CONTROLLED UNCLASSIFIED INFORMATION (CUI)

Do you know what CUI is? Can you identify CUI or know how to protect it against potential risks?

Currently, Federal agencies develop, use, store, and share sensitive information that may not be handled with the strict standards of classified materials such as national security or atomic energy information. Nonetheless, this information does require a certain level of protection from unauthorized access and release. The Information Security Oversight Office's (ISSO) Title 32 Part 2002 (CUI) Code of Federal Regulations (CFR) Final Rule was published on September 14, 2016. This Final Rule serves as the "Implementing Guidance" for the CUI Program.

You can access and read that letter at: **https://www.cdse. edu/Portals/124/Documents/jobaids/information/ISOO-letter.pdf?ver=gG7RNV_vCpQDXvpr4fGE_w%3d%3d**

If you are an authorized holder of a document or material, you are ultimately responsible for determining whether the information falls into a CUI category at the time of creation. If so, you are responsible for applying CUI markings and dissemination instructions accordingly. All individuals, no matter their current designation (DOD civilian, contractor, or military personnel), who provide support to the DOD are to comply with the requirements in DOD Instruction (DODI) 5200.48 - Controlled Unclassified Information, (March 6, 2020). This instruction establishes policy, assigns responsibilities, and prescribes procedures for CUI safeguards throughout the DOD.

There are two types of CUI standards:

Authorized holders must safeguard CUI using one of the following types of standards:

1. **CUI Basic:** CUI Basic is the default set of standards authorized holders must apply to all CUI unless the CUI Registry annotates CUI Specified.

2. **CUI Specified:** Authorized holders safeguard CUI Specified in accordance with the requirements of the underlying authorities indicated in the CUI Registry.

SAFEGUARDING CONTROLLED UNCLASSIFIED INFORMATION:

LIS Solutions Employees are required to protect CUI in accordance with the requirements under the basic level of safeguard and dissemination unless specifically identified otherwise in a law, regulation, or government-wide policy. During working hours, it is imperative to take proactive steps to actively minimize the risk of access by unauthorized personnel, such as not reading, discussing, or leaving CUI unattended where unauthorized personnel are present. The use of CUI coversheets is optional but highly recommended when protecting and safeguarding CUI.

After use and during non-working hours, CUI material will be stored in secured desks, file cabinets, bookcases, locked rooms, or similarly access-controlled areas. These protections provide a controlled environment with internal security measures in place to detect unauthorized access to CUI.

To learn more and to take the Controlled Unclassified Information course, please use the link below:
https://securityawareness.usalearning.gov/cui/index.html

CONTROLLED UNCLASSIFIED INFORMATION
REPLACES "FOR OFFICIAL USE ONLY" DESIGNATION

CUI

APPROVED

LIS Solutions
Analyze. Inform. Empower.

718-237-8919 • info@lissol.com