



# CUI OVERVIEW FOR THE FSO

An Industry Perspective  
Curtis H. Chappell, ISP®,  
NCMS National Board Member  
Director of Security,  
Thales Defense & Security, Inc.

*20 April 2022  
Spring FISWG/NCMS  
Virtual Training Event*





CUI and CMMC for FSOs & Security Professionals

# CURTIS H. CHAPPELL, ISP®



**CURTIS H. CHAPPELL, ISP®**

NCMS National Board Member  
Vice Chair,  
Government & Industry Committee  
Director of Security,  
Thales Defense & Security, Inc.



[classmgmt.com](http://classmgmt.com)

A graphic for Thales featuring a dark blue background with a glowing globe and network lines. The Thales logo is at the top. Below it is a list of bullet points. At the bottom, there are three circular icons representing Air, Land, and Sea capabilities, followed by the text 'Air • Land • Sea' and 'Lives Depend On What We Do'. There is also a small 'USA' logo with the American flag.

**THALES**

- 20+ years in International Business, Logistics and Security Management
- Director of Security and Corporate FSO for Thales Defense & Security, Inc. (a Proxy Company)
- NCMS National Board Member; Committees: Government & Industry (G&I), CUI and Community Development Committee
- Recipient of multiple James S. Cogswell and DCSA Excellence in Counterintelligence awards

Serving Defense, Federal and Commercial Markets

**Air • Land • Sea**

Lives Depend On What We Do

**USA**





# CUI OVERVIEW



CONTROLLED  
UNCLASSIFIED  
INFORMATION



# CONTROLLED UNCLASSIFIED INFORMATION (CUI)

For the record: "C – U – I"  CORRECT  
"Cooey" ['kōōē]  WRONG

CUI is an "initialism" – an abbreviation consisting of initial letters pronounced separately (e.g. FBI, CIA, DCSA)

NOT...

An acronym, or abbreviation formed from the initial letters of other words and pronounced as a word (e.g. NASA, CFIUS, LASER)



# CONTROLLED UNCLASSIFIED INFORMATION (CUI)

2008

THE WHITE HOUSE  
WASHINGTON

May 7, 2008

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

SUBJECT: Designation and Sharing of Controlled  
Unclassified Information (CUI)

## Purpose

(1) This memorandum (a) adopts, defines, and institutes "Controlled Unclassified Information" (CUI) as the single, categorical designation henceforth throughout the executive branch for all information within the scope of that definition, which includes most information heretofore referred to as "Sensitive But Unclassified" (SBU) in the Information Sharing Environment (ISE), and (b) establishes a corresponding new CUI Framework for designating, marking, safeguarding, and disseminating information designated as CUI. The memorandum's purpose is to standardize practices and thereby improve the sharing of information, not to classify or declassify new or additional information.

The White House

Office of the Press Secretary

For Immediate Release

2010

November 04, 2010

## Executive Order 13556 -- Controlled Unclassified Information

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

"...inefficient, confusing patchwork... resulted in inconsistent marking and safeguarding of documents, led to unclear or unnecessarily restrictive dissemination policies, and created impediments to authorized information sharing. The fact that these agency-specific policies are often hidden from public view has only aggravated these issues."

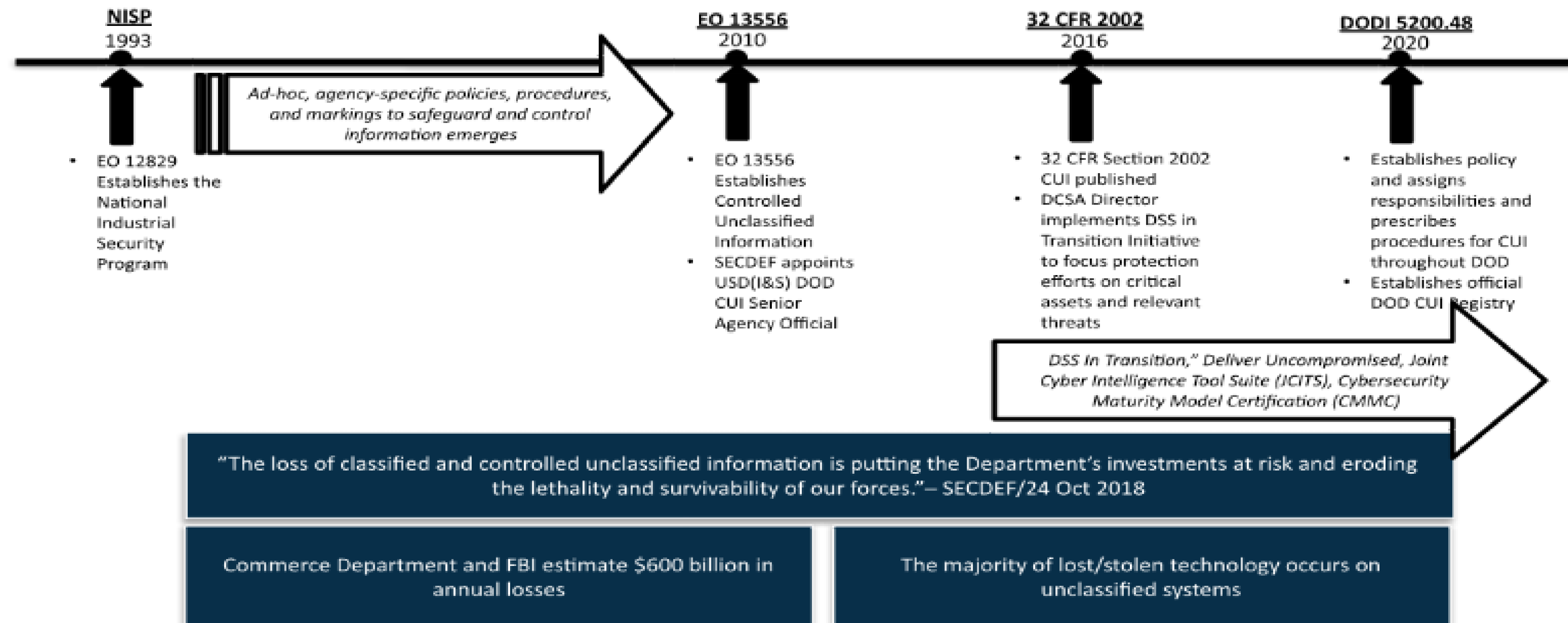
At present, executive agencies have used ad hoc, agency-specific policies, procedures, and markings to safeguard and control this information, such as information that involves privacy, security, proprietary business interests, and law enforcement investigations. This inefficient, confusing patchwork has resulted in inconsistent marking and safeguarding of



