

# Controlled Unclassified Information

*The Program, Implementation, and Features*

Shared • Standardized • Transparent



Information Security Oversight Office (ISOO)

# Outline

- What is CUI?
- Laws, Regulations, and Government-wide policies (LRGWP)
- An Information Security Reform
- Contracts, Legacy Information, Resources



# What is Controlled Unclassified Information (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 of information that the Executive branch protects. The CUI Registry can be found at:

<https://www.archives.gov/cui>

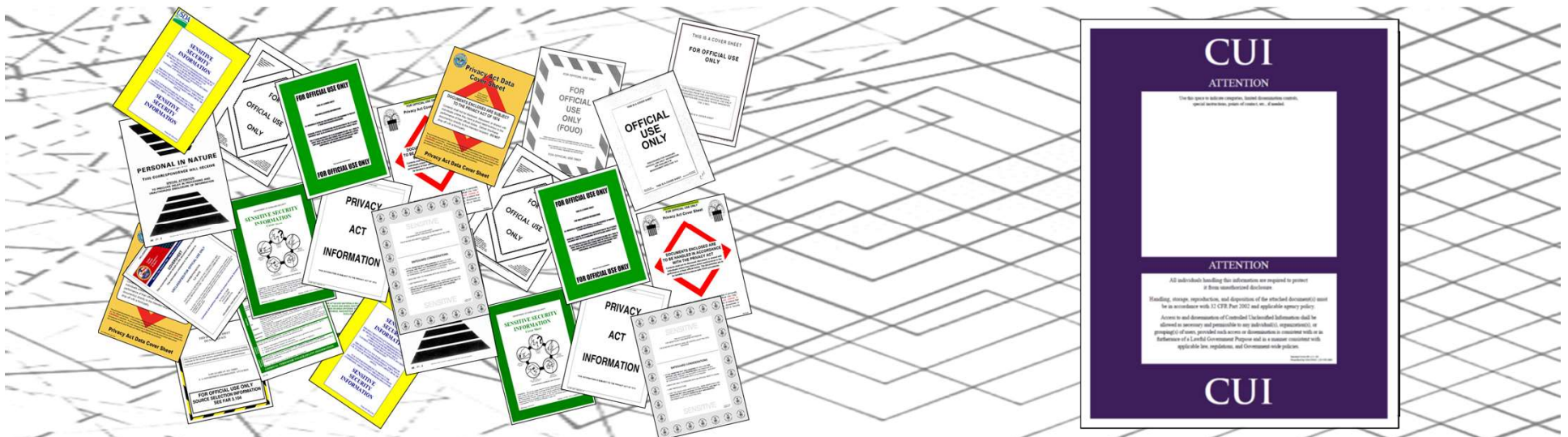
# CUI includes, but is not limited to:

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



# Information Security Reform

- Clarifies what to protect
- Defines safeguarding
- Reinforces existing LRGWP
- Promotes authorized information sharing



# What we protect and How we protect it

[www.archives.gov/cui](http://www.archives.gov/cui)

**Controlled Unclassified Information (CUI)**

Home > CUI

Established by Executive Order 13526, 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 procedures.

Search the Registry:

Access Registry by

- Category-Subcategory
- Executive Order 13526
- 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

**Under Development - Registry**

- Marking Handbook
- Markings
- Limited Dissemination
- Decentral

**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.

**CUI Registry**

NIST Special Publication 800-171  
Revision 1

**Protecting Controlled Unclassified Information in Federal Systems Organizations**

RON ROSS  
KELLEY DEMPSEY  
Computer Security Division  
of Standards and Technology

PATRICK VISCUSO  
MADON RIDDLE  
Senior Security Oversight Officer  
and Security Administration

GARY GUSSANE  
Assistant for Defense Analysis  
of the Department of Defense

Available free of charge from:  
[dx.doi.org/10.1115/SP.800-171v1](http://dx.doi.org/10.1115/SP.800-171v1)

December 2016

DEPARTMENT OF COMMERCE  
NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

Part IV  
National Archives and Records Administration  
Information Security Oversight Office  
32 CFR Part 2002  
Controlled Unclassified Information; Final Rule

63380 Federal Register / Vol. 81, No. 178 / Wednesday, September 14, 2016 / Rules and Regulations

1221 Establishes a mechanism by which authorized holders (with standards and controls) the agency's can control a designated agency representative for

(b) Agencies may use only those categories or subcategories approved by 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

63386 Federal Register / Vol. 81, No. 178 / Wednesday, September 14, 2016 / Rules and Regulations

List of Subjects in:

Administrative procedure, Archives, Controlled Unclassified Information, Freedom of information, the President, Act, 5, reference, National security, National Open government.

