An Overview of the CUI Program

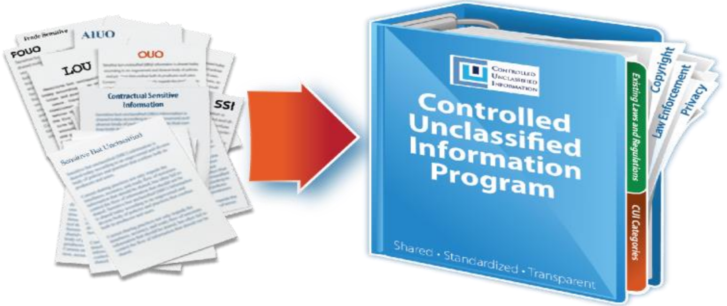
Controlled
Unclassified
Information

Updated 01/21

What is CUI?

CUI is Information that needs protection and is not classified.

- The Controlled Unclassified Information (CUI) Program standardizes the way the Executive branch handles information that requires protection and is not classified.
- CUI ensures safeguards employed while information is being stored or used by the agency and the controls involving how the information is disseminated.
- The CUI Program replaces hundreds of different agency policies and associated markings with one shared system of markings.


Trade Sensitive
AIUO
FOUO
OUO
LOU
Contractual Sensitive Information
SSI
Sensitive But Unclassified
Controlled Unclassified Information
Controlled Unclassified Information Program
Shared • Standardized • Transparent
Existing Laws and Regulations
CUI Categories
Copyright
Law Enforcement
Privacy

Leadership

CUI Executive Agent: NARA's Information Security Oversight Office (ISOO)

CUI Advisory Council: Lead by the Executive Agent; Membership from Executive Branch agencies

GSA Leaders:

- Senior Agency Official - Beth Killoran, Deputy CIO
- Program Managers (PMs) - Karen Overall and Andy Riordan, Enterprise Data and Privacy Management Office (IDE)

Implementation Plans

- The CUI Program is under development. Estimated timeline towards implementation:

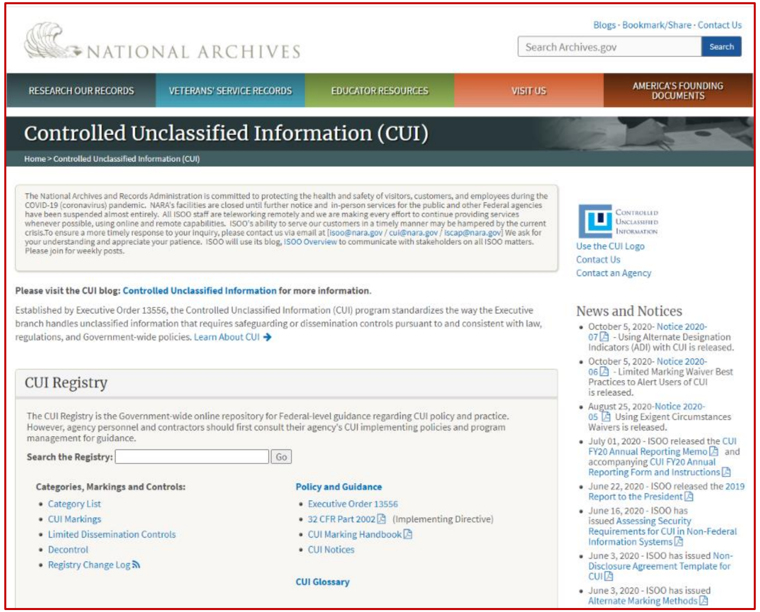
CUI Policy updated	April 2021
CUI Course - mandatory for employees	Jan-April 2021
CUI Guide published	April 2021
Begin implementation at GSA	July 1, 2021
FAR rule focused on CUI	2021
Implementation across the Executive Branch	by Dec 31, 2021

Examples of CUI

- **PII** - SSNs, personnel files, health info…
- **SBU** - PBS Building drawings/blueprints with sensitive info…
- **Contract data** – Bids, source selection info, customer data…
- **IT Operation Info** – Network diagrams, IP addresses….
- **Legal** – Administrative proceedings, Witness Protection…

The CUI Registry

- NARA’s repository that contains info, guidance, training, and requirements for handling CUI.
- Identifies 100+ approved Categories.
- Lists the applicable authorities for each category that says the information should be protected.
- Establishes CUI markings for each category.