# CONTROLLED UNCLASSIFIED INFORMATION (CUI)

UNCLASSIFIED

## CUI Background and History





# CONTROLLED UNCLASSIFIED INFORMATION (CUI)

UNCLASSIFIED

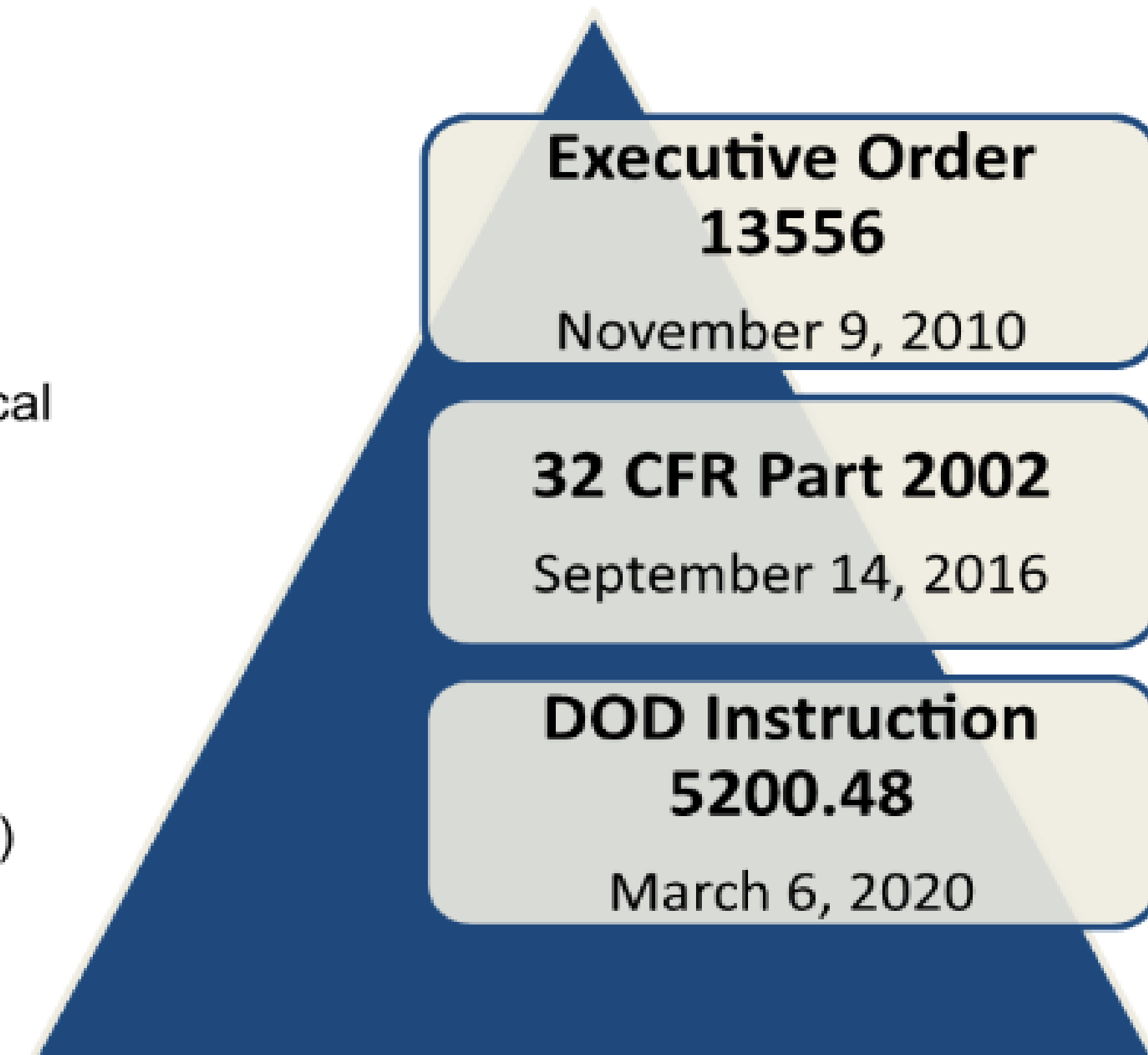
## CUI Overview

### WHAT IS CUI?

- Intended to establish an open and uniform program for managing information that requires safeguarding or dissemination controls
- Replaces FOUO, SBU, LES, and other labels and markings used
- Categories such as Privacy, Tax, Law Enforcement, Critical Infrastructure, Export Control, Financial, and Intelligence information that requires special safeguarding

### WHAT IS NOT CUI?

- Classified information or a classification
- Corporate intellectual property (unless created for or included in requirements related to a government contract)
- Publically available information





# NARA – CUI EXECUTIVE AGENT

 NATIONAL ARCHIVES

[Blogs](#) · [Bookmark/Share](#) · [Contact Us](#)

RESEARCH OUR RECORDS

VETERANS' SERVICE RECORDS

EDUCATOR RESOURCES

VISIT US

AMERICA'S FOUNDING DOCUMENTS

## Information Security Oversight Office (ISOO)

Home > Information Security Oversight Office (ISOO) > About ISOO

About ISOO

[About ISOO](#)

[History](#)

[40th Anniversary](#)

[Our Staff](#)

[Director's Bio](#)

