

Controlled Unclassified Information

Implementation and Features

Shared • Standardized • Transparent



Information Security Oversight Office (ISOO)

Outline

- Why protect CUI?
- Impacts to National Security
- Existing Agency Policy and Procedure
- Protection Today
- An Information Security Reform
 - Protection defined
 - What we protect (CUI Registry)
 - How we protect (32 CFR 2002)
 - NIST SP 800-171
 - Federal Acquisition Regulation
 - Oversight Approach
 - Phased Implementation
- Features

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
- The loss or improper safeguarding of CUI has a direct impact on national security

Impacts to National Security

- The OPM Data breach is a **significant CUI incident**
 - Personnel files of 4.2 million former and current government employees.
 - Security clearance background investigation information on 21.5 million individuals.

OPM **failed to implement** a longstanding requirement to use **multi-factor** authentication for network access.

“The intelligence and counterintelligence value of the stolen background investigation information for a foreign nation cannot be overstated, nor will it ever be fully known.”

- The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation
September 7, 2016.

Government expense (to notify and protect those impacted) = \$350 Million

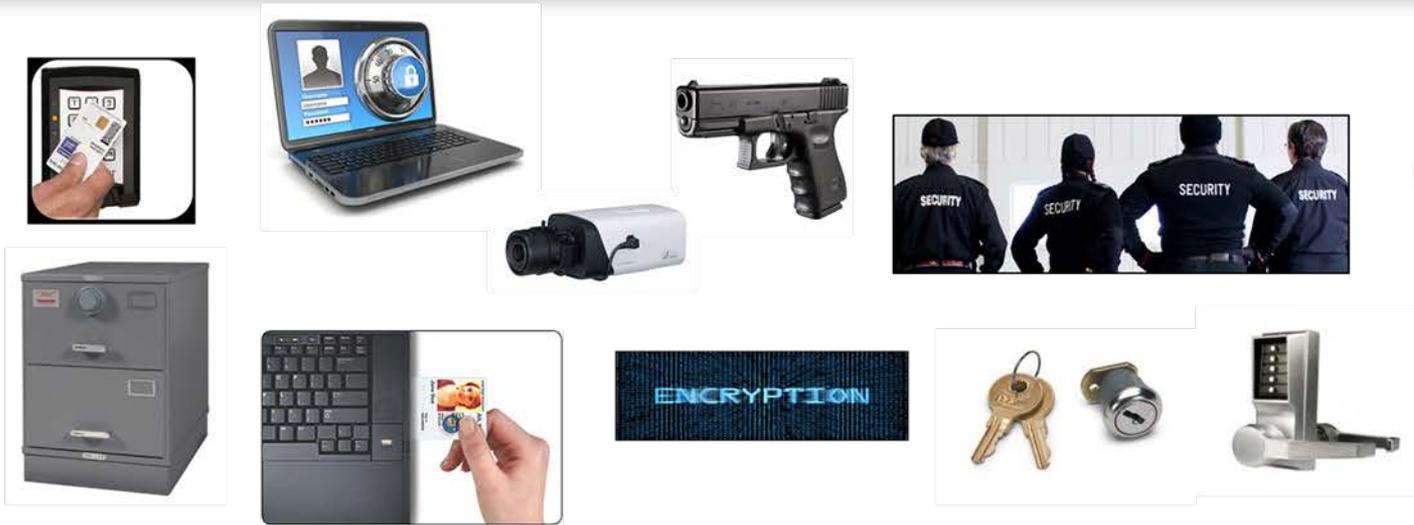
How did we get here?

- **Laws, Regulations, and Government-wide policies (LRGWP) identified what to protect but failed to say how.**
- Agencies took steps to define protection through the issuance of policy and procedure
 - Physical
 - Electronic
 - Dissemination (sharing)
 - Destruction
- **Lack of oversight over sensitive information programs**

Agency Policy and Procedure created:

