Controlled Unclassified Information

Department of Commerce Controlled Unclassified Information (CUI)

The Department of Commerce CUI Basic User Awareness Training

OMB Control No. 0690-0038

Agenda

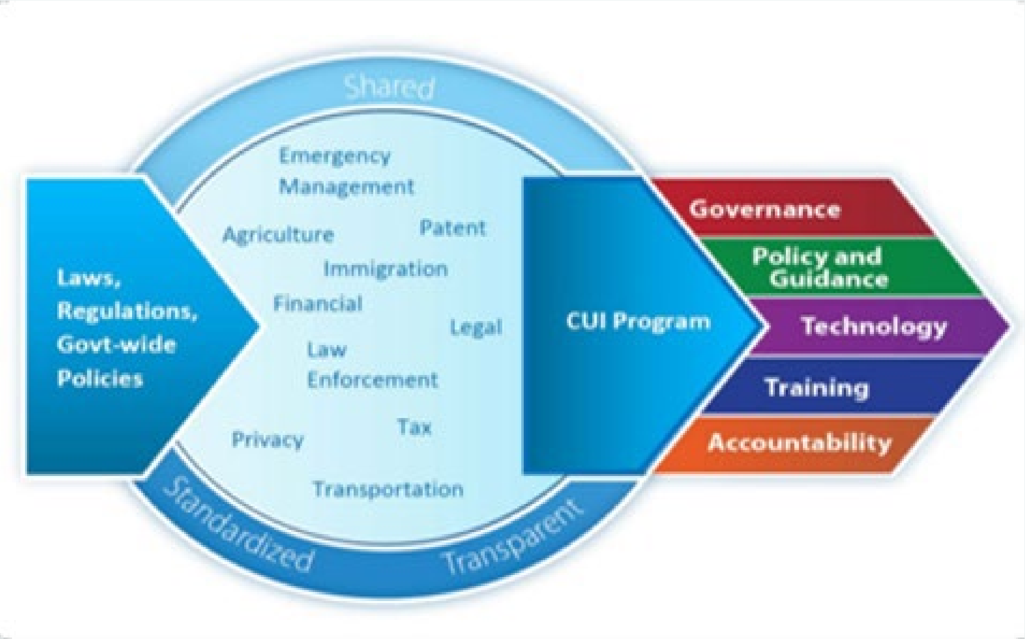
- CUI Program Overview
- All About CUI
- CUI Marking Standards
- Sending and Receiving CUI
- Safeguarding, Decontrolling and Destruction of CUI
- CUI Incident Reporting
- CUI Resources
- Certificate of Completion

CUI Program Overview

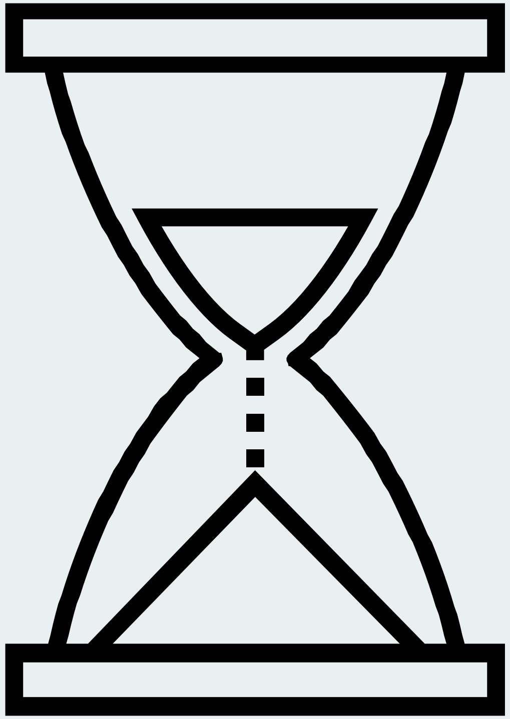
This section will cover the Purpose, History, Authorities and Benefits of the CUI Program

Purpose of CUI

The Controlled Unclassified Information (CUI) program is an information security reform that addresses an inconsistent, and often conflicting, patch work of over 100 different agency-specific policies, markings, and other requirements used to control information requiring protection in accordance with Laws, Regulations and Government-wide Policies (LRGWP) throughout the executive branch.



History of CUI



Spanning from 2004 to present day, CUI has gone through many iterations to become the program it is today.

During today’s training, there are several CUI Authorities that will continue to be mentioned:

- **Executive Order** (**E.O) 13556,** which established the CUI program in 2010
- **32 (code of federal regulations) or CFR Part 2002**, published in 2016, which establishes CUI Program requirements for designating and disposing of CUI.

Notable Dates in CUI

- **2004** - The 9/11 Commission Report recommends horizontal sharing of intelligence information.
- **2009** - The Presidential Task Force expands the recommendation to include all Controlled Unclassified Information (CUI) within the Executive Branch.
- **2010** - Executive Order 13556 establishes the comprehensive CUI Program, designates the National Archives and Records Administration (NARA) as the Executive Agent (EA), and appoints the Director of the Information Security Oversight Office (ISOO) as Director of the CUI Office.
- **2016** - 32 CFR Part 2002 Controlled Unclassified Information is published as a final rule, becoming effective on November 14, 2016.
- **2018** - ISOO issues CUI Notice 2018-03, Implementation and Compliance Reporting and Delays, recognizing various factors that might delay implementation within an agency and providing guidance on reporting issues related to implementation.
- **2021** - Agencies implement comprehensive policies for the Controlled Unclassified Information (CUI) Program, covering responsibilities, incident reporting, self-inspection, training, safeguarding, dissemination standards, and management of CUI categories.

CUI Authorities

The National Archives and Records Administration (**NARA**) is the Executive Agent (EA) of the executive branch-wide CUI Program and oversees federal agency actions to comply with **Executive Order (E.O) 13556**. NARA has delegated this authority to the Director of the Information Security Oversight Office (ISOO).

The Controlled Unclassified Information (CUI) Federal Regulation at **32 CFR 2002** implements Executive Order 13556 for CUI and establishes CUI Program requirements for designating and disposing of CUI.