[Our Programs and Groups](#)

[Contact Information](#)

### About ISOO



### Our Mission:

We support the President by ensuring that the Government protects and provides proper access to information to advance the national and public interest. We lead efforts to standardize and assess the management of classified and controlled unclassified information through oversight, policy development, guidance, education, and reporting.

### Our Vision:

- A Government whose information is properly shared, protected and managed to serve the national interest.
- An informed American public that has trust in its Government.

## CUI Guidance Impacts Dozens of Federal and State Agencies



**ISOO mission: Support the President by ensuring that the Government protects and provides proper access to information to advance the national and public interest.**



# OVER 100 TYPES OF UNCLASSIFIED INFORMATION



- For Official Use Only (FOUO)
- Sensitive But Unclassified (SBU)
- Contract Sensitive Information (CSI)
- Sensitive Security Information (SSI)
- Law Enforcement Only (LEO)
- Privacy Act Information / Personally Identifiable Information (PII)

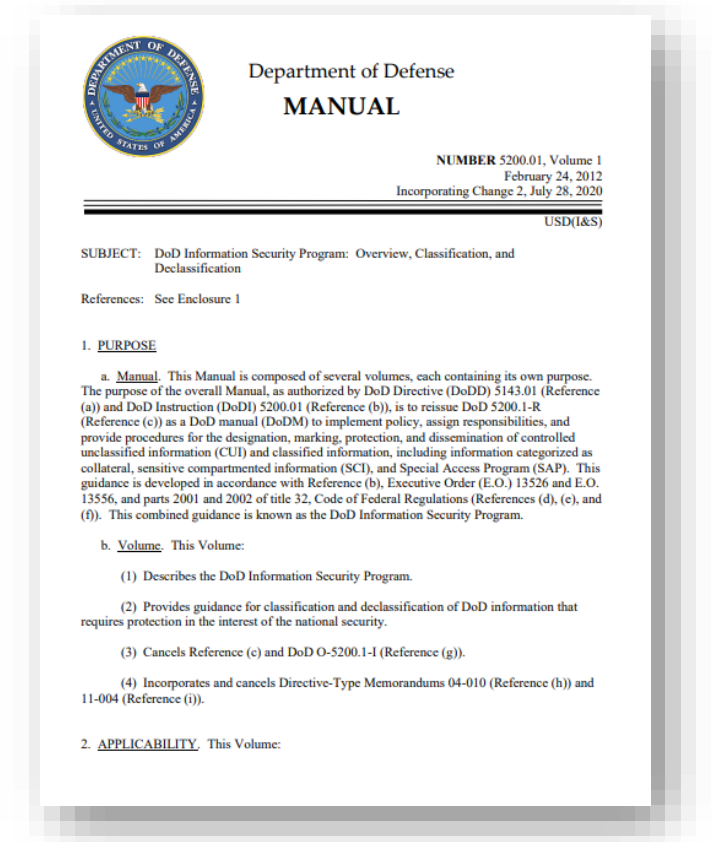


# DOD 5200.01 Vol 4 CUI CATEGORIES

For Official Use Only (FOUO)