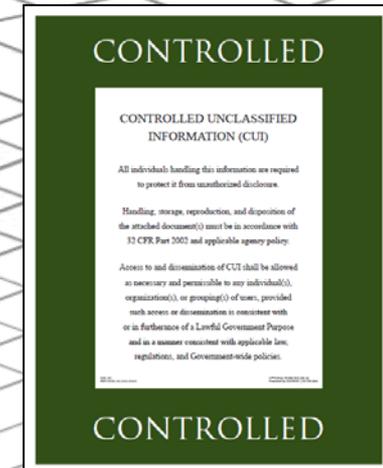
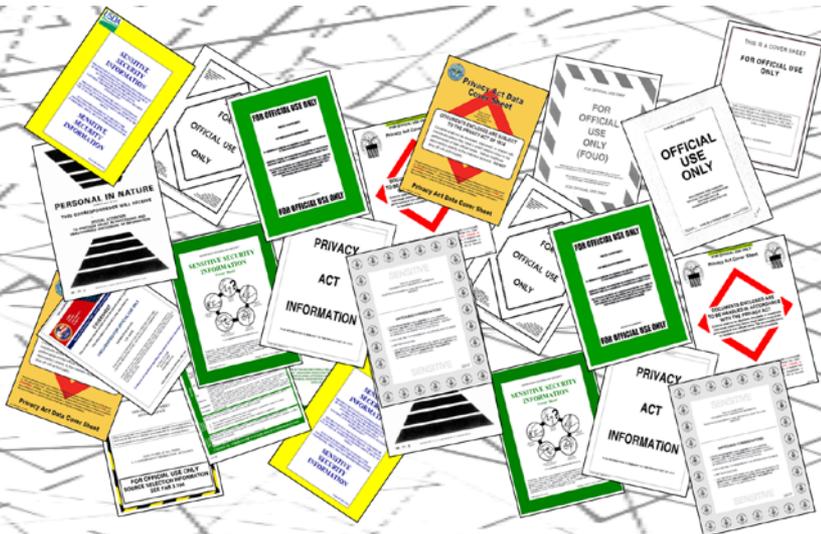
- **Inefficient patchwork system** with more than 100 different policies and markings across the executive branch
- **Inconsistent** marking and safeguarding of documents
- **Unnecessarily restrictive** dissemination policies
- **Impediments** to authorized information sharing

Protection today



Information Security Reform

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



Protection is defined under the CUI Program

The “best” (or most agreed upon) methods

www.archives.gov/cui

Controlled Unclassified Information (CUI)

Home > CUI

Established by Executive Order 13556, the Controlled Unclassified Information (CUI) program standardizes the way the Executive branch handles unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies. [Learn About CUI](#)

Registry

The CUI Registry is the authoritative source for guidance regarding CUI policies and practices.

Search the Registry:

Access Registry by

- Category-Subcategory
- Executive Order 13556
- 32 CFR Part 2002 (Implementing Regulation)
- CUI Notices
- Additional Information
- CUI Glossary

Under Development - Registry

- Marking Handbook
- Markings
- Limited Dissemination
- Decentral

Training

Learn about training developed by the Executive Agent for CUI users

- CUI Training Modules

Oversight

Learn about CUI oversight requirements and tools

- CUI Reports

CUI Registry

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 VISCUDO
MAUR ROULE
Information Security Oversight Office
Federal and Security Administration

GARY GUSSANE
Assistant for Defense Activities
within the Department of Defense

Available free of charge from:
<http://nvl.nist.gov/sp800-171/>

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 request a designated agency representative for CUI.

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

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

ARCHIVES AND RECORDS ADMINISTRATION

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

Department of Commerce
Kenney Pittzker, Secretary
Computer Security Division
Standards and Technology
Technology and Director

December 2016

63336 Federal Register

List of Subjects in: Administrative procedures, Archives, Controlled Unclassified Information, Freedom of information, the Statistic Act, reference, national security, National Open government.

