GSA

Controlled Unclassified Information

CUI Tech Talk

August 18, 2021

Karen Overall and Andy Riordan
GSA Privacy Office

The CUI Program

Purpose

- Standardize how agencies handle, share, mark, and destroy sensitive info that requires safeguarding.
- Replace 100+ markings currently in use
- **Mandated** by Executive Order 13556 (estab program/appt NARA as ISOO) and 32 CFR Part 2002 (ISOO CUI Policy for Exec Agencies).

Benefits

- Same process for all Executive Branch agencies
- Stronger protections (vs FOUO, SBU, Confidential, Restricted, etc)
- Easier sharing

If there's no law, reg, or Govt policy that says the info should be protected, it's not CUI.

CUI Includes PII and Replaces SBU

- **PII follows Privacy Act rules**
  - Generally no changes
  - New CUI-specific markings (ex: CUI//SP-PRVCY)
  - Stronger destruction methods
  - PII falls within the “General Privacy” Category - doesn’t include Personnel Records which are a separate category
- **SBU (Sensitive But Unclassified) terminology and markings should not be used**
  - Sensitive building information that was SBU is now CUI (see GSA Order PBS 3490.3 CHGE 1 - order to protect Fed Bldg info, grounds, property, etc.)
  - “Business Need to Know” is now termed “Lawful Government Purpose”
- **CUI is a new Program but encompasses many existing processes** so it could be that your processes won’t need to change much, but CUI markings will need to be added.

IT System Requirements

- Minimum Requirements:
  - FIPS 199 **Moderate** categorization of the application/system
  - Limited access to authorized users
  - System **Warning Banner** to notify people that there is CUI in the application/system
  - **Banner Markings** to be included on any extracted information (automatically or manually marked)

- Optional
  - Persistent banner on all screens
  - Automatic Marking Tool

More on InSite

Citrix VDI and WinZip

- When emailing CUI, put it in an attachment.
  - If sending within GSA network (gsa.gov) no encryption is required.
  - When emailing outside of GSA.gov it must be encrypted compliant with FIPS 140-2. For GSA that means using WinZip FIPS available through Citrix VDI.
- Include the applicable CUI Marking at the top of the email. Optional to add "Contains CUI" at the end of the Subject line.
- Before sharing CUI make sure the recipient has a Lawful Government Purpose to know the information.
- When faxing, be sure the recipient is available to get the fax immediately.

More on InSite

CUI Basic vs. CUI Specified

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.

More on InSite

Marking CUI

- CUI Markings must be on **every printed page**: top, centered, bolded, and all in caps
- GSA uses the banner marking “CUI” for ***CUI Basic*** (other agencies may use “CONTROLLED” instead)
- CUI Basic and CUI Specified have different markings. ***CUI Specified*** requires the Category name in the banner. Two slashes are used to separate CUI from the Specified Category abbreviation (e.g., CUI//SP-PRVCY)
- Designating Agency information must appear on the front page of CUI docs (can be via letterhead, or an office name and email, or specific POC info, etc.)

More on InSite

Waivers to Marking CUI

The requirement to mark CUI **may be waived in certain situations** including:

- When marking would be excessively burdensome due to large quantities or the nature of the CUI (must remain within GSA);
- Exigent circumstances when sharing outside GSA (must still be protected per CUI guidance);
- Legacy information with old markings (unless & until made active again; must remain within GSA).

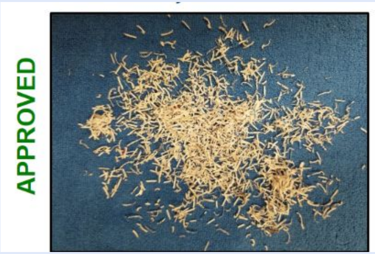
To request a waiver, email the CUI team at cui@gsa.gov

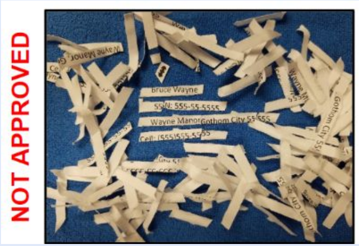
NOTE: If you deal with other agencies who create/own CUI,
work with them to get familiar with their processes and markings.

More on InSite

Destruction

CUI must be destroyed in a manner that makes it **“unreadable, indecipherable, irrecoverable”.**





Approved for the destruction of Controlled Unclassified Information
Lock

- Look for approved destruction bins to deposit CUI materials.
- Never use trash cans or recycling bins to dispose of CUI

- Regular cross-cut shredders aren't sufficient (CUI must be destroyed to at least **1mm x 5mm** particles).
- GSA has compliant **shredders** and/or approved CUI **locked storage bins** (for contractor shredding) in Central Office and ROBs.
- **Do not put CUI in the trash or in recycling bins.**

Best practice: DON’T PRINT!

But if it’s necessary to print CUI, you must destroy it properly, or return it to an office that has approved shredding capability.

More on InSite

Incident Reporting

- **What to do if you:**
  - Find CUI laying around;
  - Discover CUI that’s not marked properly;
  - Learn CUI was sent to the wrong person by mistake; or
  - Catch unencrypted CUI emailed outside of the GSA Network.
- **Call the IT Service Desk as soon as you suspect an issue!**

Reference the IT Security Incident Response Guide located on this page for more details.

More on InSite

GSA

CONTROLLED UNCLASSIFIED INFORMATION

For More Information

Sign up for an AMA - Aug 19, Aug 24, Sep 2

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 webpage - InSite.gsa.gov/cui
- GSA’s CUI Chatter group
- GSA's CUI Policy
- GSA’s Draft CUI Guide

Contact us: cui@gsa.gov