Law Enforcement Sensitive (LES)

DoD Unclassified Controlled  
Nuclear Information (DoD UCNI)



## Limited Distribution Statements

**Distribution A** - Approved for public release,  
distribution is unlimited

**Distribution B** - Distribution authorized to U.S.  
Government Agencies only

**Distribution C** - Distribution authorized to U.S.  
Government agencies and their contractors

**Distribution D** - Distribution authorized to the DoD  
and U.S. DoD contractors only

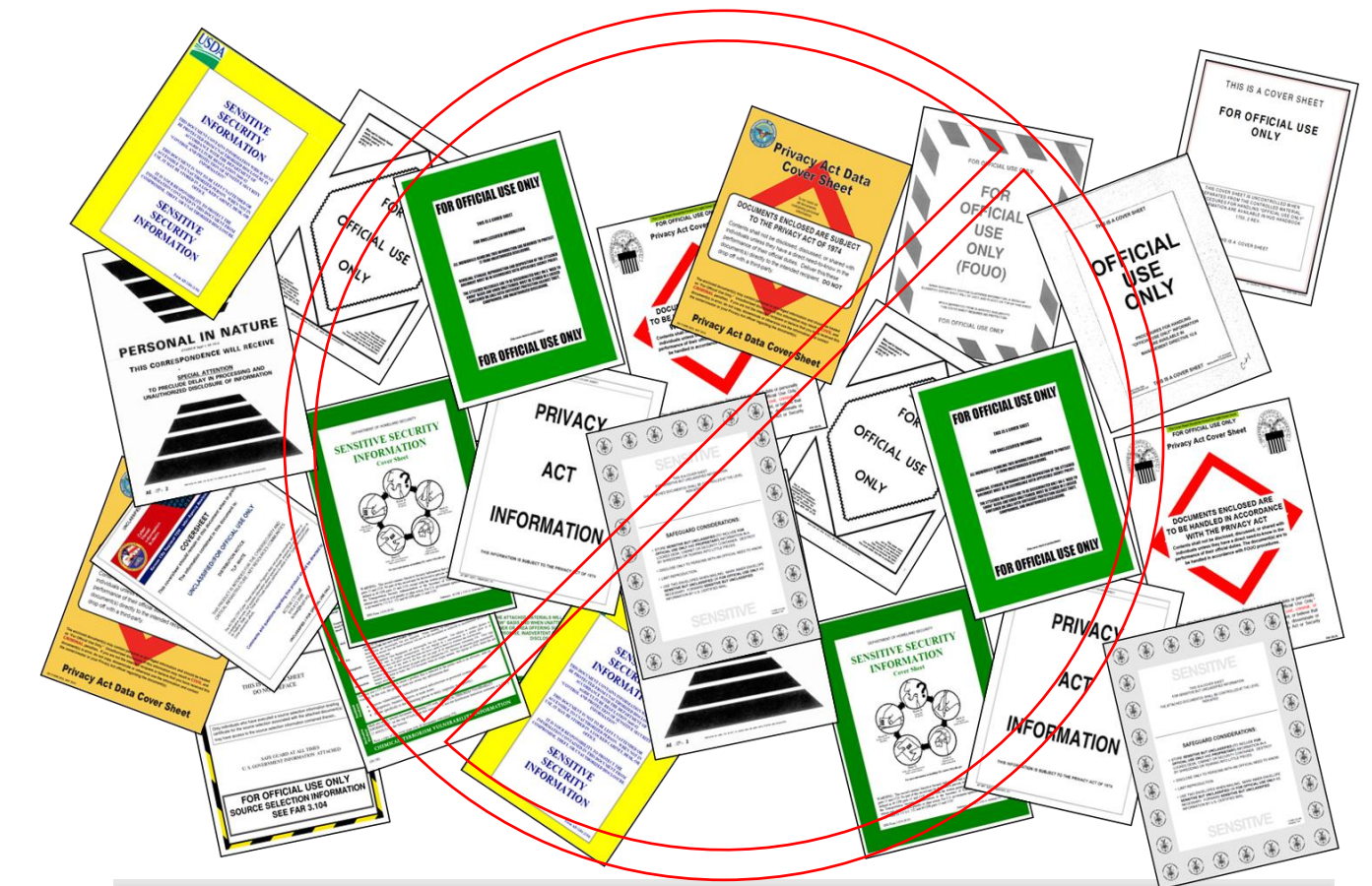
**Distribution E** - Distribution authorized to DoD  
Components only

**Distribution F** - Further distribution only as directed  
by (controlling DoD office) or higher DoD authority

**Distribution X** - Distribution authorized to U. S.  
Government agencies and private individuals or  
enterprises eligible to obtain export-controlled  
technical data in accordance with DoD Directive  
5230.25



The diagram illustrates the CUI Program framework. On the left, a blue arrow labeled "Laws, Regulations, Govt-wide Policies" points towards a central light blue circle. This circle is labeled "CUI Program" and contains a list of domains: Emergency Management, Agriculture, Patent, Immigration, Financial, Legal, Law Enforcement, Tax, Privacy, and Transportation. The circle is surrounded by a dark blue ring with the words "Shared", "Standardized", and "Transparent". On the right, a blue arrow labeled "CUI Program" points towards a stack of five colored boxes: Governance (red), Policy and Guidance (green), Technology (purple), Training (dark blue), and Accountability (orange).

