Controlled Unclassified Information

June 2018

Shared • Standardized • Transparent

Information Security Oversight Office (ISOO)

Outline

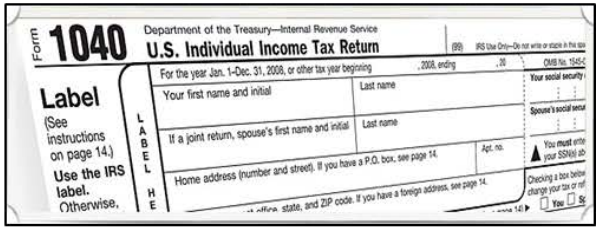
- What is CUI?
- CUI Program
- Implementation of the CUI Program
- NIST SP 800-171A (Draft)
- Federal Acquisition Regulation update
- Basic and Specified CUI
- Marking
- Destruction
- Controlled Environments (assessment and threat)
  - Physical
  - Electronic
- Other Considerations
- Q & A

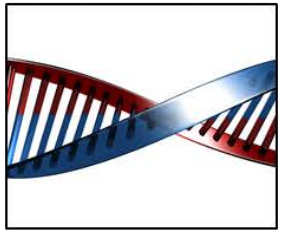
What is Controlled Unclassified Information or CUI?

- **CUI is information that needs protection.** Laws, Regulations, or Government wide policies call for this information to be protected.
  - The **CUI Registry** provides information on the specific categories and subcategories of information that the Executive branch protects.

CUI includes, but is not limited to:

- Privacy (including Health)
- Tax
- Law Enforcement
- Critical Infrastructure
- Export Control
- Financial
- Intelligence
- Privilege
- Unclassified Nuclear
- Procurement and Acquisition



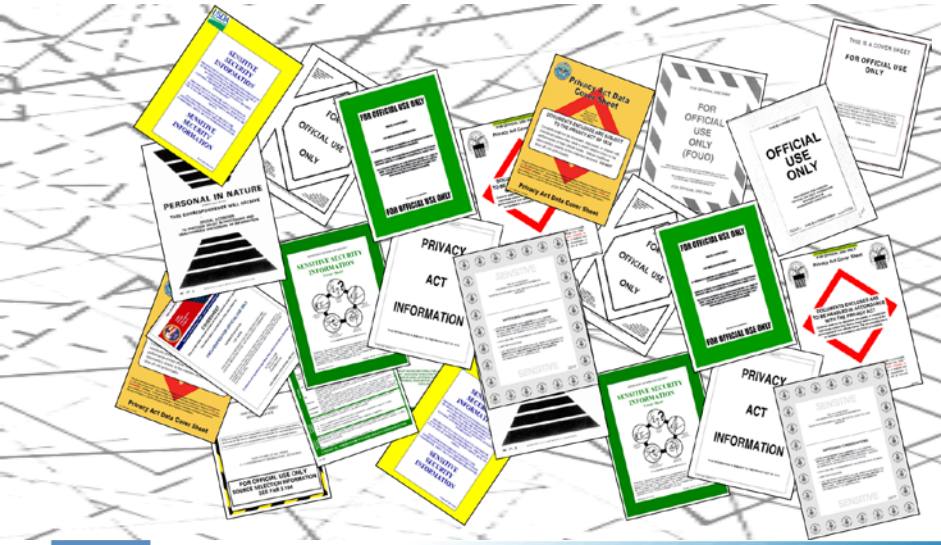


Why protect CUI?

- The loss or improper safeguarding of CUI could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
  - significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
  - significant damage to organizational assets;
  - significant financial loss; or
  - significant harm to individuals that does not involve loss of life or serious life threatening injuries

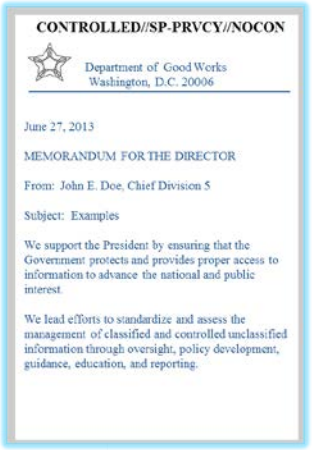
Information Security Reform = CUI Program

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



Safeguarding measures: Based on Existing Practices

- Policy and procedures
- Training and awareness
- Physical and Electronic protections
- Oversight Measures
- Reporting


CONTROLLED//SP-PRVCY//NOCON

Department of Good Works
Washington, D.C. 20006

June 27, 2013

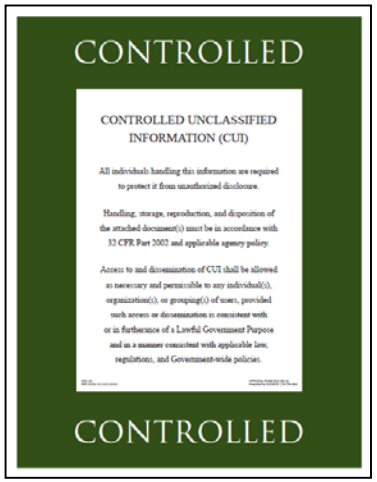
MEMORANDUM FOR THE DIRECTOR

From: John E. Doe, Chief Division 5

Subject: Examples

We support the President by ensuring that the Government protects and provides proper access to information to advance the national and public interest.

We lead efforts to standardize and assess the management of classified and controlled unclassified information through oversight, policy development, guidance, education, and reporting.