Benefits of CUI

The CUI program is one uniform, shared and transparent system for safeguarding and disseminating CUI that:

- Establishes a common understanding of CUI control
- Promotes information sharing
- Reinforces existing legislation and regulations
- Clarifies the difference between CUI controls and FOIA exemptions

Throughout The Entire Federal Government

All About CUI

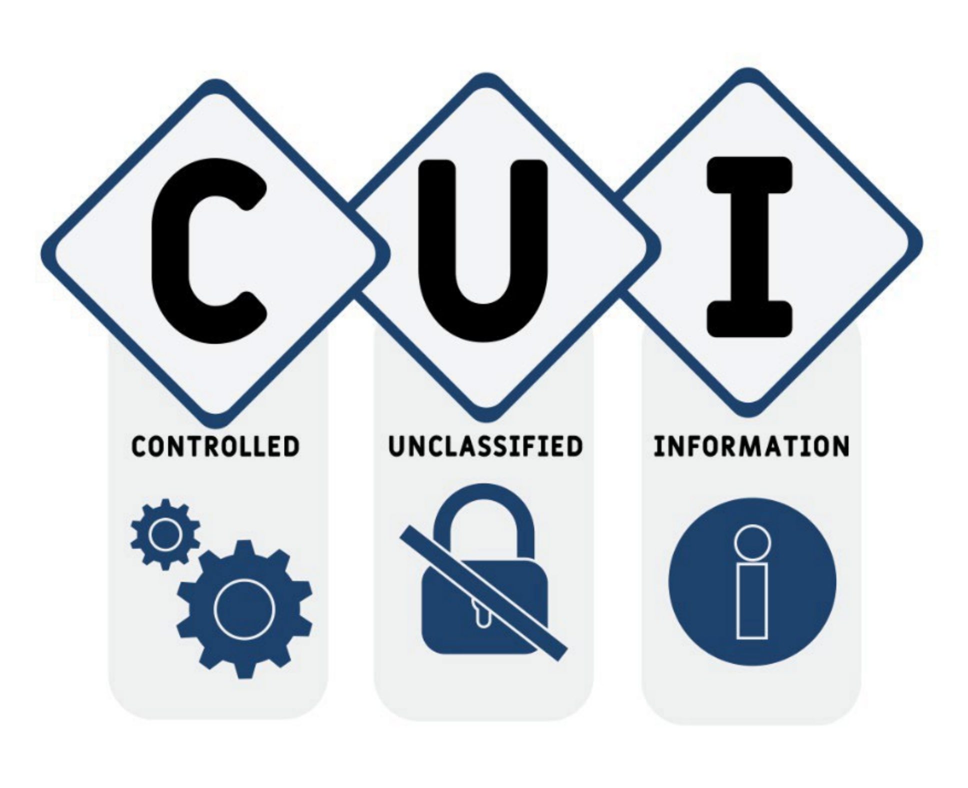
This section will specify CUI's definition, types and relationship to FOIA

What is CUI?

❖Controlled Unclassified Information (CUI) is sensitive information that executive branch agencies are required or permitted to protect, a task that has been carried out in an ad hoc and inconsistent manner for decades.

❖The legacy of inconsistent agency policies, procedures, and markings for safeguarding sensitive unclassified information has prompted a continuous reform effort spanning the past three Presidential administrations.

❖CUI replaces existing markings such as For Official Use Only (FOUO), Law Enforcement Sensitive (LES), and Sensitive But Unclassified (SBU).



Types of Controlled Unclassified Information: CUI Basic

20 Categories of CUI Basic

- Critical Infrastructure
- North Atlantic Treaty Organization (NATO)
- Defense
- Nuclear
- Export Control
- Patent
- Financial
- Privacy
- Immigration
- Procurement and Acquisition
- Intelligence
- Proprietary Business Information
- International Agreements
- Provisional
- Law Enforcement
- Statistical
- Legal
- Tax
- Natural and Cultural Resources
- Transportation

- This information is protected by a **specific** law, regulation or government wide policy
- Consider this the standard of all Controlled Unclassified Information
- All rules of CUI apply to CUI Basic Categories and Subcategories

Types of Controlled Unclassified Information: CUI Specified

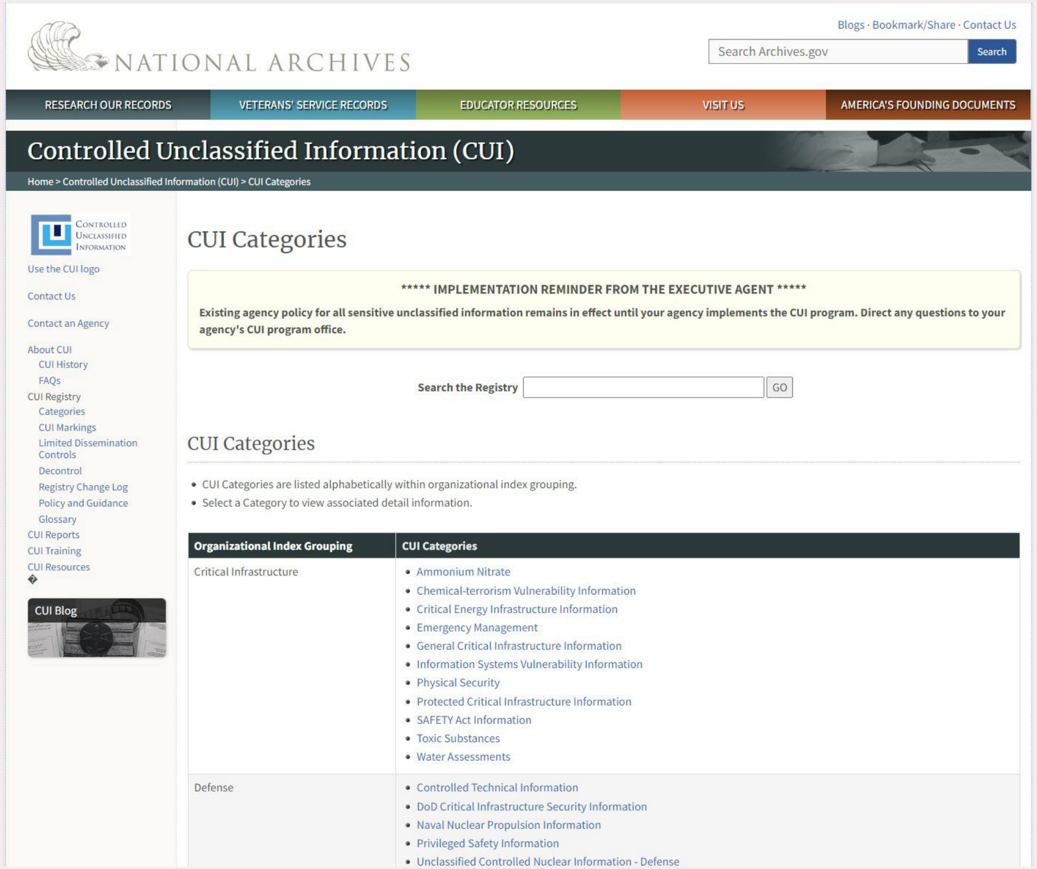
- Nuclear – **CUI Basic Category**
  - **CUI Specified Categories** within Nuclear
    - ❑ General Nuclear
    - ❑ Nuclear Recommendation Material
    - ❑ Nuclear Security Related Information
    - ❑ Safeguards Information
    - ❑ Unclassified Controlled Nuclear Information- Energy