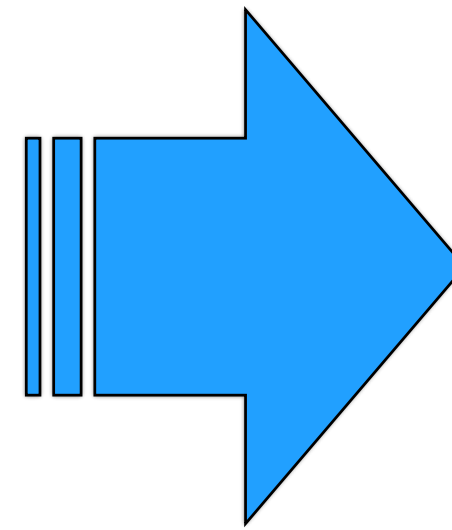



**classmgmt.com**



# CUI POLICY

DoD 5200.01 Vol 4 (2012)



 Department of Defense  
**MANUAL**

NUMBER 5200.01, Volume 4  
February 24, 2012

USD(I)

SUBJECT: DoD Information Security Program: Controlled Unclassified Information (CUI)

References: See Enclosure 1

1. **PURPOSE**

a. Manual. This Manual is composed of several volumes, each containing its own purpose. The purpose of the overall Manual, as authorized by DoD Directive (DoDD) 5143.01 (Reference (a)) and DoD Instruction (DoDI) 5200.01 (Reference (b)), is to reissue DoD 5200.1-R (Reference (c)) as a DoD Manual to implement policy, assign responsibilities, and provide procedures for the designation, marking, protection, and dissemination of CUI and classified information, including information categorized as collateral, sensitive compartmented information (SCI), and Special Access Program. This guidance is developed in accordance with Reference (b), Executive Order (E.O.) 13526 and E.O. 13556, and part 2001 of title 32, Code of Federal Regulations (References (d), (e), and (f)). This combined guidance is known as the DoD Information Security Program.

b. Volume. This Volume provides guidance for the identification and protection of CUI.

2. **APPLICABILITY**. This Volume:

a. Applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereinafter referred to collectively as the "DoD Components").

b. Does not alter existing authorities and responsibilities of the Director of National Intelligence (DNI) or of the heads of elements of the Intelligence Community pursuant to policies issued by the DNI.

c. Does NOT implement the new CUI program established by Reference (e). This Volume

DoDI 5200.48



DoD INSTRUCTION 5200.48

## CONTROLLED UNCLASSIFIED INFORMATION (CUI)

**Originating Component:** Office of the Under Secretary of Defense for Intelligence and Security

**Effective:** March 6, 2020

**Releasability:** Cleared for public release. Available on the Directives Division Website at <https://www.esd.whs.mil/DD/>.

**Cancels:** DoD Manual 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information," February 24, 2012, as amended

**Approved by:**

**Purpose:** In accordance with 2010 Deputy Secretary

• Establishes policy in accordance with (CFR); and Defense 252.204-7012.

• Establishes the other

- Cancels DOD 5200.01, Vol 4
- Establishes the CUI Registry
- Establishes DCSA security oversight authority of NISP contractors' CUI Programs when DOD Components establish CUI requirements in DOD classified contracts



# CUI CONTROLS AND CONSIDERATIONS



- What laws, regulations, or government-wide policies (LRGWP) subject the information to a limited dissemination control (LDC), if applicable?

Law or Rule?... Law = CUI Specified (SP) Rule = CUI Basic

- What Organizational Index Grouping does this information support?

The CUI Registry includes 125 subcategories of Specified and Basic CUI

Examples: **Critical Energy Infrastructure Information (SP-CEII)**

**DoD Critical Infrastructure Security Information (DCRIT)**

**Protected Critical Infrastructure Information (SP-PCII)**

**General Critical Infrastructure Information (CRIT)**

- What Limited Dissemination Controls apply to this information? (there are 10)

NOFORN

DL ONLY

Attorney-WP

FED ONLY

REL TO [USA, LIST]

Attorney-Client

FEDCON

DISPLAY ONLY

Deliberative

NOCON



# CUI CATEGORIES

NARA Final Rule: "Controlled Unclassified Information," 32 CFR Part 2002, 81 Fed. Reg. 63324 (Sep. 14, 2016). NARA's CUI "[Registry](#)" states the law, regulation and policy behind each CUI category and subcategory.

DoD now has a [CUI web page](#) with much useful info – but it does *not* remove the trouble many contractors have identifying *what* information in their possession is CUI.