Implementation Projection

- 2-3 Years for full implementation
  - Resource dependent
  - **Policy**, Training, Physical Safeguarding, Systems, Contracts
- **CUI practices and Legacy practices will exist at the same time.**
  - Legacy practices will be phased out as agencies implement
- ISOO is assessing compliance (now)

CUI Registry = What we protect

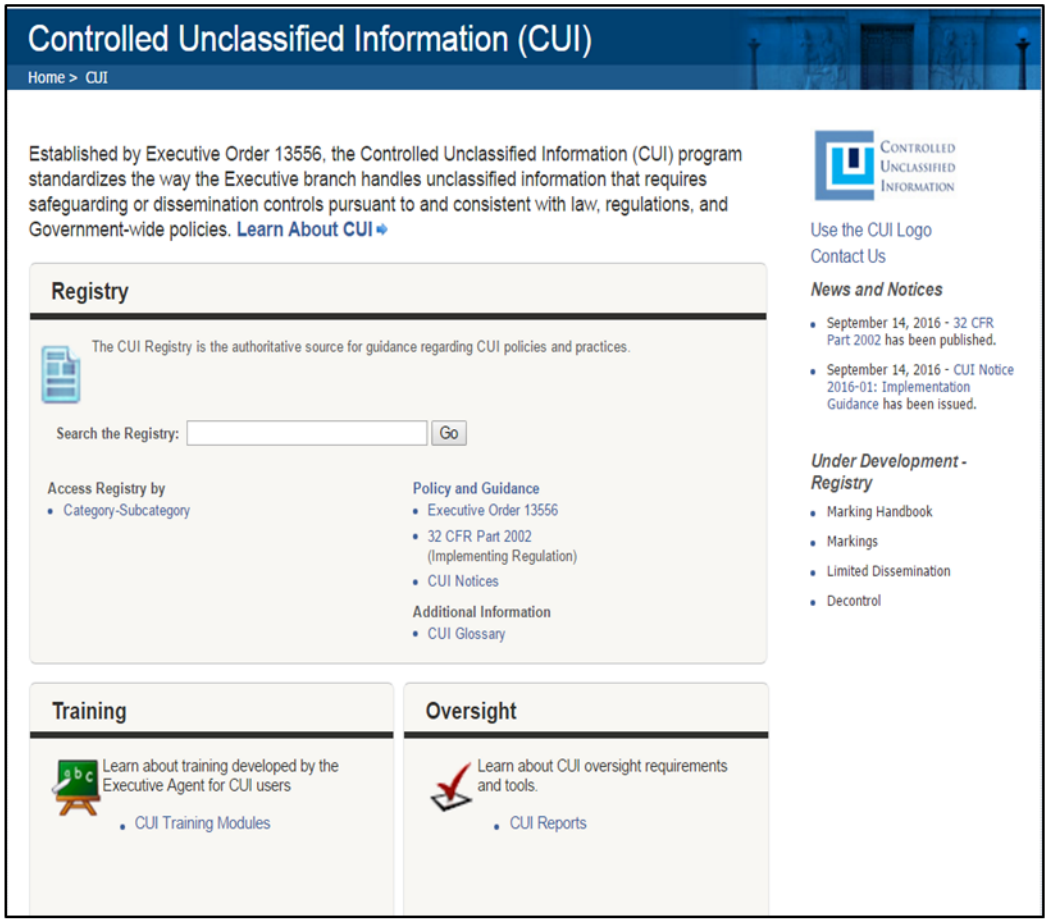
The CUI Registry is the repository for all information, guidance, policy, and requirements on handling CUI.

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

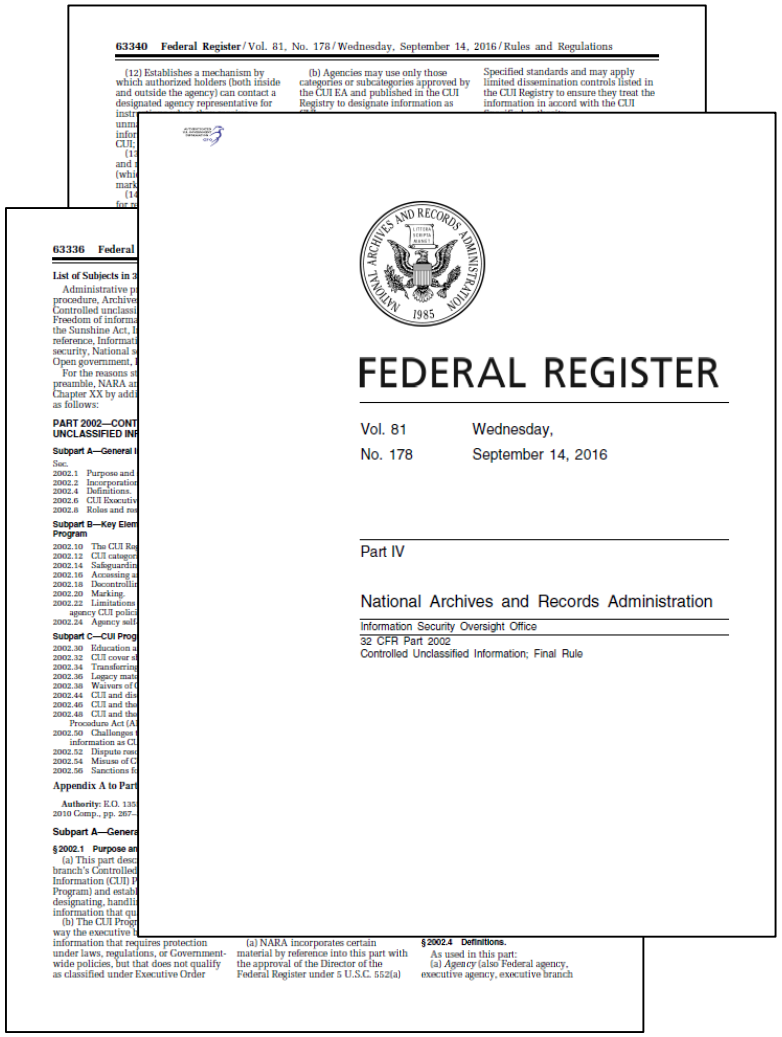
The CUI Registry identifies all approved CUI categories and subcategories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures.