- This information is protected by a specific law, regulation or government wide policy AND includes one or more specific handling standards
- CUI Specified is **NOT** a “higher level” of CUI, it is simply different.
- If the Law, Regulation, or Government-wide policy that pertains to your agency is listed in the CUI Registry as a Specified Authority**, then you must mark the CUI based in that Authority as CUI Specified and include that marking in the CUI Banner.**

CUI Registry

The National Archives and Records Administration maintains the CUI registry which shows authorized categories and associated markings, as well as applicable safeguarding, dissemination, and decontrol procedures.

The CUI registry is updated as agencies continue to submit governing authorities that authorize the protection and safeguarding of sensitive information.



Controlled Unclassified Information (CUI)

Home > Controlled Unclassified Information (CUI) > CUI Categories

CUI Categories

******* IMPLEMENTATION REMINDER FROM THE EXECUTIVE AGENT *******

Existing agency policy for all sensitive unclassified information remains in effect until your agency implements the CUI program. Direct any questions to your agency's CUI program office.

Search the Registry

CUI Categories

- CUI Categories are listed alphabetically within organizational index grouping.
- Select a Category to view associated detail information.

Organizational Index Grouping	CUI Categories
Critical Infrastructure	• Ammonium Nitrate • Chemical-terrorism Vulnerability Information • Critical Energy Infrastructure Information • Emergency Management • General Critical Infrastructure Information • Information Systems Vulnerability Information • Physical Security • Protected Critical Infrastructure Information • SAFETY Act Information • Toxic Substances • Water Assessments
Defense	• Controlled Technical Information • DoD Critical Infrastructure Security Information • Naval Nuclear Propulsion Information • Privileged Safety Information • Unclassified Controlled Nuclear Information - Defense

CUI and FOIA

- The CUI Program is established by an Executive Order, and the basis of it is to allow for the controlling of information that is unclassified but that needs protection or limited dissemination.
- The Freedom of Information Act (FOIA) is a statute that provides the public the right to request access to records from any federal agency.
- The CUI Program does **NOT** alter the current Commerce FOIA review process. Marking information as CUI does not allow information to be withheld from release in response to a FOIA request.

CUI Marking Standards

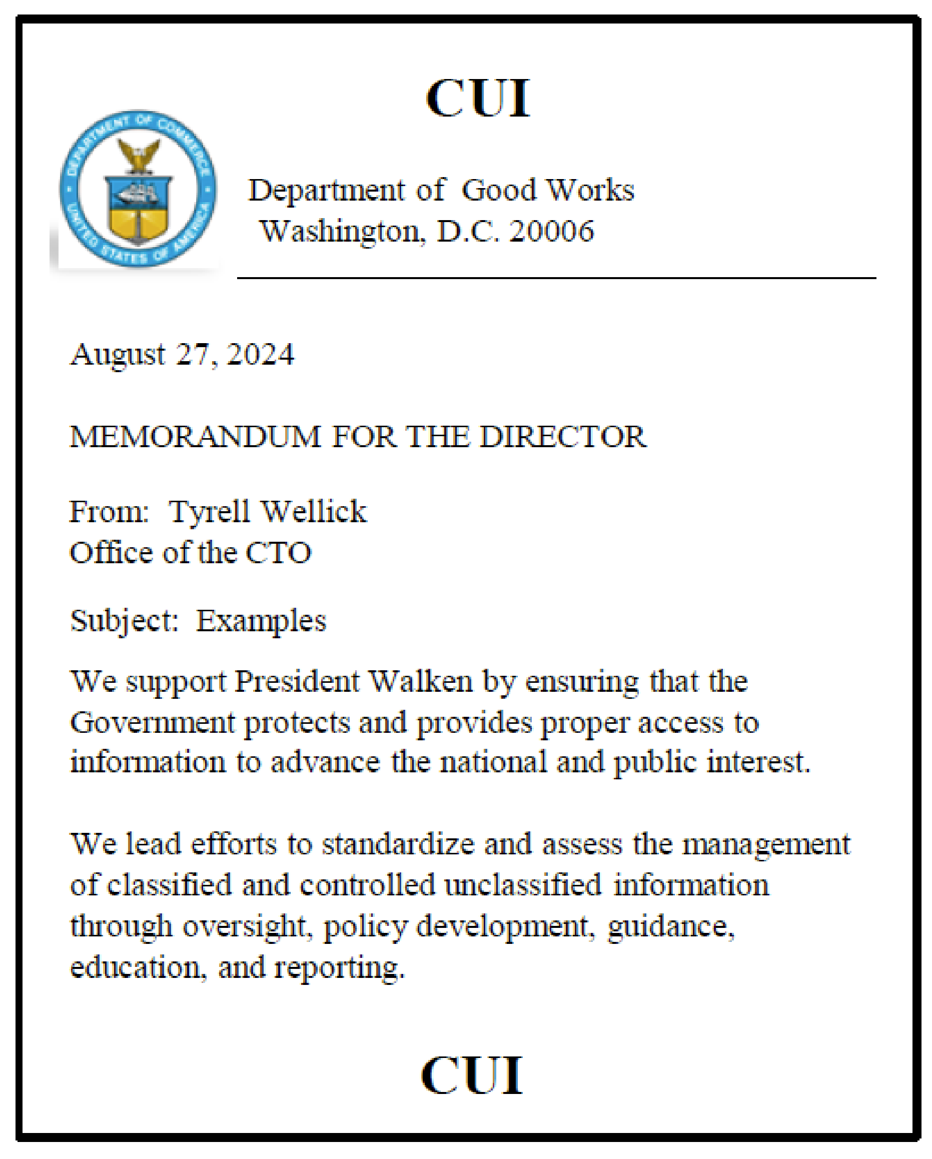
This section will specify CUI standards including Banner, Specified Category Marking and, General and Limited Dissemination Principles

Marking CUI

The CUI banner marking must appear, at a **minimum, at the top center of each page containing CUI**

Its purpose is to **inform or alert recipients /users that CUI is present and of any limited dissemination controls**

Agencies must uniformly and conspicuously apply CUI markings to **all CUI prior to disseminating it.**



CUI

Department of Good Works
Washington, D.C. 20006

August 27, 2024

MEMORANDUM FOR THE DIRECTOR

From: Tyrell Wellick
Office of the CTO

Subject: Examples

We support President Walken 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.

