Controlled Unclassified Information

The Program, Implementation, and Features

Shared • Standardized • Transparent

ISOO
INFORMATION SECURITY
OVERSIGHT OFFICE

Information Security Oversight Office (ISOO)

Agenda

SLIDES ARE AVAILABLE FOR DOWNLOAD ON THE CUI BLOG

- CUI and Metadata (Update)
- The CUI FAR case (Update)
- Recent / Planned CUI Notices / Memos

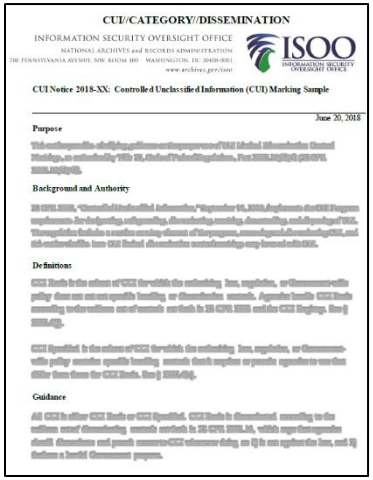
  Published: Non-Disclosure Agreement Template

  Planned: Using an Exigent Circumstances Waiver
- FAQs
- Upcoming Events
- Time for Questions and Answers.

Information Security Reform

A CUI Metadata Standard

- Public Comments are being adjudicated
- Notes on the types of comments
- A Standard, not the standard
- Metadata Marking CUI Not required



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

[illegible]

Background and Authority

[illegible]

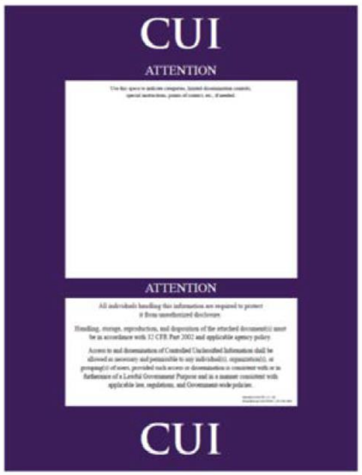
Definitions

[illegible]

[illegible]

Guidance

[illegible]



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.

CUI

CUI FAR Case (No Change)

- Currently in draft
- Working with GSA
- Status can be found on the Unified Agenda
- RIN: 9000-AN56 (https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=201910&RIN=9000-AN56)

CUI Notice 2020-1 “Implementation Deadlines”

Awareness campaign - **June 30, 2020**

Policy – **December 31, 2020**

If an agency has sub-agencies, all those subordinate components must develop and publish implementing policies and/or modify or rescind all affected policies by **June 30, 2021.**

Classification marking tools and commingling – **December 31, 2020**

Agencies that manage, own, or control Classification Marking Tools (CMT) must **initiate** any modification of such CMTs by this date.

Training – **December 31, 2021**

CUI training may be incorporated into existing agency training (such as privacy, information systems, or records management training).

Physical safeguarding – **December 31, 2021**

Information systems – **December 31, 2021**

Information systems that are used to store, process, or transmit CUI must be configured at no less than the Moderate Confidentiality impact value (see 32 CFR 2002.14).

Reporting and Extensions

Agencies that anticipate delays in implementing any of the above deadlines must include a narrative in their annual report submission that describes the issue giving rise to the delay. They must also include a copy of their implementation plan or strategy. ISOO will evaluate and formally approve delays on a case-by-case basis and may report such delays to the President.

CUI Notice 2020-03

Non-Disclosure Agreement Template for CUI

- Note: Although using the template is optional, ISOO strongly encourages agencies to make use of theform to increase standardization across the executive branch and in contracts.

Key Points:

- This Notice provides an optional Controlled Unclassified Information (CUI) non-disclosure agreement (NDA) template for executive branch agency use.
- Executive branch agencies may use the attached template when they determine that a CUI NDA is appropriate. The attached template is optional, and agencies can modify it if needed.
- ISOO will pursue developing a standard form or optional form to replace this template. Agencies are encouraged to provide us with samples of non-disclosure agreements used for CUI, feedback on aspects of the form that do not meet your agency's needs, and any modified language your agency may develop if it uses this form as a starting point. We will use this and other feedback to inform development of the formal form.

CUI Notice 2020-04:

Assessing Security Requirements for CUI in Non-Federal Information Systems

Key Points:

- 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.
- Scope: systems and components that an entity uses to store, process, or transmit CUI.
- Reciprocity: 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.

Planned Notices

CUI and Exigent Circumstances

- A generalized version of the CUI Memo 2020-03-30 that will discuss the use of the CUI Exigent Circumstance Waiver and applicability in situations other than in response to the COVID-19 Pandemic.

FAQs

Q: Is system [NAME OF SYSTEM OR APPLICATION] approved for CUI?

A: The CUI office is unable to verify individual systems or applications compliance with the CUI cybersecurity requirements.

Q: I don’t know what information I have that is CUI, how can I find out? (usually asked by contractors).

A: Usually the contractor is asking about how to comply with DFARs 7012 clause, and as such must check their contract and reach out to the contract POC with any questions. Also check some of DoDs available resources (like DoDProcurementToolbox).

FAQs (Continted)

Q: How do I mark CUI?