For the reasons in this preamble, NARA is Chapter XX by add as follows:

PART 2002—CONTROLLED UNCLASSIFIED INFORMATION

Subpart A—General

2002.1 Purpose and scope

2002.2 Definitions

2002.6 CUI Elements

2002.8 Roles and responsibilities

Subpart B—Key Elements

2002.10 The CUI in the 2002.12 CUI categories

2002.14 Subcategories

2002.16 Accounting

2002.18 Declassification

2002.20 Marking

2002.22 Limited dissemination

2002.24 Agency self-inspection

Subpart C—CUI Program

2002.30 Information

2002.32 CUI owner

2002.34 Transmittal

2002.36 Legacy systems

2002.38 Whistleblowers

2002.44 CUI and declassification

2002.46 CUI and the Statistic Act

2002.48 CUI and the Privacy Act

2002.50 Challenges

2002.52 Dispute resolution

2002.54 Misuse of CUI

2002.56 Sanctions

Appendix A to Part 2002—Authority: E.O. 13526 and Comp. sup. 801

Subpart A—General

§ 2002.1 Purpose and scope

(a) This part describes the Controlled Unclassified Information (CUI) Program and establishes the categories, subcategories, and elements that constitute CUI. (b) The CUI Program is the mechanism by which information that requires protection under laws, regulations, or Government-wide policies, but that does not qualify as classified under Executive Order 13526, is designated as CUI. (c) This part does not apply to information that is classified under 5 U.S.C. 552(a).

§ 2002.2 Definitions.

As used in this part: (a) Agency is the Federal agency, executive agency, executive branch

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

Controlled Unclassified Information (CUI)

Home > CUI

Established by Executive Order 13556, the Controlled Unclassified Information (CUI) program standardizes the way the Executive branch handles unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies. [Learn About CUI](#)



Use the CUI Logo
Contact Us

News and Notices

- September 14, 2016 - 32 CFR Part 2002 has been published.
- September 14, 2016 - CUI Notice 2016-01: Implementation Guidance has been issued.

Under Development - Registry

- Marking Handbook
- Markings
- Limited Dissemination
- Decontrol

Registry



The CUI Registry is the authoritative source for guidance regarding CUI policies and practices.

Search the Registry:

Access Registry by

- Category-Subcategory

Policy and Guidance

- Executive Order 13556
- 32 CFR Part 2002 (Implementing Regulation)
- CUI Notices

Additional Information

- CUI Glossary

Training



Learn about training developed by the Executive Agent for CUI users

- CUI Training Modules

Oversight



Learn about CUI oversight requirements and tools.

- CUI Reports

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)

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 assistance in the handling of information that requires protection under laws, regulations, or Government-wide policies, but that does not qualify as classified under Executive Order 13526.

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

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

12) Establishes a mechanism by which authorized holders (both inside and outside the agency) can contact a designated agency representative for assistance in the handling of information that requires protection under laws, regulations, or Government-wide policies, but that does not qualify as classified under Executive Order 13526.



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

63336 Federal

List of Subjects in 32

Administrative procedure, Archives, Controlled unclassified information, Freedom of information, the Sunshine Act, Information security, National security, Open government, etc.

For the reasons of this preamble, NARA is amending Chapter XX by adding the following:

PART 2002—CONT

UNCLASSIFIED INF

Subpart A—General

2002.1 Purpose and

2002.2 Incorporation

2002.3 Definitions.

2002.6 CUI Executive

2002.8 Roles and res

Subpart B—Key Element

Program

2002.10 The CUI Re

2002.12 CUI catalog

2002.14 Safeguarding

2002.16 Accessing a

2002.18 Decontrol

2002.20 Marking.

2002.22 Limitations

agency CUI policy.

2002.24 Agency self

Subpart C—CUI Prog

2002.30 Education a

2002.32 CUI cover a

2002.34 Transferring

2002.36 Legacy mat

2002.38 Waivers of C

2002.44 CUI and dis

2002.46 CUI and the

2002.48 CUI and the

Procedure Act (A)