CUI

CUI Banner Marking Overview

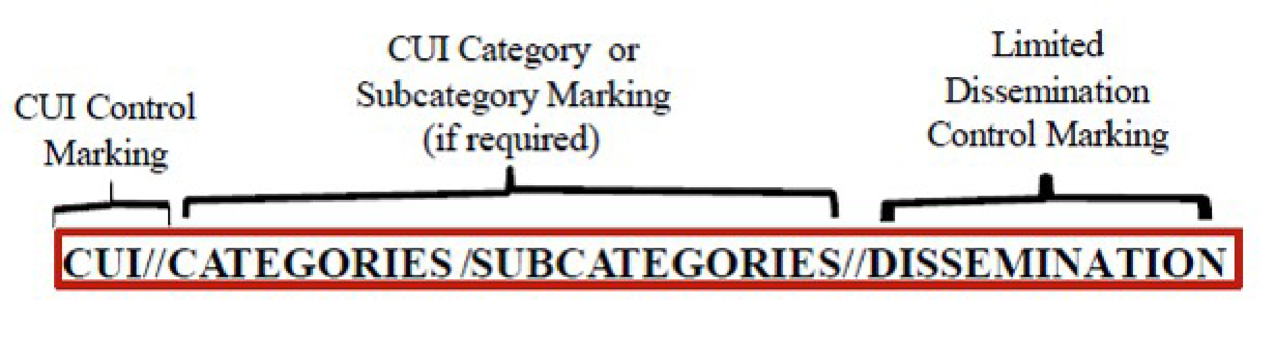
- **Components of CUI Banner Marking:**
  - CUI control marking
  - Category markings (if required)
  - Dissemination control markings
- **Mandatory CUI Control Marking:**
  - CUI control marking is obligatory for all CUI banners.
  - The CUI Control Marking will consist of "CUI."
- **Category Markings:**
  - **Mandatory** for CUI Specified.
  - **Mandatory** for CUI Basic

CUI Banner Marking Breakdown

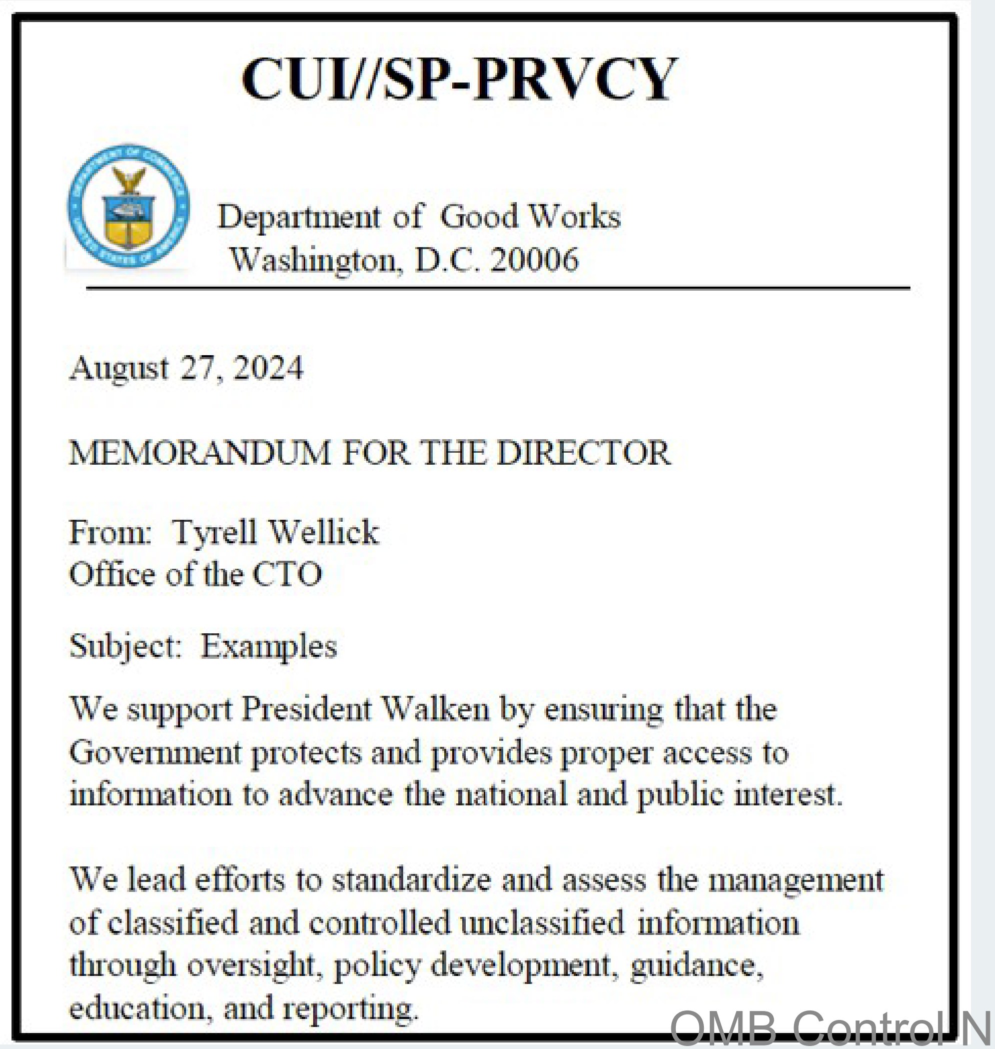
The **CUI Control Marking** is mandatory for all CUI and may consist of the acronym “CUI”.

CUI Control Marking and **Category Markings** are separated by two forward slashes(//). When including multiple categories they are separated by a single forward slash (/).