For the reasons in this preamble, NARA is amending Chapter 32, by adding as follows:

**PART 2002—CONTROLED UNCLASSIFIED INFORMATION**

**Subpart A—General**

Sec. 2002.1 Purpose and scope

2002.2 Incorporation

2002.4 Definitions

2002.6 CUI Elements

2002.8 Rules and regulations

**Subpart B—Key Element Program**

2002.10 The CUI Program

2002.12 CUI categories

2002.14 Subcategories

2002.16 Accounting

2002.18 Declassification

2002.20 Marking

2002.22 Limited dissemination agency CUI policies

2002.24 Agency and

**Subpart C—CUI Program**

2002.26 Information

2002.32 CUI cover

2002.34 Transition

2002.36 Legacy cases

2002.38 Markings

2002.44 CUI and the

2002.46 CUI and the

2002.48 CUI and the President Act 12

2002.50 Challenges

2002.52 Dispute resolution

2002.54 Misuse of

2002.56 Sanctions

**Appendix A to Part 2002**

Authority: E.O. 13526, 2016 Comp. sup. 2016

**Subpart A—General**

**§2002.1 Purpose and scope**

(a) This part does not apply to information (CUI) in the Program and shall not be used to designate, handle, or disseminate information that is not CUI.

(b) The CUI Program is the mechanism by which authorized holders (with standards and controls) the agency's can control a designated agency representative for

(c) NARA incorporates certain material by reference into this part with the approval of the Director of the Federal Register under 5 U.S.C. 553(a)

**§2002.4 Definitions.**

As used in this part, the following definitions apply: (1) Agency: the Federal agency, executive agency, executive branch

**32 CFR 2002**

# 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.

# 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



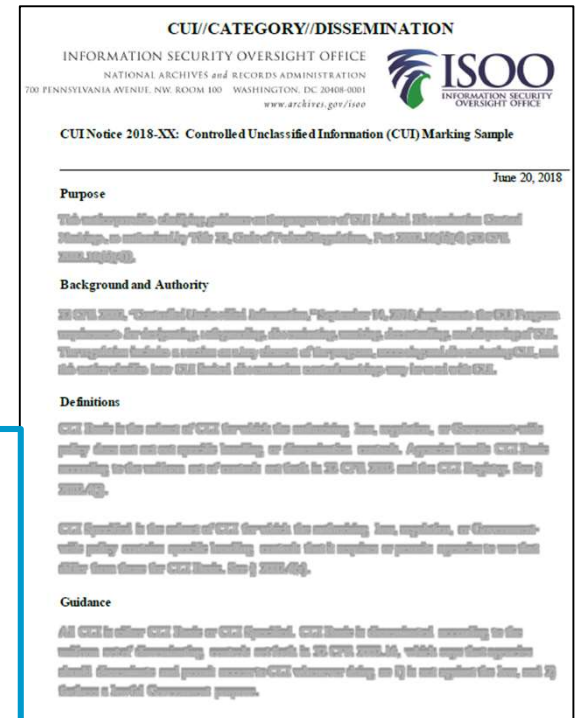


# Legacy Information and Markings



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

**Contractors do not have “legacy information” as such. Contractors should protect all information they have received in accordance with the contract that covers that information.**