2002.50 Challenges

information as CUI

2002.52 Dispute res

2002.54 Misuse of C

2002.56 Sanctions i

Appendix A to Part

Authority: E.O. 13526

2010 Comp., pp. 287.

Subpart A—Genera

§ 2002.1 Purpose of

(a) This part desc

branch's Controlled

Information (CUI) P

Program) and estab

designating, handli

information that qui

(b) The CUI Prog

way the executive

information that requires protection

under laws, regulations, or Government-

wide policies, but that does not qualify

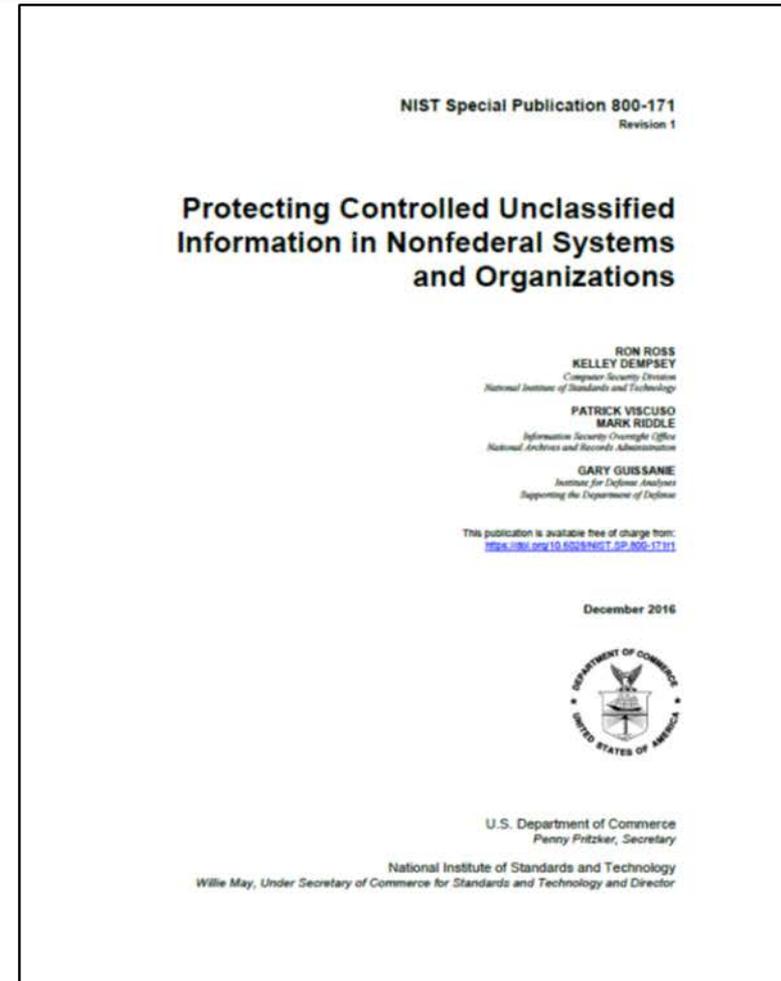
as classified under Executive Order

(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)

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



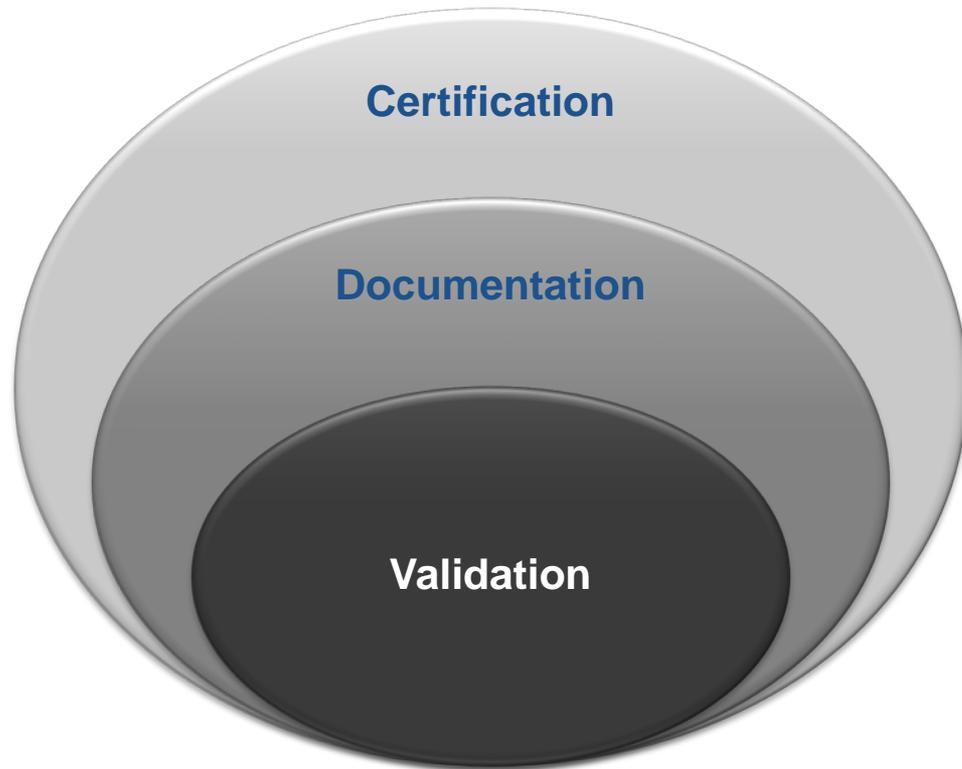
Federal Acquisition Regulation (FY18)