Limited Dissemination Control Markings are separated from preceding sections of the CUI Banner Marking by a double forward slash (//).


CUI Control Marking
CUI Category or Subcategory Marking (if required)
Limited Dissemination Control Marking
CUI//CATEGORIES /SUBCATEGORIES//DISSEMINATION

CUI Specified Category Marking



CUI//SP-PRVCY

Department of Good Works
Washington, D.C. 20006

August 27, 2024

MEMORANDUM FOR THE DIRECTOR

From: Tyrell Wellick
Office of the CTO

Subject: Examples

We support President Walken 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.

The CUI Control Marking is **mandatory** for CUI Specified Categories.

To the left is an example of a memo that is marked with CUI Specified category Privacy (SP-PRVCY).

The specified category, SP-PRVCY, refers to personal information, or, in some cases, "personally identifiable information” defined by several laws, regulations and government wide policies.

General Dissemination Principles

Access to CUI should be encouraged and permitted to the extent that access of dissemination:

- Abides by the laws, regulations, or Government-wide policies that established the information as CUI
- Furthers a lawful government purpose; is not restricted by an authorized limited dissemination control established by the CUI Executive Agent; and is not otherwise prohibited by law
- Department of Commerce may place limits on disseminating CUI for a lawful government purpose only though the use of the authorized limited dissemination controls
- DOC's CUI policy governs specific criteria for when, and by whom, it will allow for the application of limited dissemination controls and control markings and ensures that policy aligns with 32 CFR Part 2002.

Limited Dissemination Controls

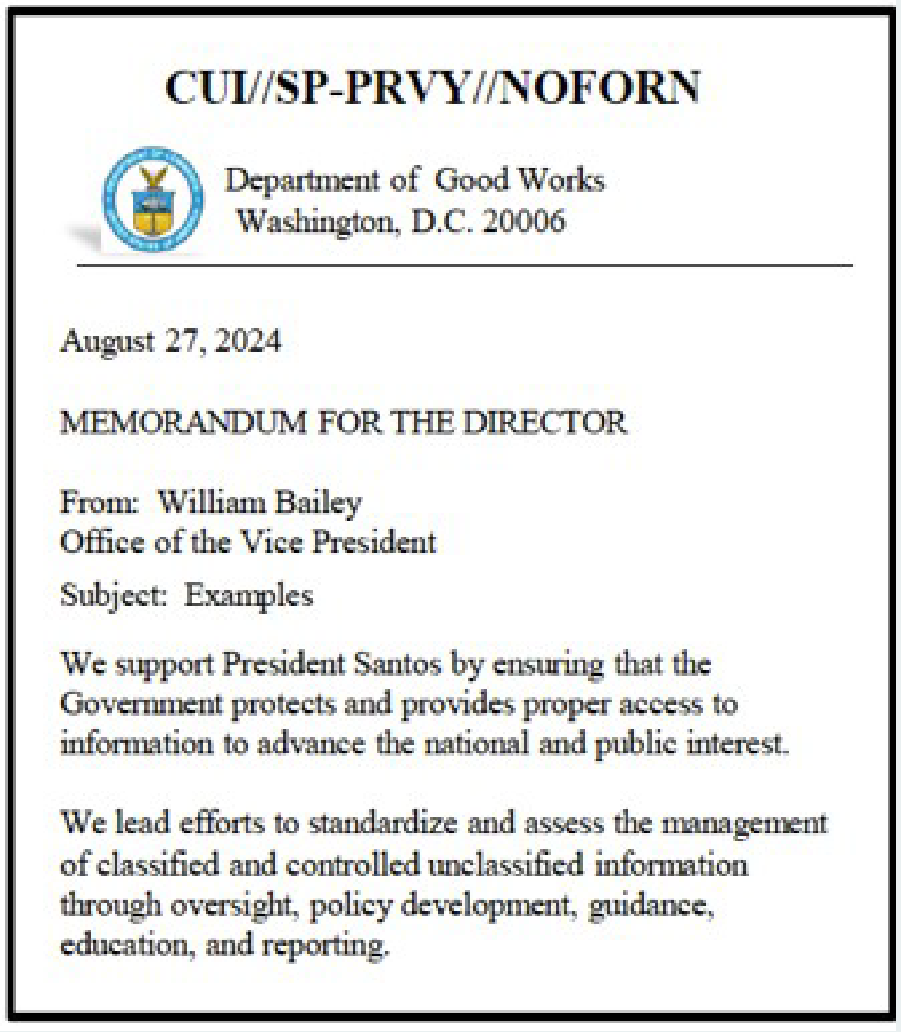
Limited dissemination control markings align with limited dissemination controls established by the CUI Executive Agent (EA).

They are used to limit or control who can or should (or should not) access CUI.

Limited dissemination controls markings may also be applied to CUI to amplify and supplement any dissemination controls authorized by a CUI Specified authority (i.e., law, regulation, or Government wide policy).

Limited Dissemination Controls Examples

- No Foreign Dissemination: **NOFORN**
- Federal Employees Only: **FED ONLY**
- Federal Employees and Contractors Only: **FEDCON**
- No Dissemination to Contractors: **NOCON**
- Releasable by information disclosure official: **RELIDO**
- No Dissemination List Controlled: **DL ONLY**
  - Ability to define per mission, project , or individuals
- Authorized for Release to Certain Nationals Only: **REL TO [USA,LIST]**
- **DISPLAY ONLY [USA,LIST]**
  * For use only by the Intelligence and Defense communities