*Who may have access to CUI?*

- Defense contractors
- Other Federal contractors
- State & Local governments
- State & Local contractors
- Tribal governments
- Colleges & Universities
- Interstate Organizations
- NGOs
- Foreign governments

<b>Critical Infrastructure (11 sub)</b>	<b>Defense (4)</b> <b>Controlled Technical Information</b> <b>DoD Critical Infrastructure Security</b> <b>Navy &amp; Controlled Nuclear</b>		<b>Export Control (2)</b>	Financial (12)
Immigration (7)	<b>Intelligence (8)</b> General Intel. Ops Security	International Agreement (1)	Law Enforcement (18)	Legal (12)
Natural and Cultural Resources (3)	<b>NATO (2)</b>	Nuclear (5)	Patent (3)	Privacy (9)
Procurement & Acquisition (3) e.g., SBR&T; SSI	Proprietary Business Info (6)	<b>"Provisional" (9) e.g., Info Sys Vuln Sens PII</b>	Statistical (4 sub)	Tax (4)
Transportation (2 sub)	<b>20 Categories, 125 Subcategories</b>			



[RESEARCH OUR RECORDS](#)[VETERANS' SERVICE RECORDS](#)[EDUCATOR RESOURCES](#)[VISIT US](#)[AMERICA'S FOUNDING DOCUMENTS](#)

# Controlled Unclassified Information (CUI)

[Home](#) > [Controlled Unclassified Information \(CUI\)](#)


## CUI Registry

The CUI Registry is the Government-wide online repository for Federal-level guidance regarding CUI policy and practice. However, agency personnel and contractors should first consult their agency's CUI implementing policies and program management for guidance.



Search the Registry:

Go

### Categories, Markings and Controls:

- [Category List](#)
- [CUI Markings](#)
- [Limited Dissemination Controls](#)
- [Decontrol](#)
- [Registry Change Log](#) 

### Policy and Guidance

- [Executive Order 13556](#)
- [32 CFR Part 2002](#)  (Implementing Directive)
- [CUI Marking Handbook](#) 
- [CUI Notices](#)

### CUI Glossary



# “THE” CUI REGISTRY



<https://www.archives.gov/cui>



National Archives and  
Records Administration\*

\*DODI 5200.48 designates  
NARA is the Executive  
Agent for the CUI Program



CUI Registry  
Categories  
CUI Markings  
Limited Dissemination  
Controls  
Decontrol  
Registry Change Log  
Policy and Guidance  
Glossary  
CUI Reports  
CUI Training  
CUI Resources

Organizational Index Grouping	CUI Categories
Defense	<ul style="list-style-type: none"><li>Controlled Technical Information</li><li>DoD Critical Infrastructure Security Information</li><li>Naval Nuclear Propulsion Information</li><li>Unclassified Controlled Nuclear Information - Defense</li></ul>
Export Control	<ul style="list-style-type: none"><li>Export Controlled</li><li>Export Controlled Research</li></ul>
Proprietary Business Information	<ul style="list-style-type: none"><li>Entity Registration Information</li><li>General Proprietary Business Information</li><li>Proprietary Manufacturer</li></ul>



Organizational Index Grouping	CUI Categories
Critical Infrastructure	<ul style="list-style-type: none"> <li>• Ammonium Nitrate</li> <li>• Chemical-terrorism Vulnerability Information</li> <li>• Critical Energy Infrastructure Information</li> <li>• Emergency Management</li> <li>• General Critical Infrastructure Information</li> <li>• Information Systems Vulnerability Information</li> <li>• Physical Security</li> <li>• Protected Critical Infrastructure Information</li> <li>• SAFETY Act Information</li> <li>• Toxic Substances</li> <li>• Water Assessments</li> </ul>
Defense	<ul style="list-style-type: none"> <li>• Controlled Technical Information</li> <li>• DoD Critical Infrastructure Security Information</li> <li>• Naval Nuclear Propulsion Information</li> <li>• Unclassified Controlled Nuclear Information - Defense</li> </ul>
Export Control	<ul style="list-style-type: none"> <li>• Export Controlled</li> <li>• Export Controlled Research</li> </ul>

CUI Category: Controlled Technical Information

Banner Marking: CUI//SP-CTI

Category Description:	Controlled Technical Information means technical information with military or space-related content that, if disclosed, could result in the unauthorized access, use, reproduction, modification, performance, display, release, dissemination, or destruction of information that is to be marked with one of the distribution statements B through F, in accordance with the "Distribution Statements of Technical Documents." The term does not include information that is already in the public domain. "Technical Information" means technical data or computer software that is developed, produced, or used in the design, development, testing, or manufacturing of a product, process, or system. Examples of technical information include research and engineering data, standards, process sheets, manuals, technical reports, technical orders, and related information, and computer software executable code and source code.
Category Marking:	CTI
Banner Format and Marking Notes:	Banner Format: CUI//Category Marking//Limited Dissemination Control