Will standardize the way the Executive branch conveys safeguarding guidance



Oversight Approach

- Based on CUI, quantity, mission/purpose, and existing practices
- Evaluation and assessment based on CUI Program standards



Phased Implementation

- Within the Executive branch and within Agencies
- **CUI practices and Legacy practices will exist at the same time.**
 - Legacy practices will be phased out as agencies implement
- Implementation includes:
 - Program Management
 - Policy
 - Training
 - Physical Safeguarding
 - Incidents
 - Systems
 - Self Inspection
 - **Contracts and agreements (likely to be last phase of implementation)**

**Executive Branch
Implementation = 3-5 years**

Features

- **Basic and Specified CUI**
- **Limitations on Applicability**
- **Safeguarding**
 - Controlled Environments (physical)
 - Controlled Environments (electronic)
- **Moderate baseline**
- **Marking (Banner & Limited Dissemination Controls)**
 - Bulk or Alternative Markings
 - Legacy and Markings
- **Destruction (including multi-phased)**
- **Products to Assist**
- **Tools you can use**

Two types of CUI: Basic and Specified

- CUI Basic = LRGWP identifies an information type and says protect it.

Examples include: Agriculture, Ammonium Nitrate, Water Assessments, Emergency Management, Bank Secrecy, Budget, Comptroller General, Geodetic Product Information, Asylee, Visas, Information Systems Vulnerabilities, Terrorist Screening, Informant, Privilege, Victim, Death Records

- CUI Specified = LRGWP identifies an information type and says to protect it, and also includes one or more specific handling standards for that information.

Examples include: Sensitive Security Information, Student Records, Personnel, Source Selection, Nuclear, Safeguards Information, NATO Restricted, NATO Unclassified, Federal Grand Jury, Witness Protection, DNA, Criminal History Records, Financial Records, Export Control, Protected Critical Infrastructure Information, Controlled Technical Information

Limitations on applicability

Limitations on applicability of agency CUI policies

- Agency policies pertaining to CUI do not apply to entities outside that agency unless the CUI Executive Agent approves their application and publishes them in the CUI Registry.
- Agencies may not levy any requirements in addition to those contained in the Order, this Part, or the CUI Registry when entering into contracts, treaties, or other agreements about handling CUI by entities outside of that agency.