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

www.archives.gov/cui



32 CFR 2002 = How we protect



63340 Federal Register / Vol. 81, No. 178 / Wednesday, September 14, 2016 / Rules and Regulations

(12) Establishes a mechanism by which authorized holders (both inside and outside the agency) can contact a designated agency representative for

(b) Agencies may use only those categories or subcategories approved by the CUI EA and published in the CUI Registry to designate information as

Specified standards and may apply limited dissemination controls listed in the CUI Registry to ensure they treat the information in accord with the CUI

63336 Federal

List of Subjects in 3

PART 2002—CONT UNCLASSIFIED INF

Subpart A—General

Subpart B—Key Elem Program

Subpart C—CUI Prog

Appendix A to Part

Subpart A—Genera

§ 2002.1 Purpose an

information that requires protection under laws, regulations, or Government-wide policies, but that does not qualify as classified under Executive Order

(a) NARA incorporates certain material by reference into this part with the approval of the Director of the Federal Register under 5 U.S.C. 552(a)

§ 2002.4 Definitions.

As used in this part:

(a) *Agency* (also Federal agency, executive agency, executive branch

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION 1985

FEDERAL REGISTER

Vol. 81 Wednesday,

No. 178 September 14, 2016

Part IV

National Archives and Records Administration

Information Security Oversight Office

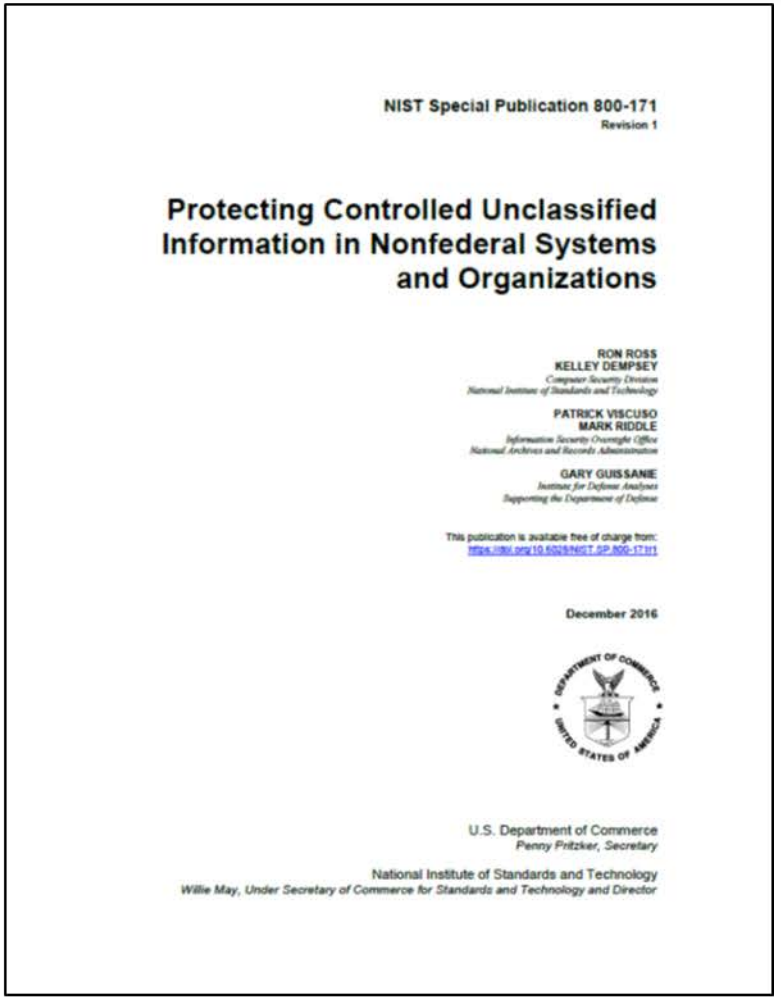
32 CFR Part 2002

Controlled Unclassified Information; Final Rule

- 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)

NIST Special Publication 800-171 (Revision 1)

- Agencies must use NIST SP 800-171 when establishing security requirements to protect CUI's confidentiality on non-Federal information systems.
- The NIST 800-171 is intended for use by federal agencies in appropriate contractual vehicles or other agreements established between those agencies and nonfederal organizations.
- Establishes requirements for protecting CUI at the **Moderate Confidentiality Impact Value**.
- Non-tailorable requirements
- Allows for Flexibility in how to meet requirements



NIST Special Publication 800-171
Revision 1

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

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

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

GARY GUISSANE
Institute for Defense Analyses
Supporting the Department of Defense

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r1

December 2016

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

NIST Special Publication 800-171A

Title: Assessing Security Requirements for Controlled Unclassified Information (June 2018)

- This publication is intended to help organizations develop assessment plans and conduct efficient, effective, and cost-effective assessments of the CUI security requirements defined in Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

- https://csrc.nist.gov/CSRC/media/Publications/sp/800-171a/draft/documents/sp800-171a-draft-20180220.pdf

