

# Controlled Unclassified Information

*The Program, Implementation, and Features*

Shared • Standardized • Transparent



Information Security Oversight Office (ISOO)



# Information Security Reform

## A CUI Metadata Standard

- Currently in draft
- Working with NIEM and will likely include new CUI Domain
- Still being circulated to SMEs
- Will go out for Public Comment

## CUI FAR Case

- 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.

## Applying an Exigent Circumstances Waiver to CUI Safeguarding Requirements while Teleworking in Response to the COVID-19 Pandemic

Note: “This memorandum does not have the force and effect of law and is not meant to bind the public, except as authorized by law or regulation or as incorporated into a contract....”

### Key Points:

- CUI program office should be involved in any risk-accepting decisions
- CUI must be safeguarded at all times
- In exigent circumstances, the CUI Program provides an avenue for agency heads or CUI Senior Agency Officials (SAO) to waive safeguarding provisions
- The CUI SAO must detail in each waiver which CUI is covered by the waiver, which safeguarding provisions or requirements the agency is waiving for that CUI, and the alternate or compensatory protection methods the agency will employ instead to protect that CUI

# 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.

## Non-disclosure Agreement Template

- Intended to provide a template/language to use in non-disclosure agreements (NDAs) covering CUI. Agencies using other/existing agreements may continue to use them, this is being created to assist agencies that wanted to update or formalize their NDA practices to align with their CUI programs.

# CUI and Teleworking / web-conferencing

- **NSA Article: “Working from Home? Select and Use Collaboration Services More Securely”**  
<https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/2163484/working-from-home-select-and-use-collaboration-services-more-securely/>
- **General guidelines to consider as you telework with CUI:**
  - CUI should not be stored on personal systems.
  - Printing and hard copy storage should be kept to a minimum.
  - Agency sponsored/ approved virtual desktops (or similar) should be used.
  - Personal email accounts should not be used to store or transmit CUI.

# FCI and CUI, what is the difference?

## Blog post on the way! (Venn diagram included)

Both CUI and FCI include information created or collected by or for the Government, as well as information received from the Government. But, while FCI is any information that is "not intended for public release," CUI is information that requires enhanced safeguarding.

**Common Question:** "Is (name of application) certified for CUI?"

**Answer:** There is no program wide certification process for applications or systems. Any system used to store, process, or transmit CUI must meet the moderate confidentiality baseline from NIST SP 800-53 or NIST SP 800-171 as applicable.

# Questions about DoD Implementation

1. **Contract compliance** questions should be addressed to the Contract POC
2. **DFARs 7012** compliance questions: Use DoD Procurement Toolbox covered on the next slide
3. Questions about **CMMC**: <https://www.acq.osd.mil/cmmc/>
4. Inquiries about **DoD CUI Program Policies and Implementation** should be addressed to the Office of the Under Secretary of Defense for Intelligence & Security (OUSD I&S)  
Email: [osd.pentagon.ousd-intel-sec.mbx.dod-cui@mail.mil](mailto:osd.pentagon.ousd-intel-sec.mbx.dod-cui@mail.mil)

# 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](mailto: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) <ul style="list-style-type: none"> <li>• General</li> </ul> Q1 –Q18 <ul style="list-style-type: none"> <li>• Covered Defense Information</li> </ul> Q19 –Q30 <ul style="list-style-type: none"> <li>• Operationally Critical Support</li> </ul> Q31 <ul style="list-style-type: none"> <li>• Safeguarding Covered Defense Information</li> </ul> Q32 –Q34 <ul style="list-style-type: none"> <li>• Cyber Incidents and Reporting</li> </ul> Q35 –Q45 <ul style="list-style-type: none"> <li>• Submission of Malicious Software</li> </ul> Q46 <ul style="list-style-type: none"> <li>• Cyber Incident Damage Assessment</li> </ul> Q47	NIST SP 800-171 <ul style="list-style-type: none"> <li>• General Implementation Issues</li> </ul> Q49 –Q67 <ul style="list-style-type: none"> <li>• Specific Security Requirements</li> </ul> Q68 –Q98
Basic Safeguarding of Contractor Information Systems (FAR Clause 52.204.21) <ul style="list-style-type: none"> <li>Q48</li> </ul>	Cloud Computing <ul style="list-style-type: none"> <li>• General</li> <li>Q99 –101</li> <li>• Cloud solution being used to store data on DoD's behalf (DFARS 252.239-7009 and 252.204-7010, Cloud Computing Services, apply)</li> </ul> Q102 <ul style="list-style-type: none"> <li>• Contractor using cloud solution to store covered defense information (DFARS 252.204-7008 and 252.204-7012 apply)</li> </ul> Q103 –Q109
	Limitations on the use or disclosure of third-party contractor reported cyber incident information (DFARS Clause 252.204-7009) <ul style="list-style-type: none"> <li>Q47</li> </ul>

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

## CUI Marking Fundamentals (online class)

- 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.

# Common Question: Legacy Information and Markings



**All legacy information is not automatically CUI. Agencies must determine what legacy information qualifies as CUI**

**Contractors do not have “legacy information” as such. Contractors should protect all information they have received in accordance with the contract that covers that information.**



# Open Q&A

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