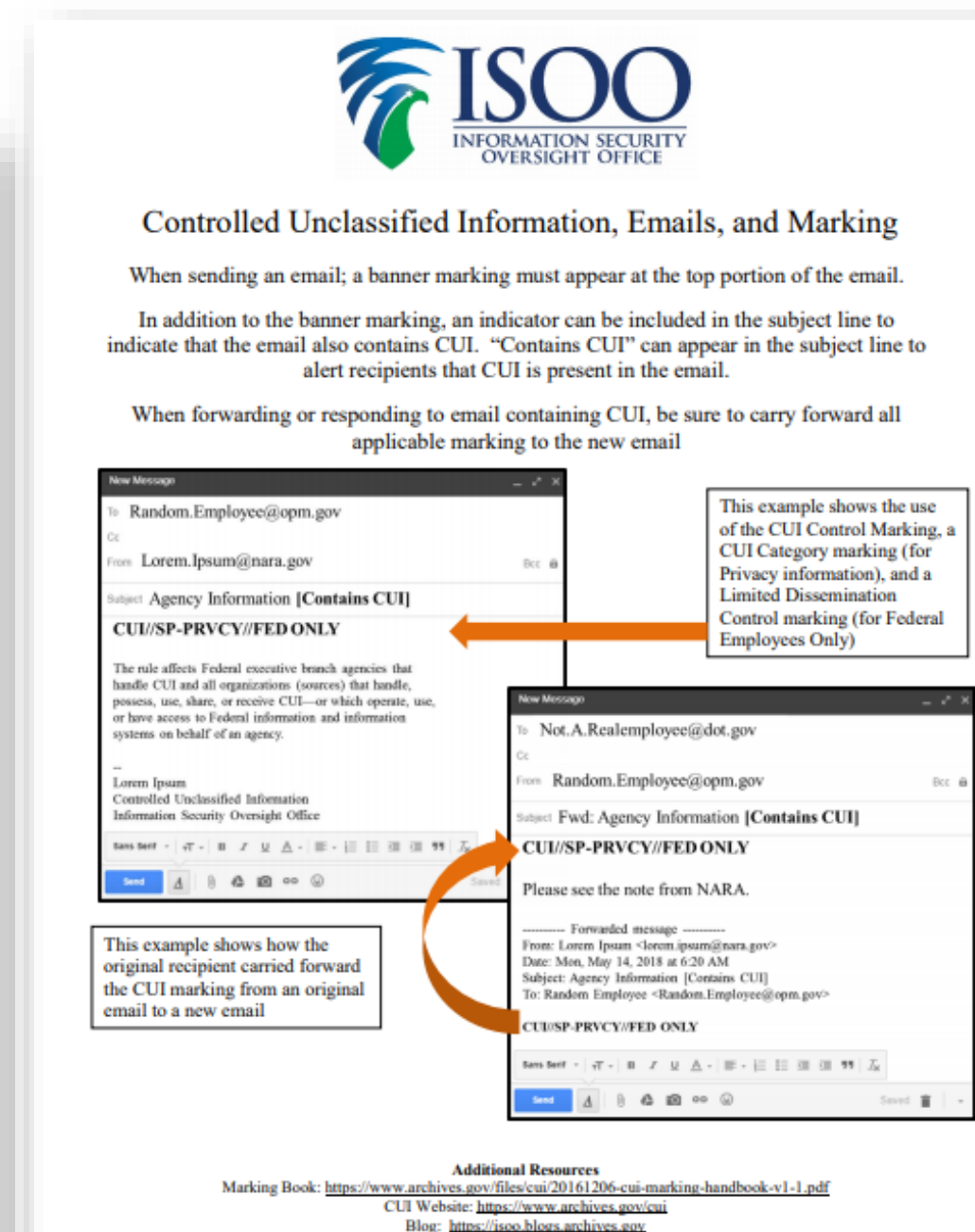
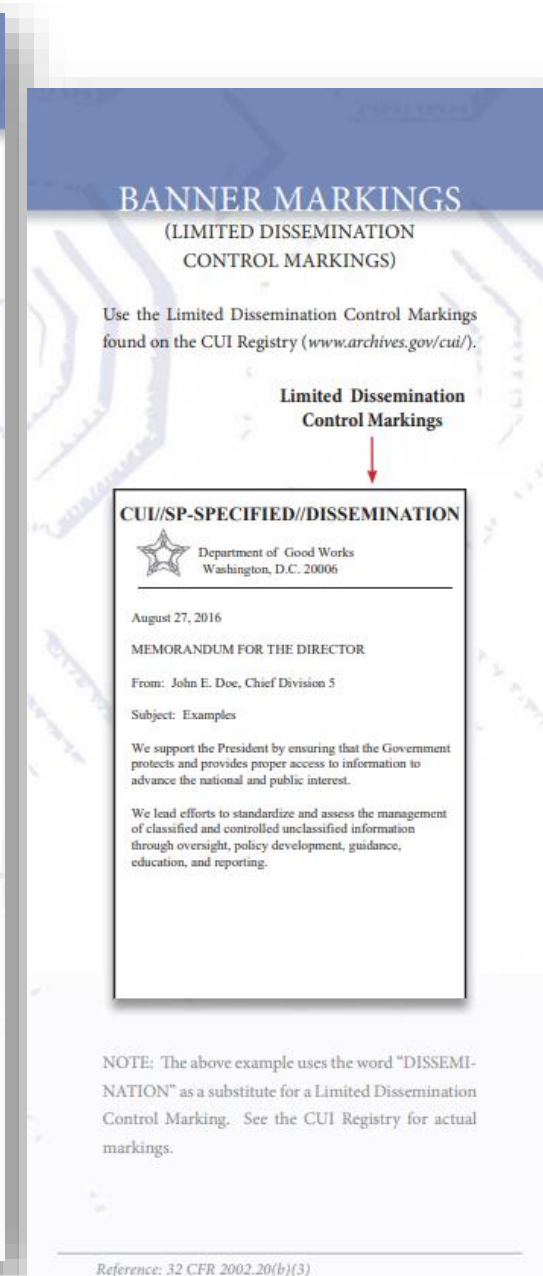