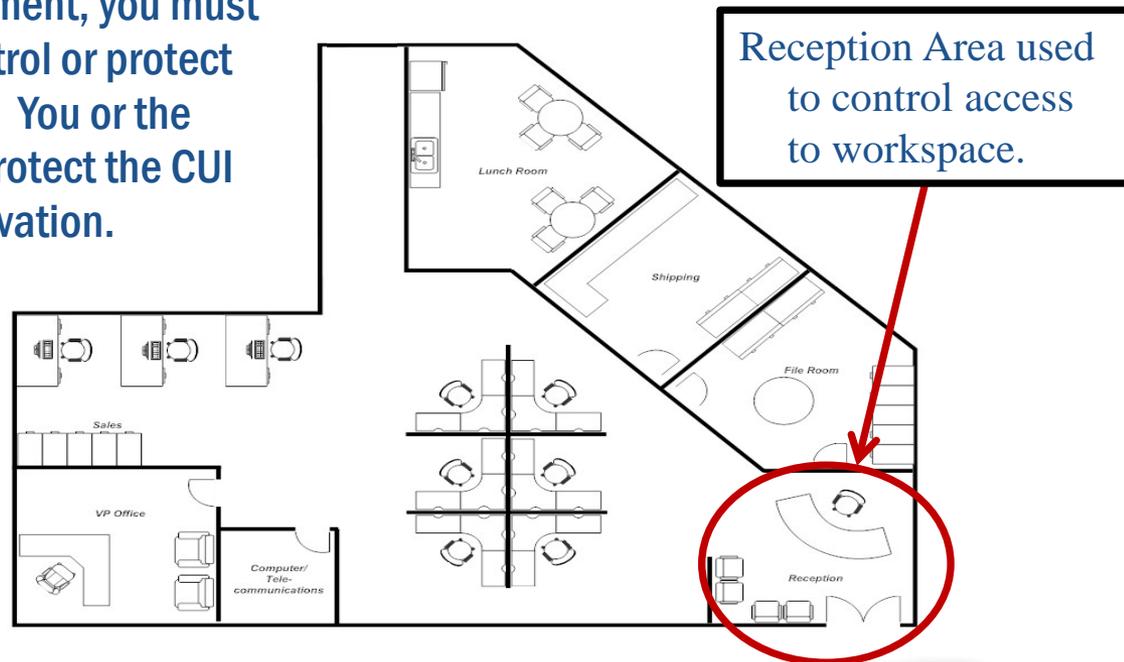
General Safeguarding Policy

- 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.

- When outside a controlled environment, you must keep the CUI under your direct control or protect it with **at least one physical barrier**. You or the physical barrier must reasonably protect the CUI from unauthorized access or observation.



Controlled Environments (Electronic)

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

- Dedicated network drives, SharePoint sites, intranet sites
- Assess who has a lawful government purpose for access
 - **Mission or function**



System Requirements: Moderate

- Systems that store or process CUI must be protected at the Moderate Confidentiality Impact Value.
 - FIPS PUB 199 & 200
 - NIST SP-800-53 (Risk Based Tailoring)

Government
Systems



Marking CUI

- Agencies must uniformly and conspicuously apply CUI markings to all CUI prior to disseminating it.
- The CUI banner marking must appear, at a minimum, at the top center of each page containing CUI.
- **Purpose is to inform or alert recipients/users that CUI is present and of any special handling requirements.**

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.

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

Limited Dissemination Controls

No Foreign Dissemination	Information may not be disseminated in any form to foreign governments, foreign nationals, foreign or international organizations, or non-US citizens.	NOFORN
Federal Employees Only	Dissemination authorized only to (1) employees of United States Government Executive branch departments and agencies (as agency is defined in 5 U.S.C. 105), or (2) armed forces personnel of the United States or Active Guard and Reserve (as defined in 10 USC 101).	FED ONLY
Federal Employees and Contractors Only	Dissemination authorized only to (1) employees of United States Government Executive branch departments and agencies (as agency is defined in 5 U.S.C. 105), (2) armed forces personnel of the United States or Active Guard and Reserve (as defined in 10 USC 101), or (3) individuals or employers who enter into a contract with the United States (any department or agency) to perform a specific job, supply labor and materials, or for the sale of products and services, so long as dissemination is in furtherance of that contractual purpose.	FEDCON
No Dissemination to Contractors	No dissemination authorized to individuals or employers who enter into a contract with the United States (any department or agency) to perform a specific job, supply labor and materials, or for the sale of products and services. Note: This dissemination control is intended for use when dissemination is not permitted to federal contractors, but permits dissemination to State, local, or tribal employees.	NOCON
Dissemination List Controlled	Dissemination authorized only to those individuals, organizations, or entities included on an accompanying dissemination list. Note: Use of this limited dissemination control supersedes other limited dissemination controls, but cannot supersede dissemination stipulated in federal law, regulation, or Government-wide policy.	DL ONLY
Authorized for release to certain nationals only	Information has been predetermined by the designating agency to be releasable or has been released only to the foreign country(ies)/international organization(s) indicated, through established foreign disclosure procedures and channels. It is NOFORN to all foreign country(ies)/international organization(s) not indicated in the REL TO marking. Note: See list of approved country codes for use with REL TO here. USA must always appear first when using REL TO followed by additional permitted trigraph country codes in alphabetical order.	REL TO XXXX
Display Only	Information is authorized for disclosure to a foreign recipient, but without providing the foreign recipient with a physical copy for retention, regardless of medium to the foreign country(ies)/international organization(s) indicated, through established foreign disclosure procedures and channels.	DISPLAY ONLY

Marking CUI with Dissemination Controls

Dissemination Controls can be applied to **limit sharing** or to **convey requirements** found in Laws, Regulations, or Government wide policies.

