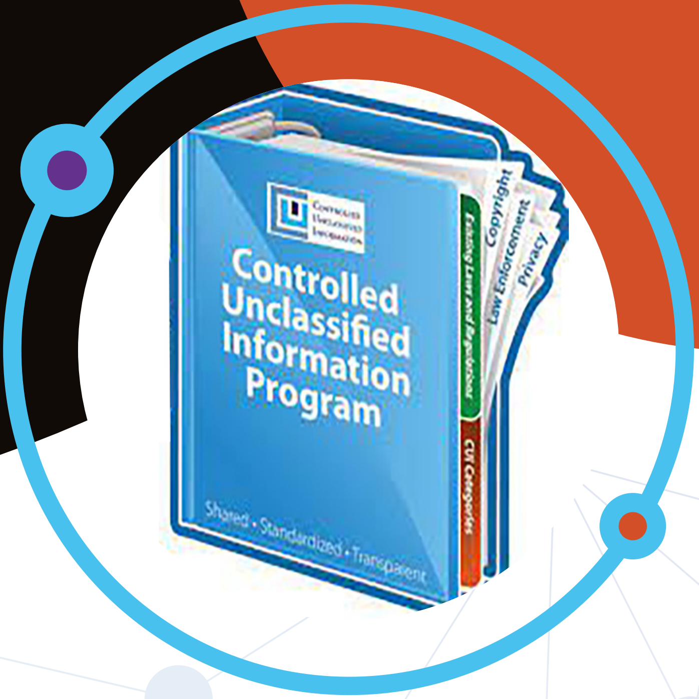
LIS SOLUTIONS

SECURITY MONTHLY NEWSLETTER

JUNE2023


Controlled Unclassified Information Program
Shared • Standardized • Transparent
Copyright
Law Enforcement
Privacy
Existing Laws and Regulations
CUI Categories

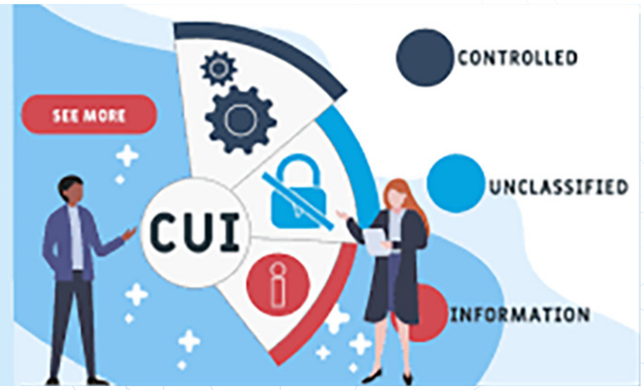
CONTROLLED UNCLASSIFIED INFORMATION (CUI)

CUI (Controlled Unclassified Information) is information that is not considered "SECRET, or TOP Secret, etc. However, it IS sensitive data and still requires protection. It is the type of information that may be found in Personally Identifiable Information (PII), Proprietary Business Information (PBI), technical information, law Enforcement Sensitive (LES), contracts, etc.; basically, any government information that is not meant for general public consumption.

As stated in the Title 32 CFR, CUI can be as follows:

- Information the Government creates or possesses;
- Information another entity creates or possesses on behalf of the Government.

Examples of CUI include defense critical infrastructure information, export-controlled information, information related to sensitive international agreements, and law enforcement information. Information that does not qualify as CUI is classified, not created by, or not under the control of the U.S. Government such as, a non-executive branch journal article on counterinsurgency.



IT and End User Perspective and Responsibility

CUI is handled, stored, transmitted, and destroyed in a similar manner to the legacy For Official Use Only (FOUO) program. It should be processed on government furnished equipment, encrypted if sent via Non-classified Internet Protocol Router Network (NIPRNet), and only accessible on a limited basis to those with a lawful Government purpose.

It must be destroyed by means approved for destroying classified information or in a manner making it unreadable, indecipherable, and irrecoverable. After working hours, CUI can be stored in unlocked containers, desks, or cabinets if the Government building provides security for continuous monitoring of access. If there is no building security, the information must be stored in locked desks, file cabinets, bookcases, locked rooms, or similarly secured areas.

CUI information may be found in physical documents or in computer files. Properly marked CUI in either form should normally be marked as CUI, however, you may run into documents that are NOT marked.

If you receive unmarked documents that, to you, seem like they should be considered CUI, you should notify whoever provided you with the document(s), asking for guidance & unless clearly and officially informed it is NOT CUI, you should protect it as if it IS CUI. (Note: Even though it may not be officially considered CUI, information unrelated to the government can still be sensitive to your client, vendor, or your own organization and should be treated just as carefully.)

Some methods an individual should use to protect CUI are:

- Limit access to only those with a legitimate need/purpose.
- When not in use, store physical documents in a secure area such as locking cabinets, drawers, or rooms.
- Any computer should be either logged-out or have the Console locked if the user will be away from it for any reason.
- Users should maintain an awareness of their surroundings including others present, blocking any CUI documents from view when necessary.
- Computers should be stored in a secure location when not in use.
- Do not share computers or login information.
- Keep computer Operating Systems and applications up to date with any security updates.
- Install and keep Antivirus software up to date.
- Use care when visiting Internet sites, providing private information, including (but not limited to) login information or CUI of any kind.
- Change passwords frequently.
- Use Multi-Factor Authentication (MFA), or Two Factor Authentication (2FA) as an additional layer of login security. MFA can take a number of forms including texts being sent to a pre-selected cell phone with a private code, or a USB "key" device, sometimes known as a "Dongle" that must be inserted into a USB port on the computer, or a badge or other card that may need to be inserted into a SD Card slot on, or attached to, the computer. Any dongles, badges, SD cards should be kept securely stored when not in active use & should be removed if a user will be stepping away from the computer.
- Encrypt any data being sent over the Internet.
- Escort visitors, monitor their activity, and maintain logs of visitors & their activity/access.
- Depending upon the instructions/requirements of a client, all CUI documents (physical or in computer file format) should be returned to the appropriate representative of the providing organization, or securely shredded or deleted.

These methods of CUI protection often make doing work less convenient, however, the impact of release of CUI can not only cause your organization to be blocked from working with a government agency in the future, but also cause harm to any organization or individual whose information was released.

If you have any questions about your role in CUI protection, contact your security professionals at LIS Solutions at **security@lissol.com**.

WHAT EXACTLY IS CUI? (AND HOW TO MANAGE IT)

by Mark Knowles | Mar 24, 2022

"It certainly sounds official—like it might be the subject of the next action-packed, government espionage, Jason Bourne-style thriller. Or maybe put it before the name of a racy city and have your next hit crime series. A history of mysterious aliases like "official use only", "law enforcement sensitive", and "sensitive but unclassified" only adds to the intrigue. "

"So, what exactly is CUI, and why should your company care? Hint alert—obtaining a government contract could depend on how your organization addresses CUI, so for many it's a topic worthy of discussion."

"CUI, or controlled unclassified information, didn't have much of an established identity before 2010. It went by any number of aliases and took a back seat to the more glamorous classified category. However, should CUI fall into the wrong hands, something as serious as national security could be at risk. This article will explore CUI—what it is, why it's so important, how CUI management is changing, and the single most important action your company can take to properly manage CUI today."

Continue reading article at: **https://hyperproof.io/resource/what-is-cui/**