NIST Special Publication 800-171A

3.10.1	SECURITY REQUIREMENT Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.10.1[a] *for a facility that contains CUI, authorized individuals allowed physical access are identified.*
	3.10.1[b] *physical access to an organizational system that processes, stores, or transmits CUI is limited to authorized individuals.*
	3.10.1[c] *physical access to equipment that processes, stores, or transmits CUI is limited to authorized individuals.*
	3.10.1[d] *physical access to operating environments where CUI is processed, stored, or transmitted is limited to authorized individuals.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access authorizations; security plan; authorized personnel access list; authorization credentials; physical access list re and associated documentation; other relevant d Interview: [*SELECT FROM:* Personnel with physical access with physical access to system facility; personn responsibilities]. Test: [*SELECT FROM:* Organizational processes for physica supporting or implementing physical access authoriz
	DISCUSSION ON SECURITY REQUIREMENT 3.10.1

- How to assess
- Explanation of the requirements

3.10.1	SECURITY REQUIREMENT Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.
	DISCUSSION This requirement applies to organizational employees, individuals with permanent physical access authorization credentials, and visitors. Authorization credentials include, for example, badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed consistent with applicable laws, directives, policies, regulations, standards, procedures, and guidelines. This requirement applies only to areas within facilities that have not been designated as publicly accessible. Limiting physical access to equipment may include, for example, placing equipment in locked rooms or other secured areas and allowing access to authorized individuals only, and placing equipment in locations that can be monitored by organizational personnel. Computing devices, external hard disk drives, networking devices, monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of equipment.

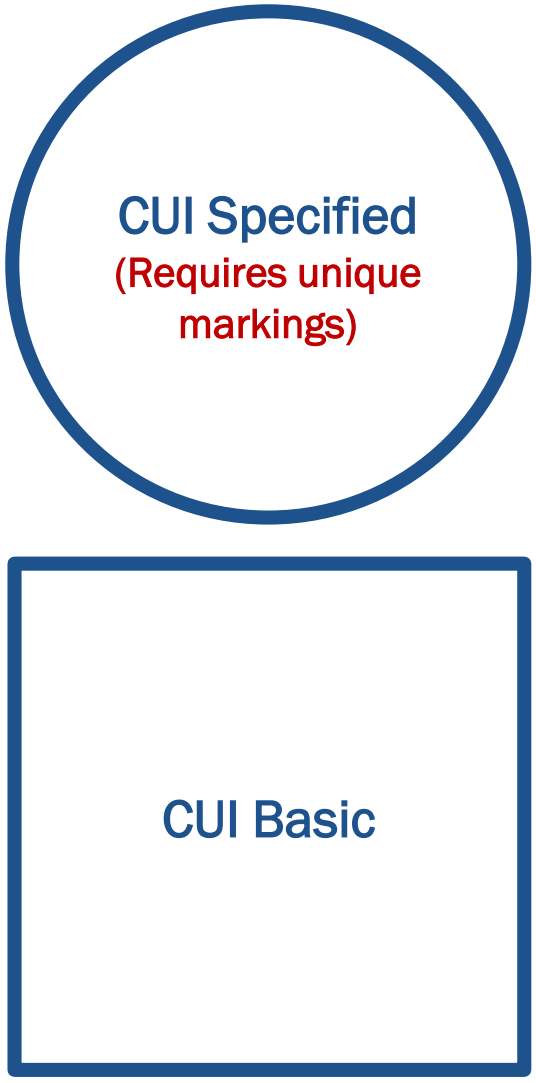
Federal Acquisition Regulation (FY19)

"This FAR rule is necessary to ensure uniform implementation of the requirements of the CUI program in contracts across the government, thereby avoiding potentially inconsistent agency-level action." –Unified Agenda

Public Comment
Open: December 2018 (Est.)
Close: February 2019 (Est.)

https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=201804&RIN=9000-AN56

CUI Basic and CUI Specified



Laws, Regulations, or Government-wide policies require specific protections. For example:

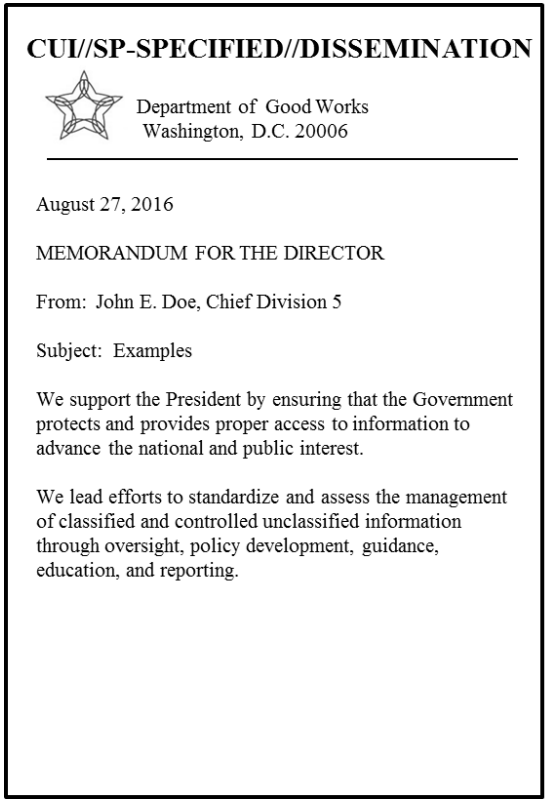
- Unique markings
- Enhanced physical safeguards
- Limits on who can access the information

Laws, Regulations, or Government-wide policies **DO NOT** require specific protections.