The image displays three overlapping memorandum templates, each with a different dissemination control marking. Each template includes a star icon, the text 'Department of Good Works, Washington, D.C. 20006', a date of 'June 27, 2013', and the following fields: 'MEMORANDUM FOR THE DIRECTOR', 'From: John E. Doe, Chief Division 5', and 'Subject: Examples'. The body text of each memorandum is: '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.'

CONTROLLED//FED ONLY

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.

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.

CONTROLLED//SP-PCII//NOFORN

Department of Good Works
Washington, D.C. 20006

June 27, 2013

MEMORANDUM FOR THE DIRECTOR

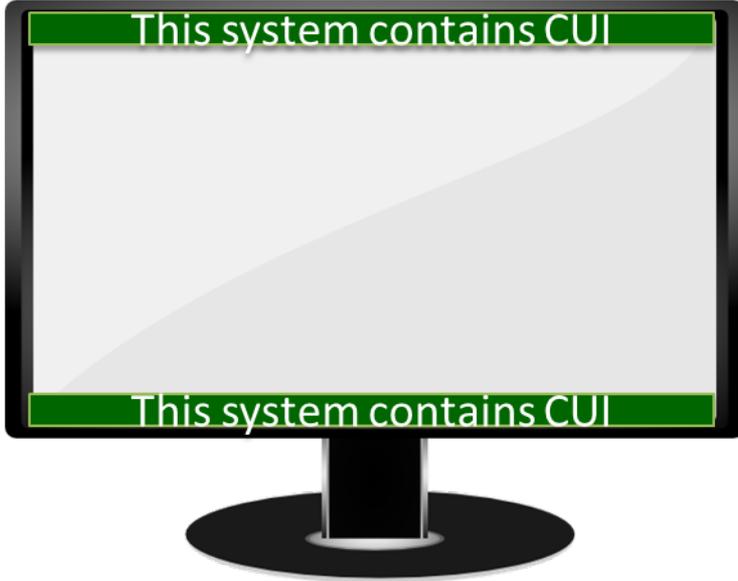
From: John E. Doe, Chief Division 5

Subject: Examples

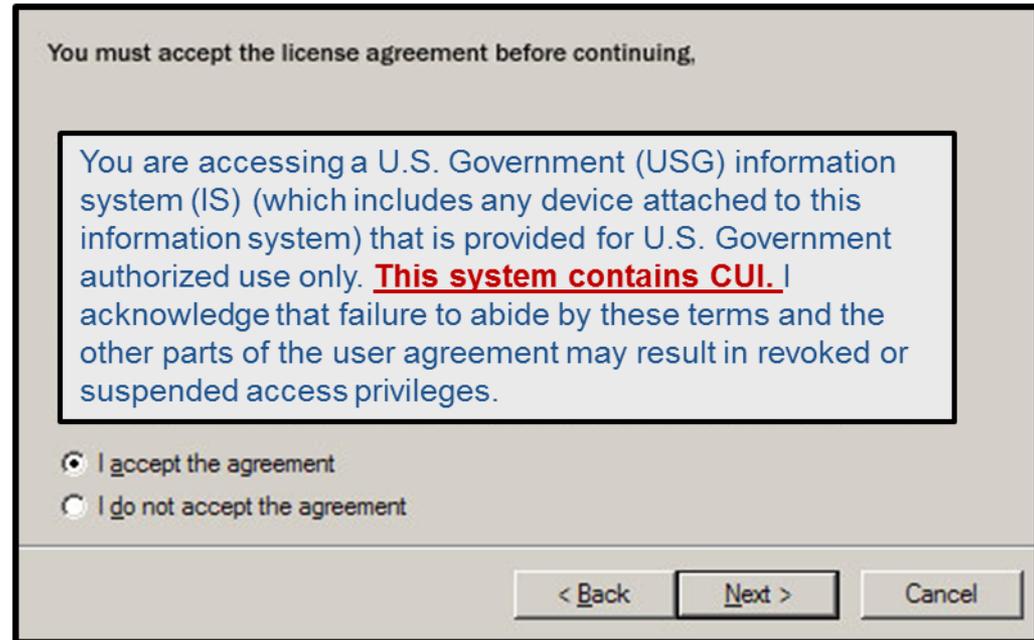
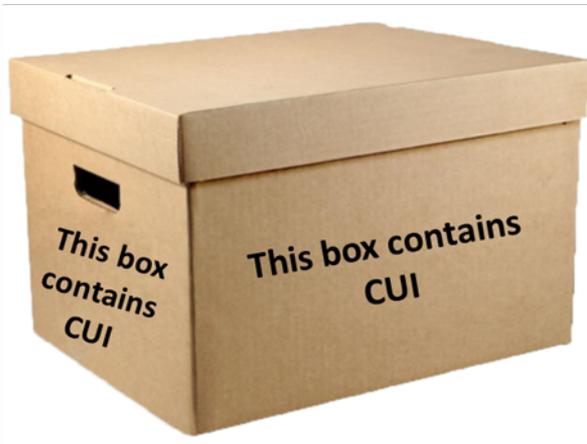
We support the President by ensuring that the Government protects and provides proper access to information to advance the national and public interest.

