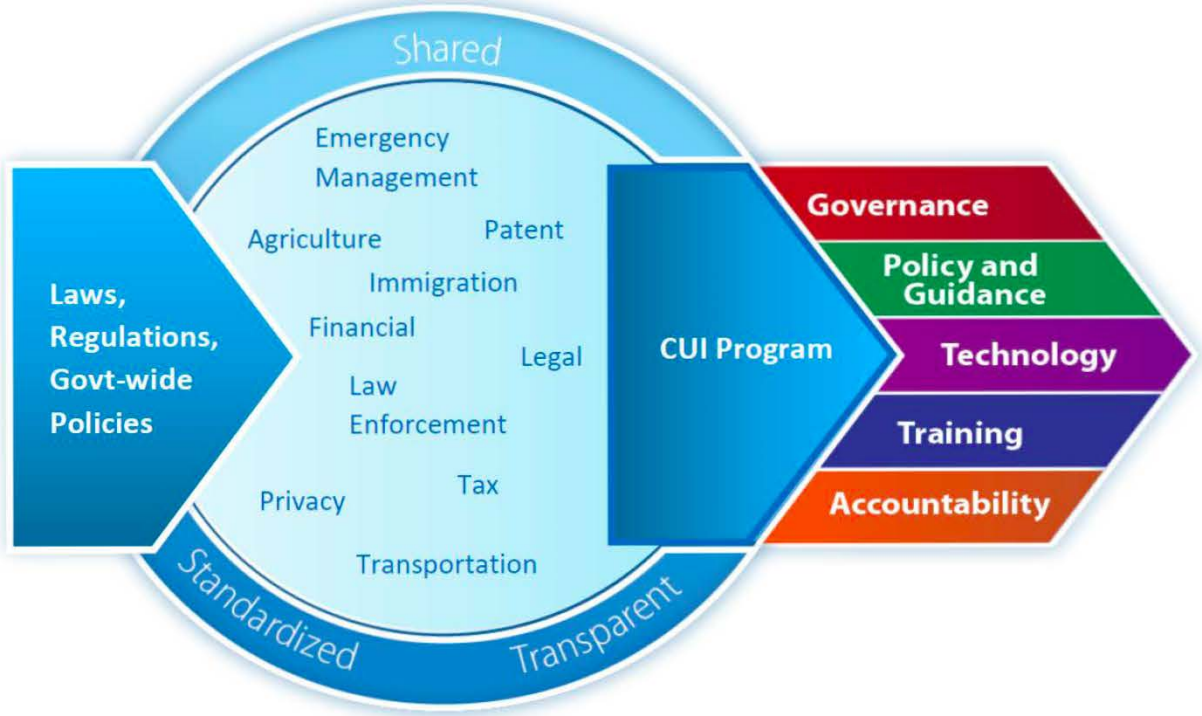
- When destroying CUI, including in electronic form, agencies must do so in a manner that makes the media unreadable, indecipherable, and irrecoverable. The National Institute of Standards and Technology Special Publication 800-88, "Guidelines for Media Sanitization," provides agencies with recommendations on how CUI can be destroyed or sanitized.

1. Assess the methods currently used to destroy or sanitize CUI, regardless of media, and across the agency, including component agencies or internal lines of business;
2. Identify any current policy or procedures within the agency that require a particular method of destruction or sanitization for sensitive information;
3. Identify all destruction equipment, procedures, and methods, approved and not approved for CUI destruction or sanitization; and
4. Establish a system to routinely evaluate and assess the destruction equipment, procedures, and methods used for the destruction or sanitization of CUI.

Self Inspections

- Each year, agencies must conduct a review and assessment of their agency's CUI Program to evaluate program effectiveness, to measure the level of compliance, and to monitor implementation efforts.

Questions?


Shared
Emergency Management
Agriculture
Patent
Immigration
Financial
Legal
Law Enforcement
Tax
Privacy
Transportation
Standardized
Transparent
Laws, Regulations, Govt-wide Policies
CUI Program
Governance
Policy and Guidance
Technology
Training
Accountability