Controlled Unclassified Information

The Program, Implementation, and Features

Shared • Standardized • Transparent

Information Security Oversight Office (ISOO)

Agenda

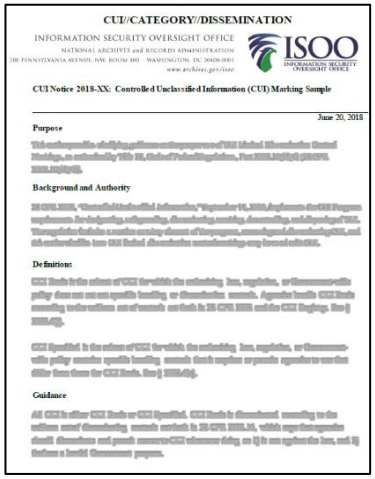
SLIDES ARE AVAILABLE FOR DOWNLOAD ON THE CUI BLOG

- CUI and Metadata (update)
- CUI Federal Acquisition Regulation case (update)
- NIST SP 800-172 (update)
- NIST SP 800-171A and CUI Notice 2020-04 discussion
- Recent CUI Notices (2020-06 and 7)
- Live Question and Answer period

A CUI Metadata Standard

A CUI Metadata Standard

- NIEM is in the process of refining and preparing to release NIEM 5.0 which contains the CUI metadata markings.
- A Standard, not the standard.
- Metadata Marking CUI is not required though it is encouraged to be used by agencies when needed to protect and track CUI.


CUI//CATEGORY//DISSEMINATION

INFORMATION SECURITY OVERSIGHT OFFICE
NATIONAL ARCHIVES and RECORDS ADMINISTRATION
700 PENNSYLVANIA AVENUE, NW, ROOM 100 · WASHINGTON, DC 20408-0001
www.archives.gov/isoo

ISOO
INFORMATION SECURITY OVERSIGHT OFFICE

CUI Notice 2018-XX: Controlled Unclassified Information (CUI) Marking Sample

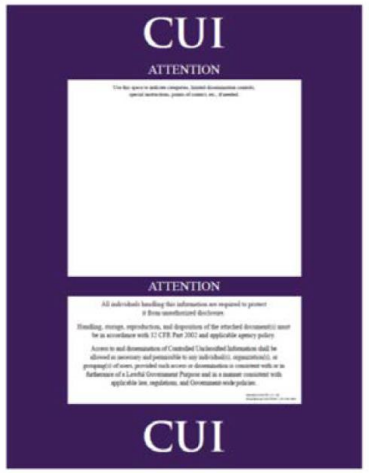
June 20, 2018

Purpose

Background and Authority

Definitions

Guidance



CUI FAR Case

CUI FAR Case

- Currently in drafting process with GSA. **Projected** public comment period from March – May 2021.
- ISOO will host an ad hoc CUI Stakeholder meeting during the public comment period to answer questions about content and intent of draft FAR language.
- More information can be found in the Unified Agenda.

RIN: 9000-AN56: https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202010&RIN=9000-AN56

NIST SP 800-172

Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171

Provides an enhanced security requirements to help protect the confidentiality, integrity, and availability of Controlled Unclassified Information (CUI) associated with critical programs or high value assets in nonfederal systems and organizations from the advanced persistent threat (APT).

The enhanced security requirements, as identified and selected by a federal agency, can be implemented in addition to the basic and derived requirements in NIST SP 800-171 since those requirements are not designed to fully address high-end threats such as the APT.

NIST SP 800-171a and CUI Notice 2020-4

- "When any entity assesses compliance with the security requirements of NIST SP 800-171, they must use the NIST SP 800-171A procedures to evaluate the effectiveness of the tested controls. NIST SP 800-171A is the primary and authoritative guidance on assessing compliance with NIST SP 800-171" (CUI Notice 2020-4).
- "Each agency is responsible for taking appropriate steps to minimize redundant and duplicative security inspections and audit activity. Agencies may execute appropriate interagency agreements to avoid or minimize redundant and duplicative oversight actions by agencies or internal component elements" (CUI Notice 2020-4).

CUI Notice 2020-06

Limited Marking Waiver Best Practices to Alert Users of CUI

Provides guidance to agencies on how to alert users to the presence of CUI when they have issued a limited marking waiver. Users should be aware of CUI on the system and how to handle that CUI if it is removed from the system.

- Informational banners
- Warning boxes / notifications / splash screens
- Training and awareness
- User access agreements

CUI Notice 2020-07

Using Alternate Designation Indicators (ADI) with CUI

If permitted by, and in accordance with, agency authorities and applicable laws or regulations, CUI Senior Agency Officials (SAO) may authorize the use of alternate designation indicators that don't directly identify their agency.

- These ADIs must be documented and reported to the CUI EA.
- The ADI must still provide sufficient information to enable recipients to know whom to contact regarding the information.
- ADIs must be reviewed periodically to ensure they are still needed and are being applied correctly.

DoD Resources for CUI/CMMC/DFARs 7012

- DoD CUI Website: DoDCUI.mil
- Contract compliance questions should be addressed to the Contract POC
- DFARs 7012 compliance questions: Use DoD Procurement Toolbox https://dodprocurementtoolbox.com (Click on the Cybersecurity Tab)
- Questions about CMMC: https://www.acq.osd.mil/cmmc/
- CDSE CUI Toolbox: https://www.cdse.edu/toolkits/cui/index.php
- DCSA CUI Page: https://www.dcsa.mil/mc/ctp/cui/

Open Q&A

(Please follow instructions to submit questions via chat or phone)