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

Bulk & System Markings



Agencies may authorize or require the use of alternate CUI indicators on IT systems, websites, browsers, or databases through agency CUI policy. These may be used to alert users of the presence of CUI where use of markings has been waived by the agency head.



Legacy Information and Markings



Legacy Information is unclassified information that an agency marked as restricted from access or dissemination in some way, or otherwise controlled, prior to the CUI Program.

All legacy information is not automatically CUI. Agencies must examine and determine what legacy information qualifies as CUI

Discontinue all use of legacy markings

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.

Destruction

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

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

NOT APPROVED



APPROVED

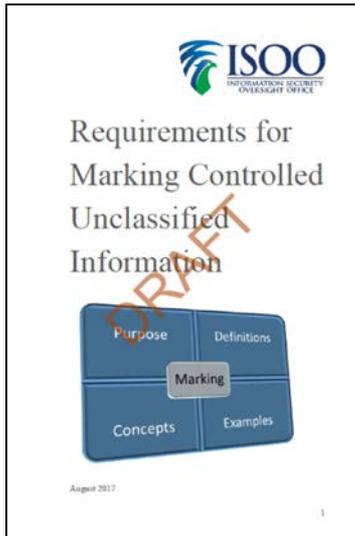
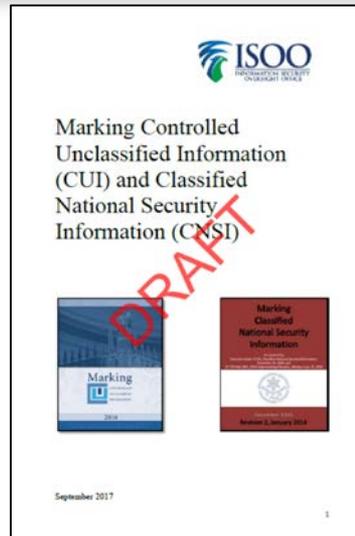


Products to assist



- **Marking Book**
 - <https://www.archives.gov/files/cui/20161206-cui-marking-handbook-v1-1.pdf>
- **YouTube Video**
 - <https://www.youtube.com/watch?v=OvOHwezHww>
- **CUI Marking Trifold Brochure**
 - <https://www.archives.gov/files/cui/documents/2016-marking-trifold-v1.pdf>
- **CUI Audio, Photography and Video Markings Brochure**
 - <https://www.archives.gov/files/cui/documents/2017-Audio-Photo-Video-bifold-v1.pdf>

New and Coming Soon!



CUI BLOG

Training Videos:

- Marking Requirements
- Marking Options (coversheets)
- Controlled Environments
- Decontrol
- Lawful Government Purpose
- Destruction

Questions?