Marking CUI: Banner Marking

The CUI Banner Marking may include up to three elements:

- The CUI Control Marking (mandatory) may consist of either the word "CONTROLLED" or the acronym "CUI."
- CUI Category or Subcategory Markings (mandatory for CUI Specified). CUI Control Markings and Category Markings are separated by two forward slashes (//). When including multiple categories or subcategories in a Banner Marking they are separated by a single forward slash (/).
- Limited Dissemination Control Markings. CUI Control Markings and Category Markings are separated from Limited Dissemination Controls Markings by a double forward slash (//).



CUI//SP-SPECIFIED//DISSEMINATION

Department of Good Works
Washington, D.C. 20006

August 27, 2016

MEMORANDUM FOR THE DIRECTOR

From: John E. Doe, Chief Division 5

Subject: Examples

We support the President by ensuring that the Government protects and provides proper access to information to advance the national and public interest.

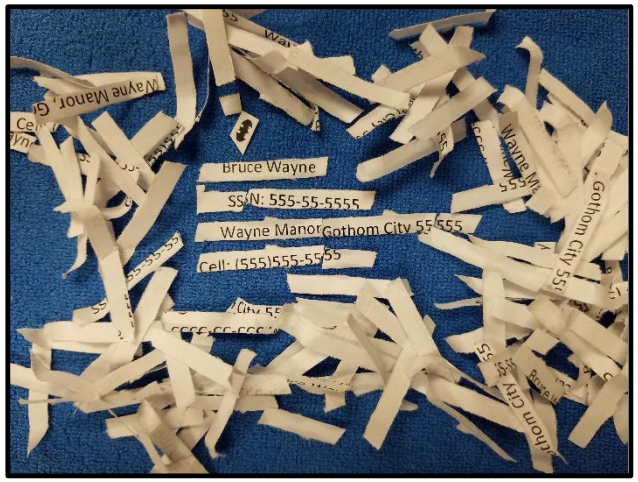
We lead efforts to standardize and assess the management of classified and controlled unclassified information through oversight, policy development, guidance, education, and reporting.

Portion Marking = Best Practice

Destruction

- Unreadable, Indecipherable, and Irrecoverable
- NIST SP 800-88, Guidelines for Media Sanitization
- Other methods acceptable with verification and documentation
  - Multi-phased destruction

NOT APPROVED



Destroy paper using cross cut shredders that produce particles that are 1mm by 5 mm.

APPROVED

Approved Destruction Methods

- Signage can be placed on equipment to indicate that it is approved for CUI destruction.

General Safeguarding Policy

- Agencies must safeguard CUI at all times in a manner that minimizes the risk of unauthorized disclosure while allowing for access by authorized holders.
  - For categories designated as CUI Specified, personnel must also follow the procedures in the underlying law, regulation, or Government-wide policy that established the specific category or subcategory involved.

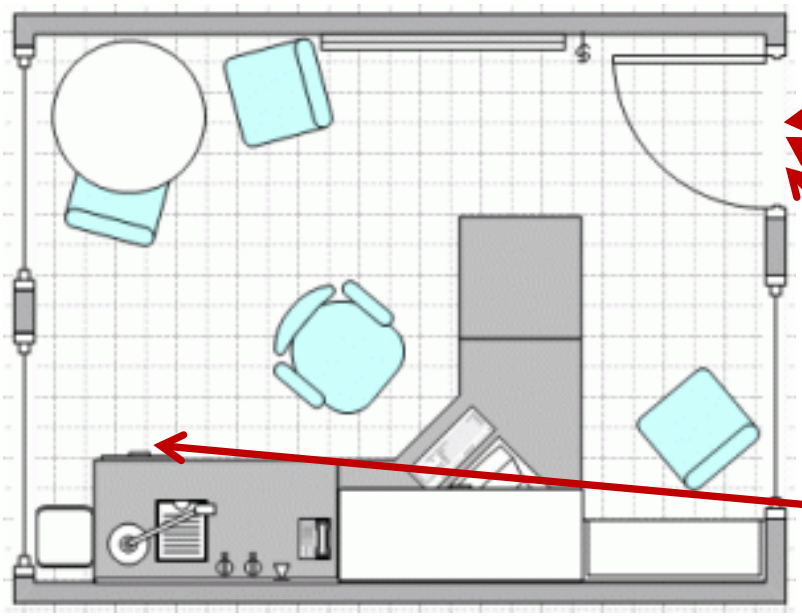
- Safeguarding measures that are authorized or accredited for classified information are sufficient for safeguarding CUI.

Controlled Environments (physical)

Controlled environment is 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.

- Going beyond gates, guns, and guards: Internal security
- Establish a controlled environment that prevents access
- Assess:
  - ✓ Who works in the space?
  - ✓ Who has access to the space (cleaning, maintenance, general workforce, etc.) during and after business hours?
  - ✓ Do individual workspaces (cubes & offices) have adequate safeguards to prevent access (locking cabinets, drawers, or overhead bins)?
  - ✓ Suitable for sensitive discussions?
  - ✓ Clean desk policy? Is CUI secured when not in use? Enforcement or Verification?
  - ✓ Open storage of CUI? Measures to prevent or detect access?
  - ✓ Visitor escort policy?