CUI//SP-PRVY//NOFORN

Department of Good Works
Washington, D.C. 20006

August 27, 2024

MEMORANDUM FOR THE DIRECTOR

From: William Bailey
Office of the Vice President

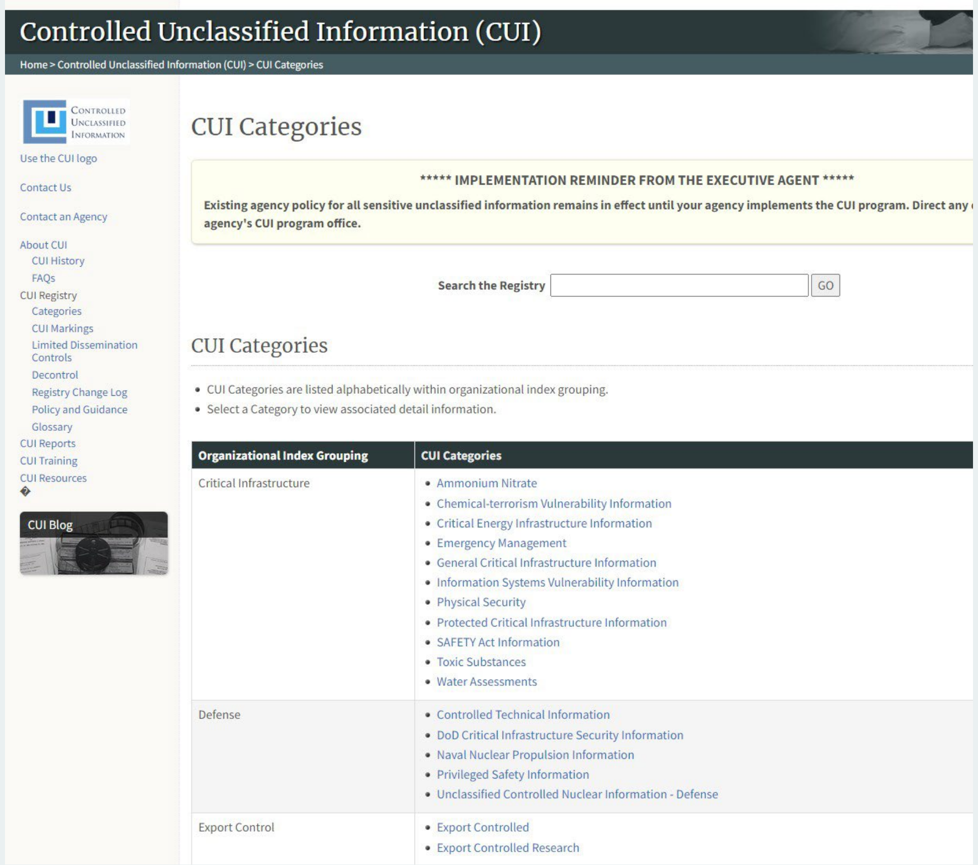
Subject: Examples

We support President Santos 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.

Document Marking

As you become more familiar with document marking, a quick reference to the National Archives and Records Administration CUI registry will help you recognize CUI categories and markings.



Controlled Unclassified Information (CUI)

Home > Controlled Unclassified Information (CUI) > CUI Categories

Use the CUI logo

Contact Us

Contact an Agency

About CUI
- CUI History
- FAQs

CUI Registry
- Categories
- CUI Markings
- Limited Dissemination Controls
- Decontrol
- Registry Change Log
- Policy and Guidance
- Glossary

CUI Reports

CUI Training

CUI Resources

�

CUI Blog

CUI Categories

******* IMPLEMENTATION REMINDER FROM THE EXECUTIVE AGENT *******

Existing agency policy for all sensitive unclassified information remains in effect until your agency implements the CUI program. Direct any agency's CUI program office.

Search the Registry

CUI Categories

- CUI Categories are listed alphabetically within organizational index grouping.
- Select a Category to view associated detail information.

Organizational Index Grouping	CUI Categories
Critical Infrastructure	Ammonium Nitrate Chemical-terrorism Vulnerability Information Critical Energy Infrastructure Information Emergency Management General Critical Infrastructure Information Information Systems Vulnerability Information Physical Security Protected Critical Infrastructure Information SAFETY Act Information Toxic Substances Water Assessments
Defense	Controlled Technical Information DoD Critical Infrastructure Security Information Naval Nuclear Propulsion Information Privileged Safety Information Unclassified Controlled Nuclear Information - Defense
Export Control	Export Controlled Export Controlled Research

Document Marking Examples

TOP of EACH page:

CUI//Category1/Category2//Dissemination Control (Types of CUI)

Examples:

- CUI//EMGT **(CUI Basic)**
  - CUI//SP-PER/PRVCY//FEDONLY **(CUI Specific, Basic and Limited Dissemination)**
    - CUI //SP-CENS/SP-TAX/ /DL ONLY **(CUI Specific and Limited Dissemination)**

Note: Specified categories are listed first alphabetically followed by Basic categories in alphabetical order

Document Marking Examples pt.2

Bottom of Each page:

Markings here are not required but are considered a best practice

If marking the bottom of the page, be sure to mirror the marking at the top of the page.

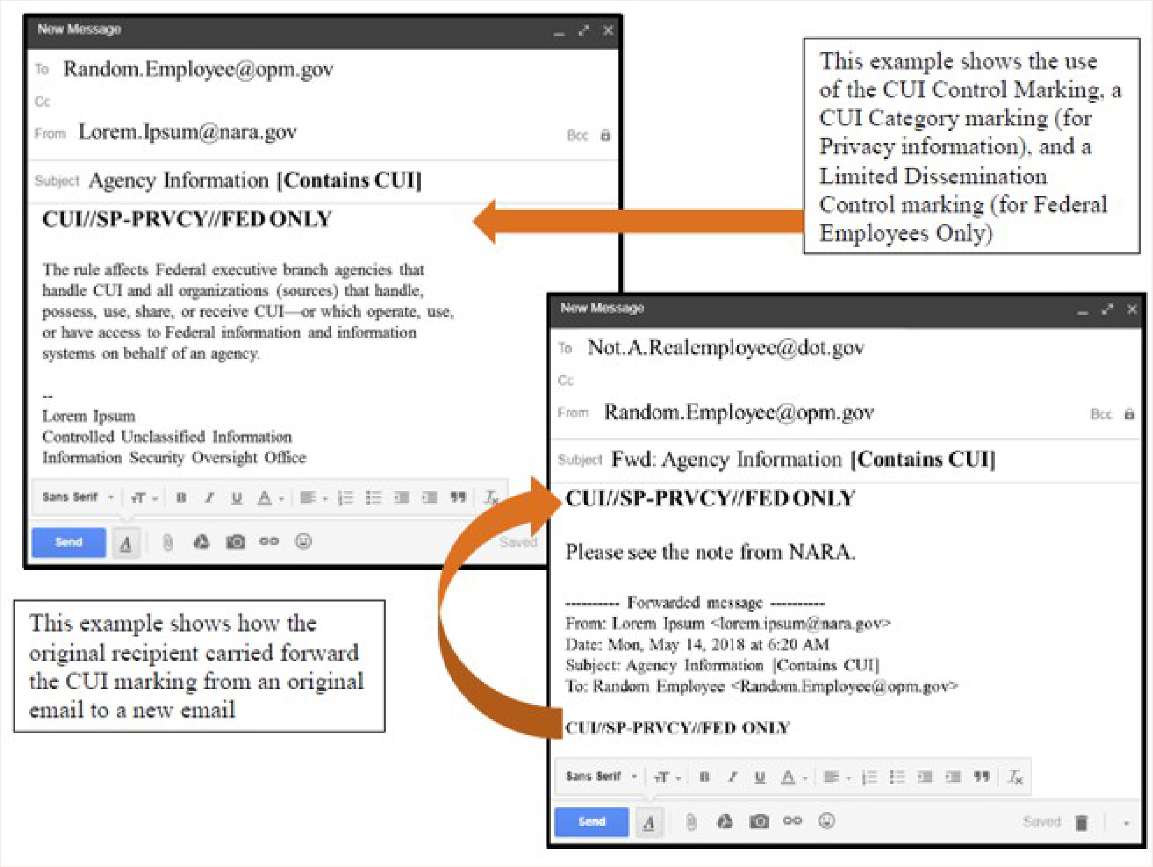
Portion Marking is **NOT required; however, if you portion mark any paragraph, the entire document must be portion marked.