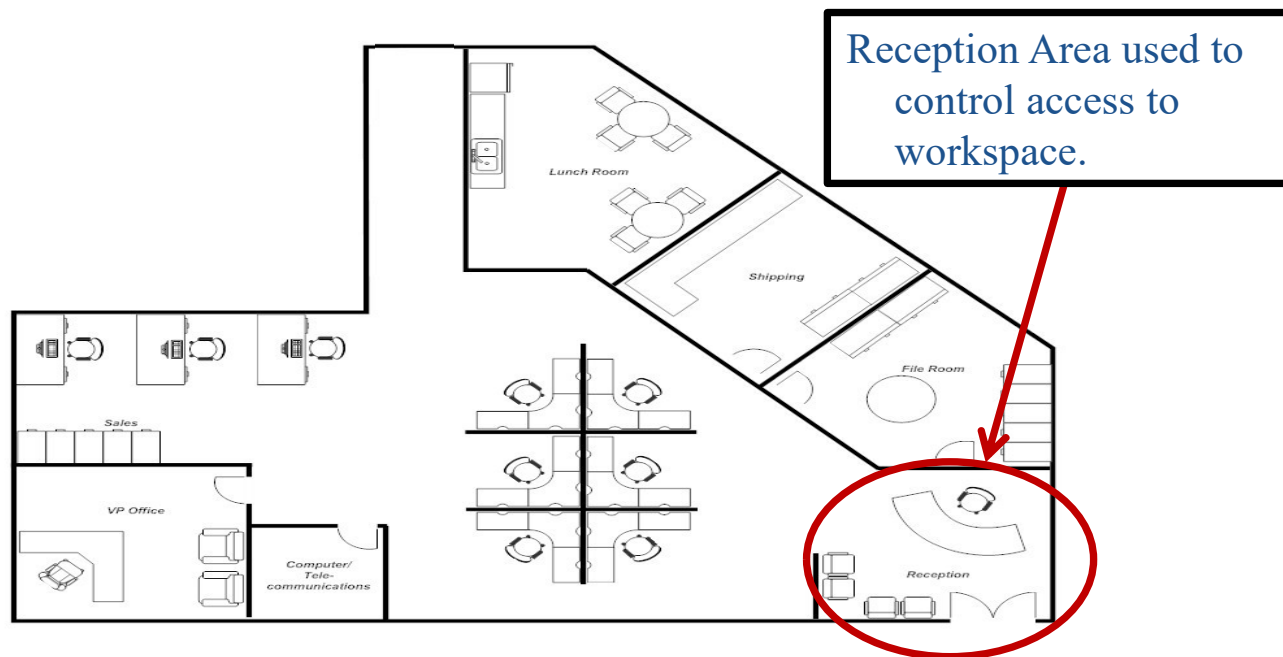
# Implementation

- Implementation has begun
  - Program officials, resources, policy, training, systems, contracts, oversight
- **CUI practices and Legacy practices will exist at the same time.**



# Controlled Environments

- 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.

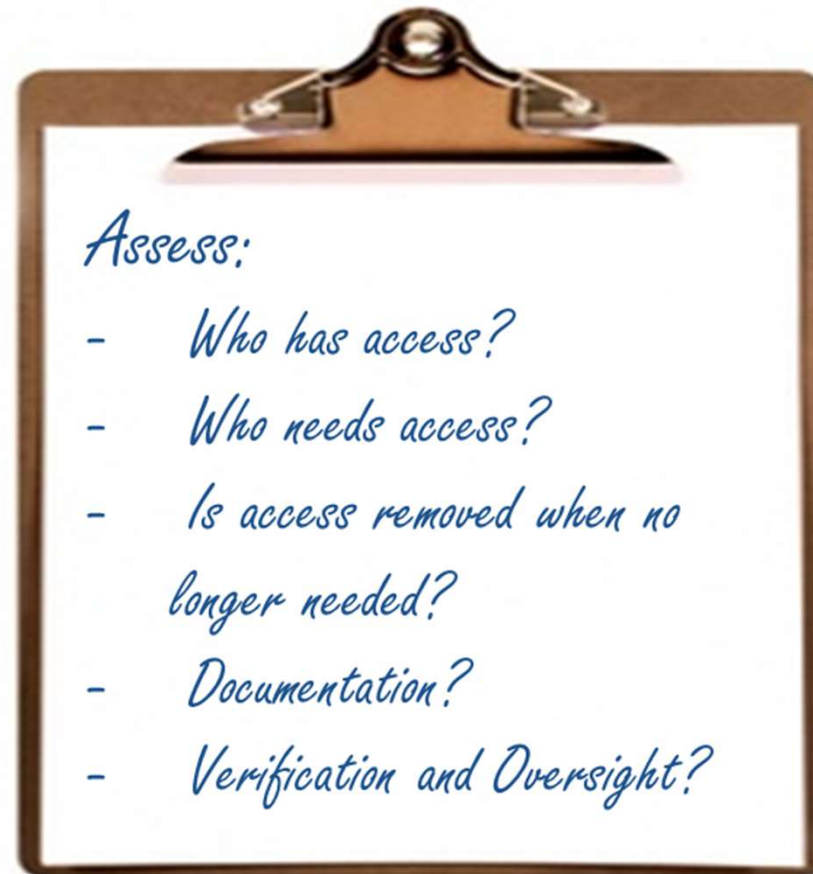


# Assessing physical environments

- **Going beyond gates, guns, and guards: Internal security**
  - Who works in the space?
  - Who has access to the space 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?