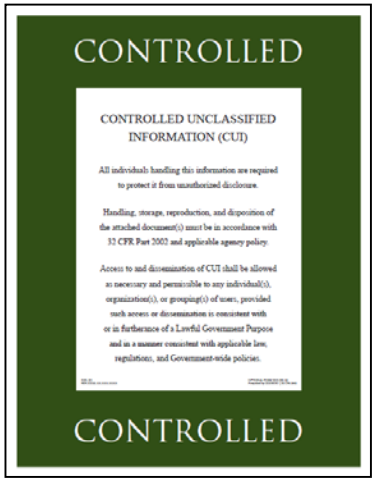
How to prevent access

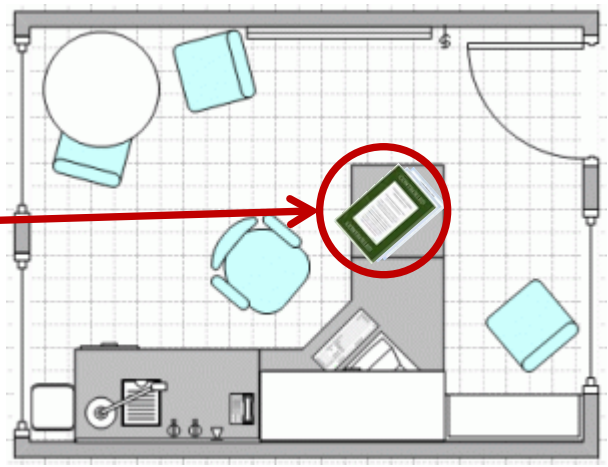


Electronic Access Control Device

Mechanical, Push Button, Access Control Lock

Key Lock



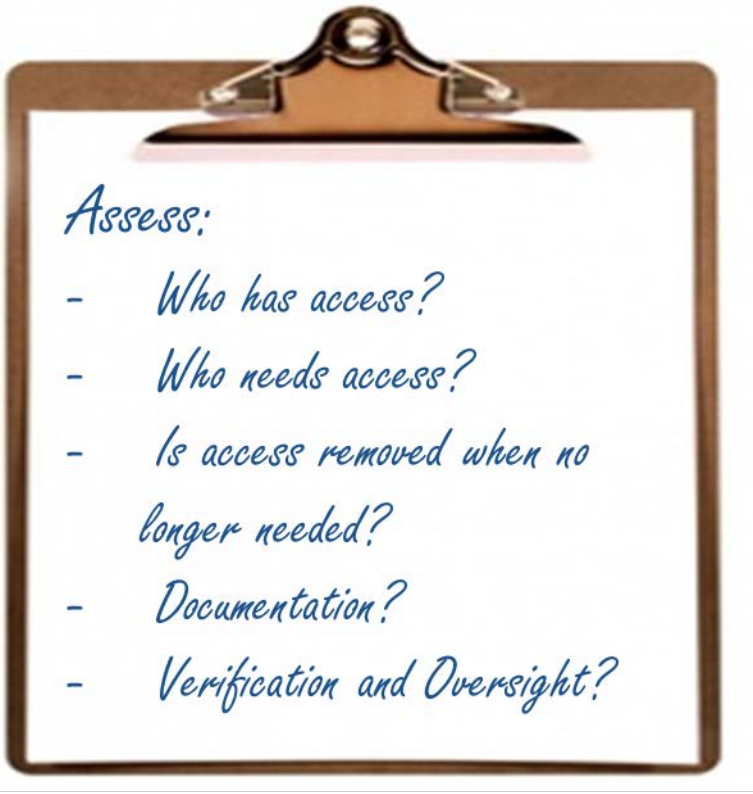


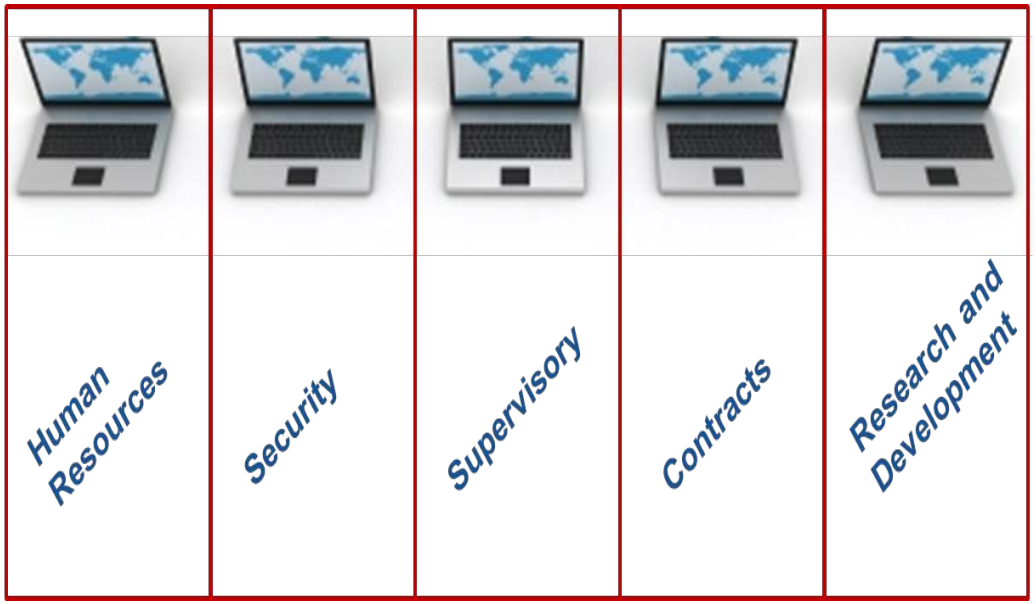
Enter Password to Unlock the Computer

Controlled Environments (Electronic)

Limit and control access to CUI within the workforce by establishing electronic barriers.