A: Understanding how to mark CUI requires knowledge of the principles in the CUI Marking Handbook and Agency guidance or training. Both are necessary because there is some flexibility given to agencies with regards to marking.

Q: Does my email system have to be CUI compliant? (from a contractor)

A: Check the terms of the contract, but likely only if it is used to store, process, or transmit CUI, this is likely a decision made when deciding on boundaries and scoping for the SSP.

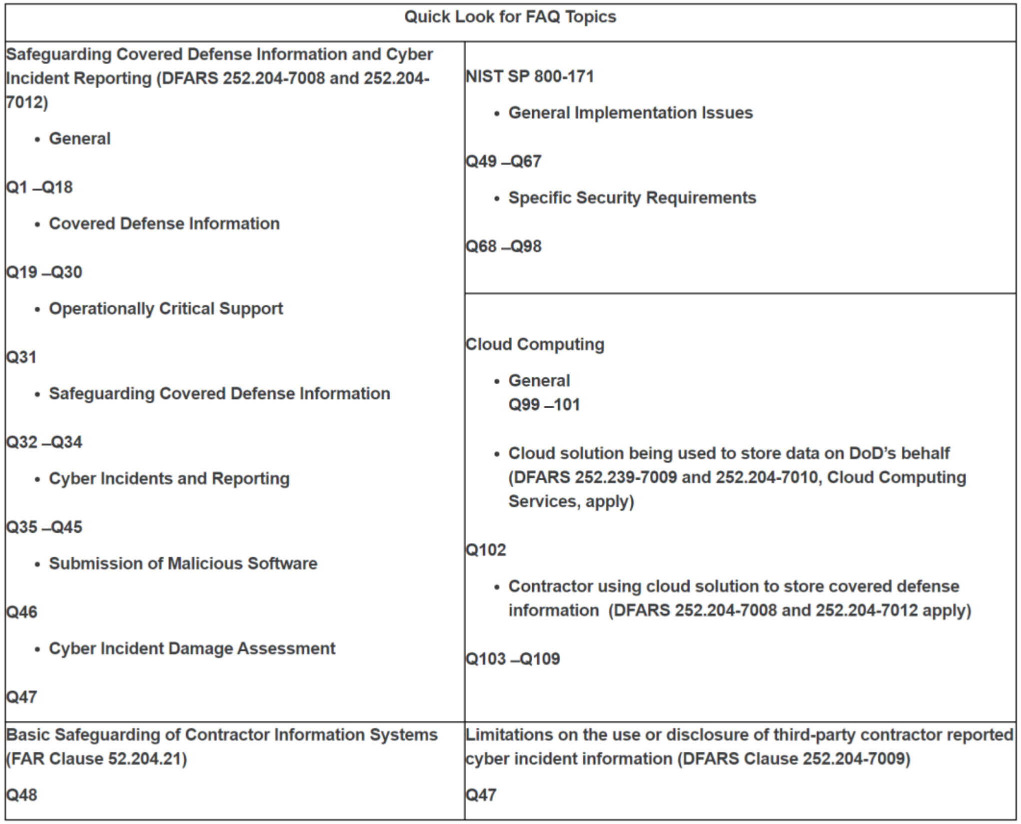
DoD Resources for CUI/CMMC/DFARs 7012

- 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/

DoD Procurement Toolbox

Q13: Who in DoD can I contact for clarification on DFARS 252.204-7012 or NIST SP 800-171 in support of DFARS 252.204-7012?

A13: Contractors should email their query to osd.dibcsia@mail.mil. Emails received at this address are reviewed daily and distributed as appropriate to a cross-functional team of subject matter experts for action.



Quick Look for FAQ Topics	
Safeguarding Covered Defense Information and Cyber Incident Reporting (DFARS 252.204-7008 and 252.204-7012) • General Q1 –Q18 • Covered Defense Information Q19 –Q30 • Operationally Critical Support Q31 • Safeguarding Covered Defense Information Q32 –Q34 • Cyber Incidents and Reporting Q35 –Q45 • Submission of Malicious Software Q46 • Cyber Incident Damage Assessment Q47	NIST SP 800-171 • General Implementation Issues Q49 –Q67 • Specific Security Requirements Q68 –Q98
	Cloud Computing • General Q99 –101 • Cloud solution being used to store data on DoD's behalf (DFARS 252.239-7009 and 252.204-7010, Cloud Computing Services, apply) Q102 • Contractor using cloud solution to store covered defense information (DFARS 252.204-7008 and 252.204-7012 apply) Q103 –Q109
Basic Safeguarding of Contractor Information Systems (FAR Clause 52.204.21) Q48	Limitations on the use or disclosure of third-party contractor reported cyber incident information (DFARS Clause 252.204-7009) Q47

https://dodprocurementtoolbox.com
Click on the Cybersecurity Tab

Upcoming Event:

CUI Marking Fundamentals (online class) August 28 11-1:00 ET

- Provides an overview of the principles of marking in the unclassified environment.
- Note: Do not use CUI markings until directed to in agency policy/training (for federal personnel) or contracts/agreements (for non-federal entities) .

Common Question: "When is FOUO (or other legacy markings) going away?"

Answer: Legacy markings will continue be used until an agency transitions to using the CUI markings. After that legacy markings will continue to coexist with CUI Markings in accordance with the requirements of Legacy Marking Waivers, that agencies may apply.

Open Q&A

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