Blogs · Bookmark/Share · Contact Us
NATIONAL ARCHIVES
Search Archives.gov
Search
RESEARCH OUR RECORDS
VETERANS' SERVICE RECORDS
EDUCATOR RESOURCES
VISIT US
AMERICA'S FOUNDING DOCUMENTS
Home > Controlled Unclassified Information (CUI)
Controlled Unclassified Information

Controlled Unclassified Information (CUI)

The National Archives and Records Administration is committed to protecting the health and safety of visitors, customers, and employees during the COVID-19 (coronavirus) pandemic. NARA's facilities are closed until further notice and in-person services for the public and other Federal agencies have been suspended almost entirely. All ISOO staff are teleworking remotely and we are making every effort to continue providing services whenever possible, using online and remote capabilities. ISOO's ability to serve our customers in a timely manner may be hampered by the current crisis.To ensure a more timely response to your inquiry, please contact us via email at [isoo@nara.gov / cui@nara.gov / iscap@nara.gov] We ask for your understanding and appreciate your patience. ISOO will use its blog, ISOO Overview to communicate with stakeholders on all ISOO matters. Please join for weekly posts.

Please visit the CUI blog: Controlled Unclassified Information for more information.

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 →

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: Go

Categories, Markings and Controls:

- Category List
- CUI 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

Use the CUI Logo
Contact Us
Contact an Agency

News and Notices

- October 5, 2020- Notice 2020-07 - Using Alternate Designation Indicators (ADI) with CUI is released.
- October 5, 2020- Notice 2020-06 - Limited Marking Waiver Best Practices to Alert Users of CUI is released.
- August 25, 2020-Notice 2020-05 Using Exigent Circumstances Waivers is released.
- July 01, 2020 - ISOO released the CUI FY20 Annual Reporting Memo and accompanying CUI FY20 Annual Reporting Form and Instructions
- June 22, 2020 - ISOO released the 2019 Report to the President
- June 16, 2020 - ISOO has issued Assessing Security Requirements for CUI in Non-Federal Information Systems
- June 3, 2020 - ISOO has issued Non-Disclosure Agreement Template for CUI
- June 3, 2020 - ISOO has issued Alternate Marking Methods

www.archives.gov/cui

CUI Categories

- The CUI Categories that GSA will likely use:

Critical Infrastructure

Emergency Management

General Critical Infrastructure Information

Information Systems Vulnerability Information

Physical Security

Financial

Budget

Comptroller General

Electronic Funds Transfer

General Financial Information

Legal

Administrative Proceedings

Collective Bargaining

Legal Privilege

Legislative Materials

Protective Order

Natural and Cultural Resources

Historic Properties

Privacy

Contract Use

General Privacy

Inspector General Protected

Personnel Records

Procurement and Acquisition

Source Selection

Proprietary Business Information

Entity Registration Information

General Proprietary Business Information

Types of CUI

- CUI Basic

CUI Basic is when the applicable authority says the information should be protected and nothing else is required. Therefore, only the standard CUI marking and protection procedures must be followed. This is the most common type of CUI.

- CUI Specified

CUI is specific when the applicable authority includes specific or additional guidance for that type of information. That could mean additional markings, extra protection, limited dissemination, or some other specific direction. Therefore, more protections are required of CUI Specified than of CUI Basic.

Safeguarding

Safeguard CUI at all times in a manner that minimizes the risk of unauthorized disclosure while allowing timely access by authorized holders.

Controlled environments

- Physical: At least 1 physical barrier such as a locked cabinet
- General: Be aware of surroundings; do not review or discuss in common areas
- Electronic: Protect IT systems from unauthorized access

Marking

Marking of CUI documents is required in order to show that the document contains sensitive information.

- Printed copy - Banner marking on the top of each page
- IT Systems - Must have splash screens, banners, or other forms of notification that the system contains CUI
- IT Systems printout - Either automatically print banners or the holder must write the banner marking on each page
- First page - Indicate the agency of designation and a contact person/organization

Banner Markings

- For ***CUI Basic*** the only required banner marking is CUI in Capital letters (other agencies may use the word Controlled instead) at the top of every page of the document.
- For ***CUI Specified***, the marking must also include the category or categories, in alphabetical order, separated by 1 slash.

  Example: CUI//SP-BUDG/SP-PRVCY
- Either banner marking may also include limited dissemination information at the end of the marking.

  Example: CUI//SP-PRVCY//NOFORN
- The CUI Registry has more information on markings.
- CUI Coversheets may also be used to protect printed docs.

Destroying

- Destruction must make CUI unreadable, indecipherable, and irrecoverable.
- Shredders and Shredding Services must comply with NIST 800-88. Destroy to 1mm x 5mm particles.
- Do NOT put CUI in trash cans or recycle bins

Cross cut shredders

1x5mm shredders

Reporting CUI Incidents

Incidents involving CUI must be reported immediately to the IT Service Desk who will work with the OCISO Incident Response team. Report incidents such as:

- Improper storage
- Mishandling
- Unauthorized individuals gaining access
- Unauthorized release of CUI
- Mismarked or unmarked CUI

Resources

- Implementing Directive: 32 CFR part 2002
- The CUI Registry: archives.gov/cui
- NARA’s training videos: archives.gov/cui/training
- NARA’s CUI Blog: isoo.blogs.archives.gov
- NIST 800-171 Rev 2: Protecting CUI in Non-Federal systems
- GSA's CUI Policy

For more information contact the CUI Team at cui@gsa.gov