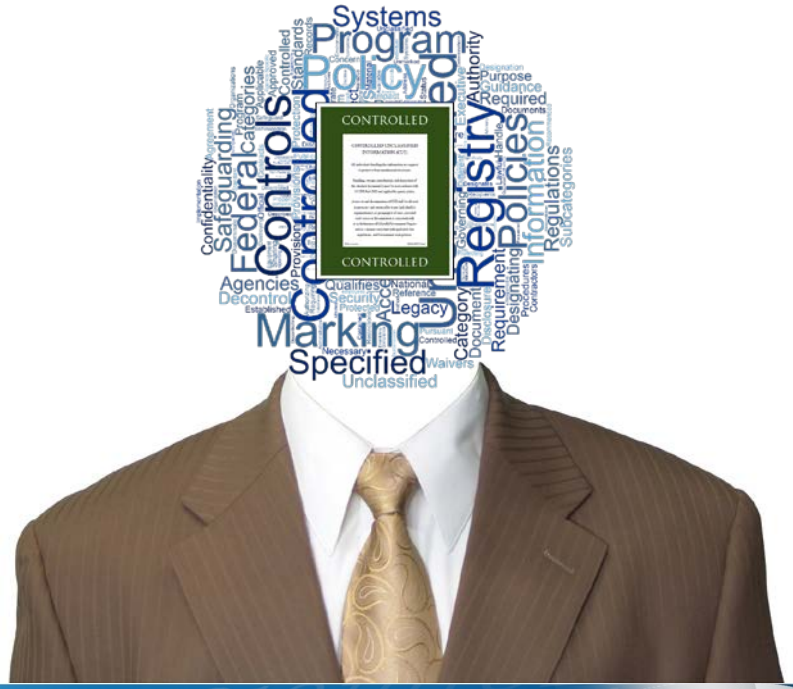
- Dedicated network drives, SharePoint sites, intranet sites



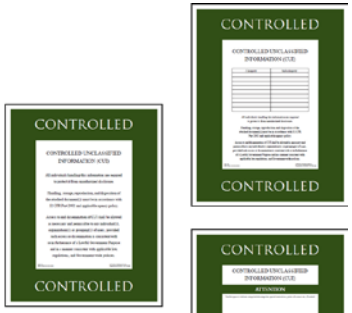


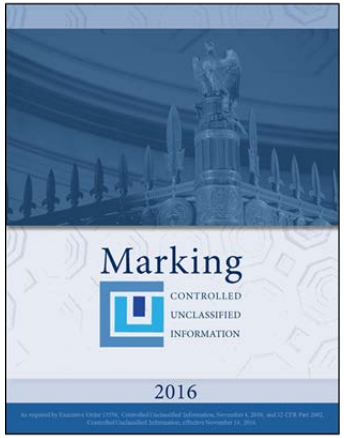
Other Considerations

- Personal Devices
  - Photographic and recording capabilities?
- Telework
  - Work arounds (email to personal account, perform the work, then send back)?
- Bring/Use your own device
  - Virtual desktops?
  - Policy?
  - Risks?
- USB Drives
  - Allowable?
  - Security?
- Travel
  - Policy and training?
- Separation and transfers
- Insider Threats