Sending and Receiving CUI

This section will focus on: Email Marking, Receiving CUI and Designation Indicators

Email Marking

- When Sending an email, a banner marking must appear at the top portion of the email.
- **[Contains CUI]** should appear in the subject line to alert recipients that CUI is present in the email.
- When forwarding or responding to email containing CUI, be sure to carry forward all applicable marking to the new email.



To Random.Employee@opm.gov

From Lorem.Ipsum@nara.gov

Subject Agency Information **[Contains CUI]**

CUI//SP-PRVCY//FED ONLY

The rule affects Federal executive branch agencies that handle CUI and all organizations (sources) that handle, possess, use, share, or receive CUI—or which operate, use, or have access to Federal information and information systems on behalf of an agency.

--
Lorem Ipsum
Controlled Unclassified Information
Information Security Oversight Office

This example shows the use of the CUI Control Marking, a CUI Category marking (for Privacy information), and a Limited Dissemination Control marking (for Federal Employees Only)

To Not.A.Realemployee@dot.gov

From Random.Employee@opm.gov

Subject Fwd: Agency Information **[Contains CUI]**

CUI//SP-PRVCY//FED ONLY

Please see the note from NARA.

---------- Forwarded message ---------
From: Lorem Ipsum <lorem.ipsum@nara.gov>
Date: Mon, May 14, 2018 at 6:20 AM
Subject: Agency Information [Contains CUI]
To: Random Employee <Random.Employee@opm.gov>

CUI//SP-PRVCY//FED ONLY

This example shows how the original recipient carried forward the CUI marking from an original email to a new email

Receiving CUI

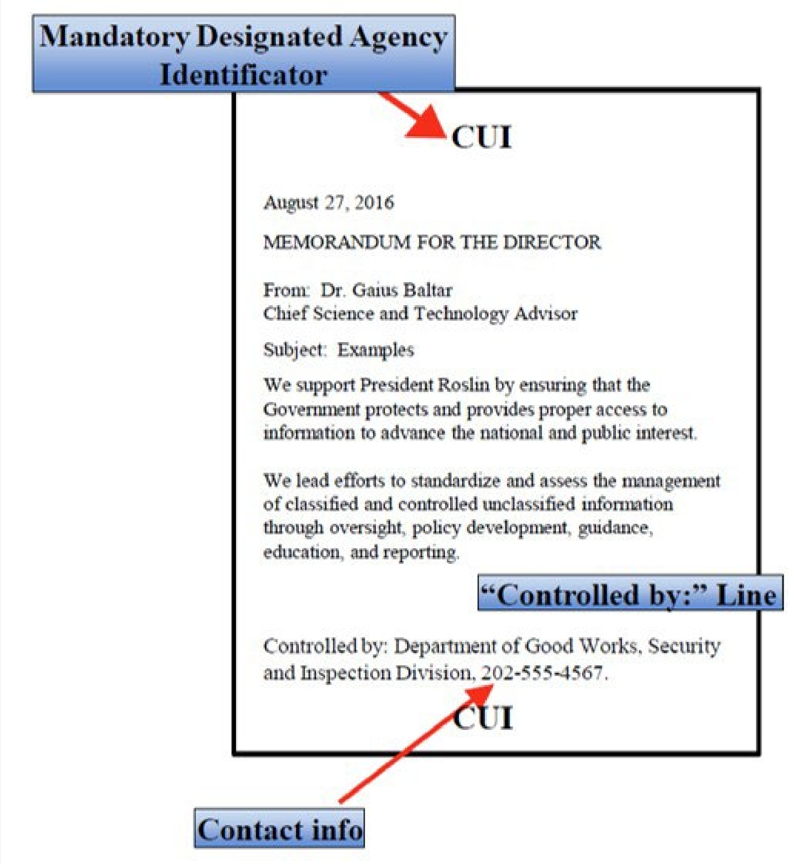
Receiving marked legacy information when the recipient HAS implemented the CUI Program:

- If receiving agency plans to reuse or transmit the legacy marked information to another agency, **then it must evaluate the information and remark it as CUI as appropriate.**
- If Applicable, the receiving agency must also adhere to any agency marking waivers as they apply to internal dissemination.
- If applicable , the receiving agency should apply any appropriate Limited Dissemination Control Markings (LDCMs).
- Reviewing agencies should not reuse legacy markings, such as FOUO or SBU, on new documents that are derived from marked legacy information.
- Agencies should contact the originator of the material if they have any questions.

All Executive Branch agencies are mandated to have a CUI program

- Agriculture
- Commerce
- Defense
- Education,
- Energy
- Health and Human Services
- Homeland Security
- Housing and Urban Development
- Interior
- Justice
- Labor
- State
- Transportation
- Treasury
- Veterans Affairs

Designation Indicator


Mandatory Designated Agency Identificator
"Controlled by:" Line
Contact info

CUI

August 27, 2016

MEMORANDUM FOR THE DIRECTOR

From: Dr. Gaius Baltar
Chief Science and Technology Advisor

Subject: Examples

We support President Roslin 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 by: Department of Good Works, Security and Inspection Division, 202-555-4567.