# Assessing electronic Environments

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



# Questions about DoD Implementation

1. **Contract compliance questions should be addressed to the Contract POC**
2. **DFARs 7012 compliance questions: Use DoD Procurement Toolbox covered on the next slide**
3. **Questions about CMMC: <https://www.acq.osd.mil/cmmc/>**
4. **Inquiries about DoD CUI Program Policies and Implementation should be addressed to the Office of the Under Secretary of Defense for Intelligence & Security (OUSD I&S)  
Email: [osd.pentagon.ousd-intel-sec.mbx.dod-cui@mail.mil](mailto:osd.pentagon.ousd-intel-sec.mbx.dod-cui@mail.mil)**

# DoD Procurement Toolbox

**Q13: Who in DoD can I contact for clarification on DFARS 252.204-7012 or NIST SP 800-171 in support of DFARS 252.204-7012?**

A13: Contractors should email their query to [osd.dibcsia@mail.mil](mailto:osd.dibcsia@mail.mil). Emails received at this address are reviewed daily and distributed as appropriate to a cross-functional team of subject matter experts for action.

Quick Look for FAQ Topics	
<p>Safeguarding Covered Defense Information and Cyber Incident Reporting (DFARS 252.204-7008 and 252.204-7012)</p> <ul style="list-style-type: none"> <li>• General</li> </ul> <p>Q1 –Q18</p> <ul style="list-style-type: none"> <li>• Covered Defense Information</li> </ul> <p>Q19 –Q30</p> <ul style="list-style-type: none"> <li>• Operationally Critical Support</li> </ul> <p>Q31</p> <ul style="list-style-type: none"> <li>• Safeguarding Covered Defense Information</li> </ul> <p>Q32 –Q34</p> <ul style="list-style-type: none"> <li>• Cyber Incidents and Reporting</li> </ul> <p>Q35 –Q45</p> <ul style="list-style-type: none"> <li>• Submission of Malicious Software</li> </ul> <p>Q46</p> <ul style="list-style-type: none"> <li>• Cyber Incident Damage Assessment</li> </ul> <p>Q47</p>	<p>NIST SP 800-171</p> <ul style="list-style-type: none"> <li>• General Implementation Issues</li> </ul> <p>Q49 –Q67</p> <ul style="list-style-type: none"> <li>• Specific Security Requirements</li> </ul> <p>Q68 –Q98</p> <hr/> <p>Cloud Computing</p> <ul style="list-style-type: none"> <li>• General Q99 –101</li> <li>• Cloud solution being used to store data on DoD's behalf (DFARS 252.239-7009 and 252.204-7010, Cloud Computing Services, apply)</li> </ul> <p>Q102</p> <ul style="list-style-type: none"> <li>• Contractor using cloud solution to store covered defense information (DFARS 252.204-7008 and 252.204-7012 apply)</li> </ul> <p>Q103 –Q109</p>
<p>Basic Safeguarding of Contractor Information Systems (FAR Clause 52.204.21)</p> <p>Q48</p>	<p>Limitations on the use or disclosure of third-party contractor reported cyber incident information (DFARS Clause 252.204-7009)</p> <p>Q47</p>

<https://dodprocurementtoolbox.com>  
**Click on the Cybersecurity Tab**

# Controlled Unclassified Information (CUI)

## What is the CUI Program?

The CUI Program is an information security reform that standardizes the way the executive branch handles information that requires protection

## What is CUI?

Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable laws, regulations, and government-wide policies.

## Policy and Guidance

- Executive Order 13556
- 32 CFR Part 2002 (Implementing Directive)
- CUI Marking Handbook
- CUI Notices
- NIST Publications
- OMB Circular No. A-11
- CUI Advisory Council

CUI Registry

The CUI Registry is the Government-wide online repository for Federal-level guidance regarding CUI policy and practice. However, agency personnel and contractors should first consult their agency's CUI implementing policies and program management for guidance.

Search the Registry:

**Categories, Markings and Controls:**

- Category-Subcategory List
- Category-Subcategory Markings
- Limited Dissemination Controls
- Decontrol
- Registry Change Log

**Policy and Guidance**

- Executive Order 13556
- 32 CFR Part 2002 (Implementing Directive)
- CUI Marking Handbook
- CUI Notices

**CUI Glossary**

 **Training Tools**  
Learn about training tools developed by the Executive Agent for CUI users.

**Contact Us!**  
Contact an Agency!

 **Additional Tools**  
Learn about additional tools for handling CUI.

- CUI Coversheets
- CUI Marking Trifold Brochure
- Audio/Photo/Video Markings Brochure

[www.archives.gov/cui](http://www.archives.gov/cui)

  **CONTROLLED UNCLASSIFIED INFORMATION**

**CUI Program Blog**

**Quarterly CUI Program Updates!**

**FOLLOW BLOG VIA EMAIL**

Enter your email address to follow this blog and receive notifications of new posts by email.

Email Address

<https://isoo.blogs.archives.gov/>