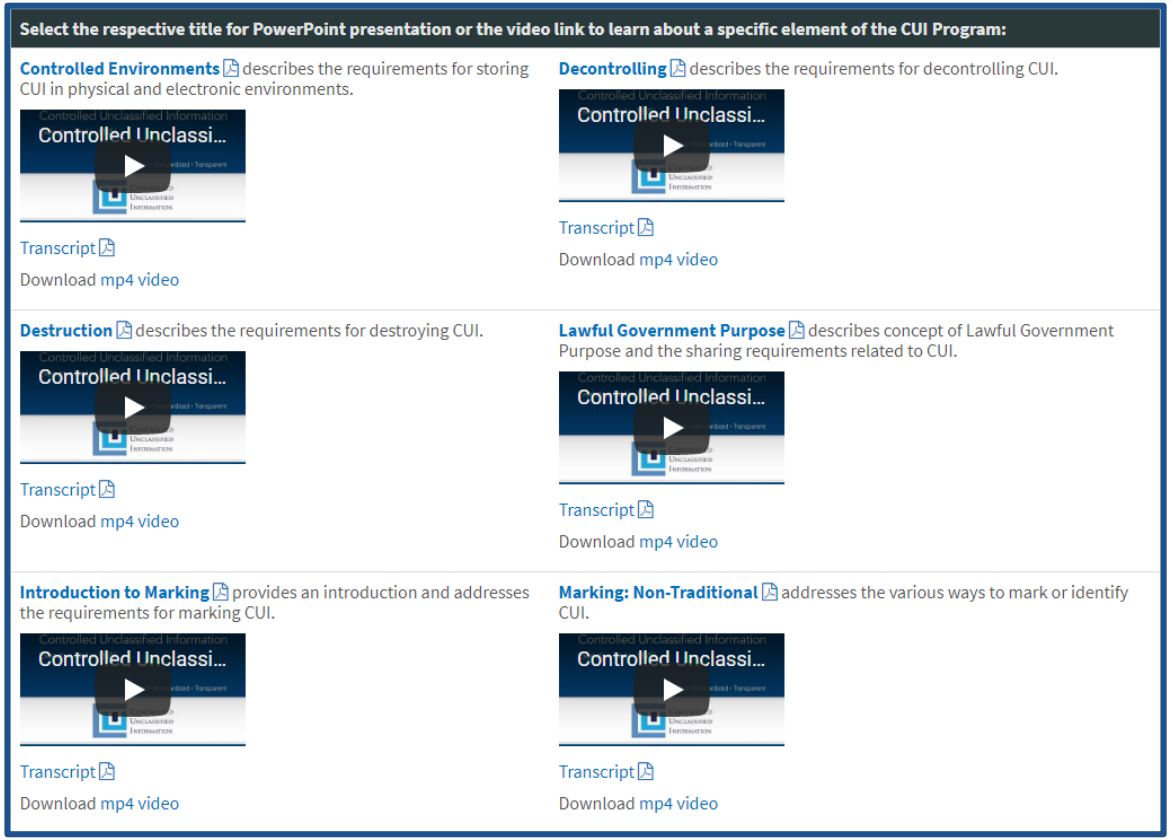
Products to assist





Our Website: Training Videos

- Controlled Environments
- Decontrolling
- Destruction
- Lawful Government Purpose
- Intro to Marking
- Marking (non-traditional)
- Unauthorized Disclosures
- **New Video:** CUI Overview



Training Tools Downloads Include:

- Video File(mp4)
- Transcript (pdf)
- PowerPoint w/ talking points (pdf)

New: CUI Overview Video (11 Minutes)

What to report

CUI incidents include but are not limited to:

- Improper storage of CUI
- Actual or suspected mishandling of CUI
- When unauthorized individuals gain access to CUI (physical or electr
- Unauthorized release of CUI (to public facing websites or to unauthor individuals)
- Suspicious behavior from the workforce (Insider Threats)
  - General disregard for security procedures
  - Seeking access to information outside the scope of current responsibilities
  - Attempting to enter or access to sensitive areas (where CUI is stored, discusse processed)

Follow your agency policy and procedures regarding how to report incid

What is CUI?

Information that requires protection.

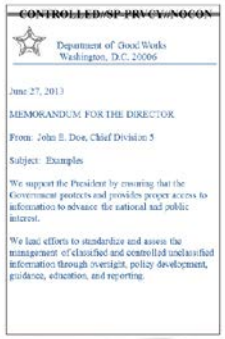
Decontrol and Marking

or strike all markings on decontrolled

ed
sed
ted

gency policy to remove or strike CUI only

age,
page, or
age of any attachment.



15

How to Send CUI in Packages and Mail

CUI may be shipped through:

- Interagency mail systems
- United States Postal Service
- Commercial Delivery Services
- Automated Tracking is a best practice

DO NOT Place Markings on Packages or Envelops!

CUI Basic and CUI Specified

CUI Specified
(Requires unique markings)

Laws, Regulations, or Government-wide policies require specific protections. For example:

- Unique markings
- Enhanced physical safeguards
- Limits on who can access the information

CUI Basic

Laws, Regulations, or Government-wide policies DO NOT require specific protections.

4

gns for approved destruction equipment and methods

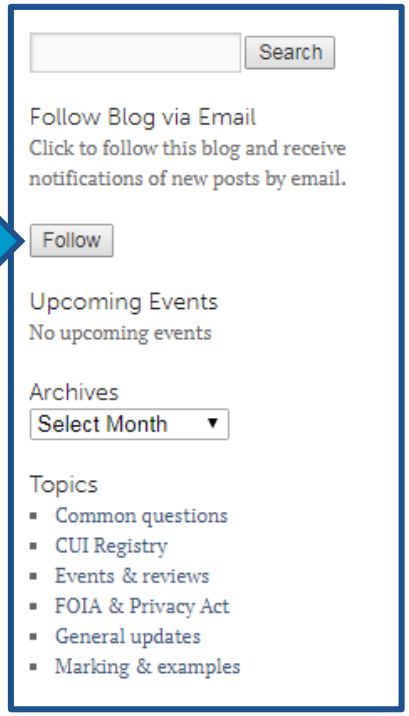
- Never use trash cans or recycling bins to dispose of CUI

14

CONTROLLED UNCLASSIFIED INFORMATION

CUI Blog = Updates Available

- FAQs
- Next Webinar:
  - ✓ August 15, 2018
  - ✓ 1-3 EDT



Questions?


CONTROLLED
CONTROLLED UNCLASSIFIED INFORMATION (CUI)
All individuals handling this information are required to protect it from unauthorized disclosure.
Handling, storage, reproduction, and disposition of the attached document(s) must be in accordance with 32 CFR Part 2002 and applicable agency policy.
Access to and dissemination of CUI shall be allowed as necessary and permissible to any individual(s), organization(s), or grouping(s) of users, provided such access or dissemination is consistent with or in furtherance of a Lawful Government Purpose and in a manner consistent with applicable law, regulations, and Government-wide policies.
CONTROLLED
Systems
Program
Policy
Federal
Controlled
Unclassified
Information
Safeguarding
Controls
Registry
Policies
Marking
Specified
Agencies
Decontrol
Qualifies
Security
Protected
Legacy
Authority
Required
Guidance
Purpose
Designation
Executive
Standards
Records
Controlled
Approved
Applicable
Categories
Agreement
Confidentiality
Regulations
Subcategories
Handle
Lawful
Designates
Recipients
Governing
Protecting
Designating
Requirement
Document
Disclosure
Category
Procedures
Contractors
Waivers
Necessary
Pursuant
Controlled
Unclassified
National
Reference
Established
Concern
Unmarked
Material
Status
Impact
Documents
Provisions
Protection
Safeguard
Contracts
Dissemination
Destroying
Official
Described
Sharing
Restrictions
Decontrolling