CUI

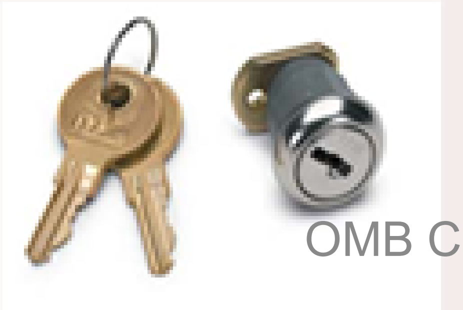
Designation Indicators, sometimes called a “controlled by” line, show which agency made the document CUI and are mandatory

It is best practice to include the **contact information of the designating agency** and **identify a point of contact or division within the organization.**

Safeguarding, Decontrolling, and Destruction of CUI

This section will focus on CUI: Controlled Physical Environments, Information systems and Disposal and Destruction

Controlled Physical Environments



CUI must be stored or handled in controlled environments that include at least one physical barrier, such as:

Sealed envelope

Locked:

- Doors
- Overhead bins
- Drawers
- File Cabinets

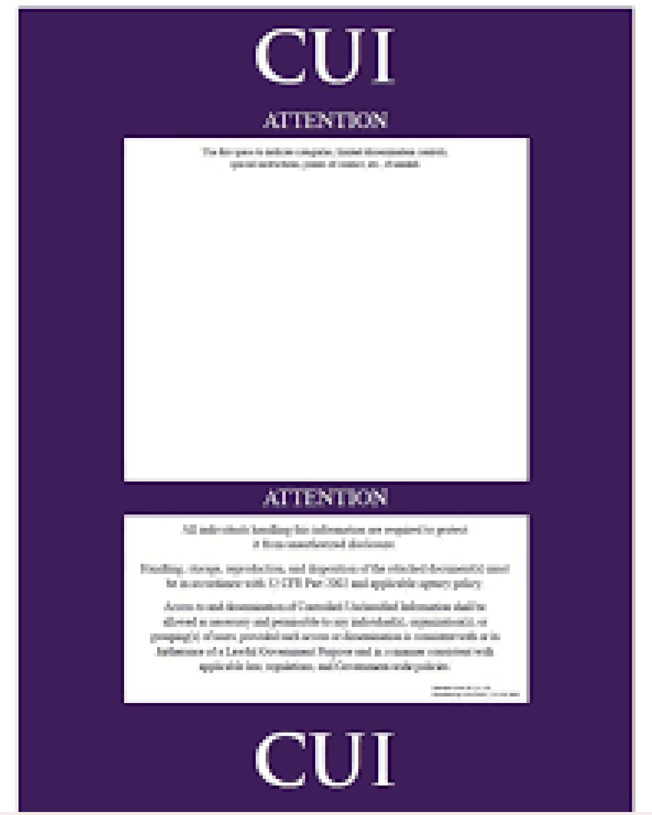
Areas equipped with electronic locks

- Authorized telework employees must store CUI materials using the guidance above while working off-site.

CUI Cover Sheet

- Agencies may use a coversheet to identify CUI, alert observers that CUI is present from a distance, and serve as shield to protect CUI from inadvertent disclosure. If an agency chooses to use a coversheet, it must use CUI EA-approved coversheet Standard Form 901.

- Cover sheets (SF901) and media labels (SF902) are available for download or purchase through the GSA website



CUI

ATTENTION

Use this space to indicate categories, limited dissemination controls, special instructions, points of contact, etc. (if needed).

ATTENTION

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 Controlled Unclassified Information 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.

[illegible]

CUI

Controlled Information Systems

All Controlled Information systems should have at least **one barrier**, such as:

- Dedicated network drives
- File folders
- Intranet sites

CUI Disposal And Destruction

- Ensure that a receptable is approved for the disposal of CUI:
  - Locked
  - Labeled for destruction of CUI
- Paper media should be destroyed in a manner that renders it:
  - Unreadable
  - Indecipherable
  - Irrecoverable
- You must either dispose of CUI in an approved receptacle or destroy the document according to NIST SP-800-88, standards.
  - Clear
  - Purge
  - Destroy (Preferred)

Approved for the destruction of Controlled Unclassified Information
Lock

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

CUI Incident Reporting

This section will define: What constitutes a CUI Incident and the reporting procedures

What is a CUI Incident?

Reportable CUI Incidents include, but are not limited to:

- **Any** knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of CUI
- **Any** knowing , willful , or negligent action to designate information as CUI contrary to the requirements of E.O 13556, and its implementing directives
- **Any** incident involving computer or telecommunications equipment or media that may result in disclosure of CUI to unauthorized individuals, or that results in unauthorized modification or destruction of CUI system data, loss of CUI computer system processing capability, or loss or theft of CUI computer system media

Reporting a CUI Incident

Suspected or confirmed misuse of CUI shall be reported via the bureau’s incident response process and to the bureau’s **CUI POC within 1 hour of discovery.**

The CUI POC shall obtain the details of the situation, coordinate with a subject matter expert regarding the severity of the incident.

The CUI POC will coordinate mitigation measures as appropriate within their incident response and management structures and provide regular status reports to the CUI PM until mitigation efforts are complete.

CUI Resources

- For more information visit the CUI Commerce Connection Website
- Please contact the DOC CUI Team with any questions or additional training inquiries at: CUI@doc.gov

- Please Scan the QR or use the CUI Training Feedback Form to provide feedback on this training:

Bureau CUI Points of Contact

BEA
Randy Carlson
Frederick.Carlson@bea.gov

BIS
Julie Lee
hajeang.lee@bis.doc.gov

Census
Harold Saintelien
harold.saintelien@census.gov

FirstNet
Enas Qutob
Enas.qutob@firstnet.gov

ITA
Ericka Ukrow
Ericka.Ukrow@trade.gov

NIST
Wade A. Deuter
wade.deuter@nist.gov

NOAA
William “Bill” Rogers
william.g.rogers@noaa.gov

NTIA
Gale Newton
GNewton@ntia.gov

NTIS
Wade A. Deuter
wade.deuter@nist.gov

OIG
Catherine Findlay
Cfindlay@oig.doc.gov

EDA, MBDA, OS, OUSEA
Sean Flowers
sflowers@doc.gov

USPTO
Lisa Lawn
Lisa.lawn@uspto.gov

Congratulations!

To receive credit for the FY26 CUI Basic User Awareness Training, please complete the CUI Training Quiz.

You must receive a score of 80% or higher to receive a completion certificate.