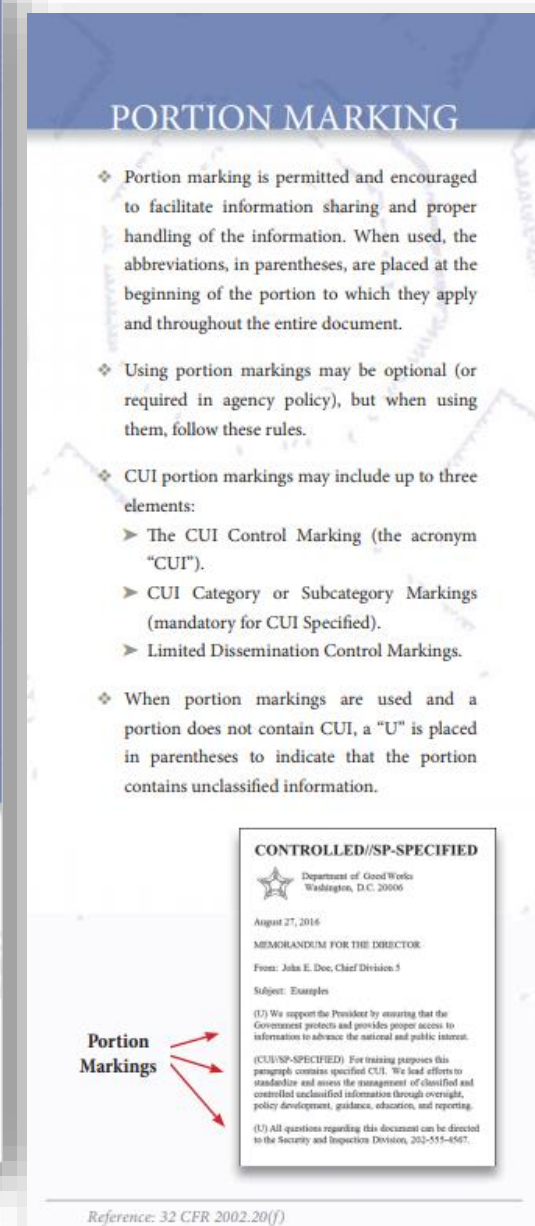
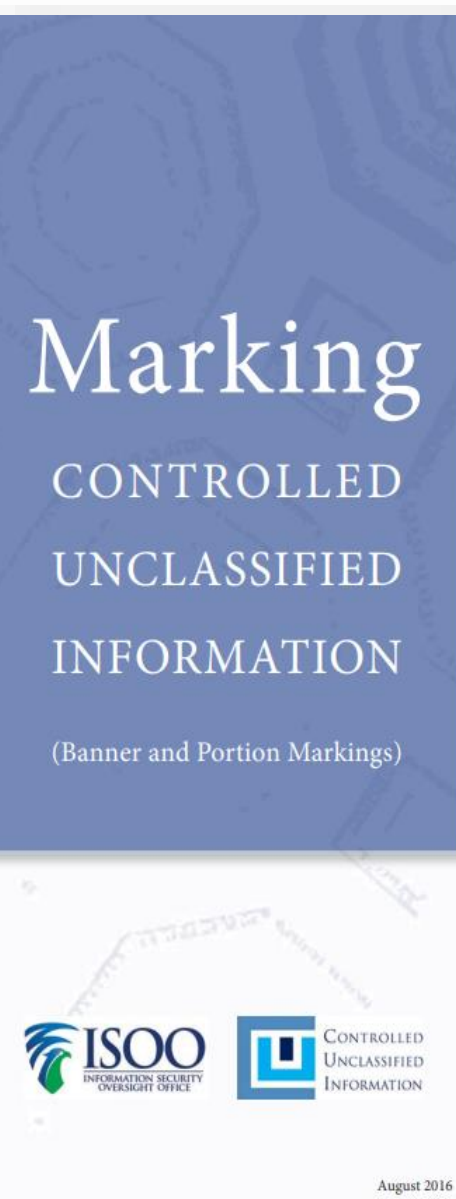
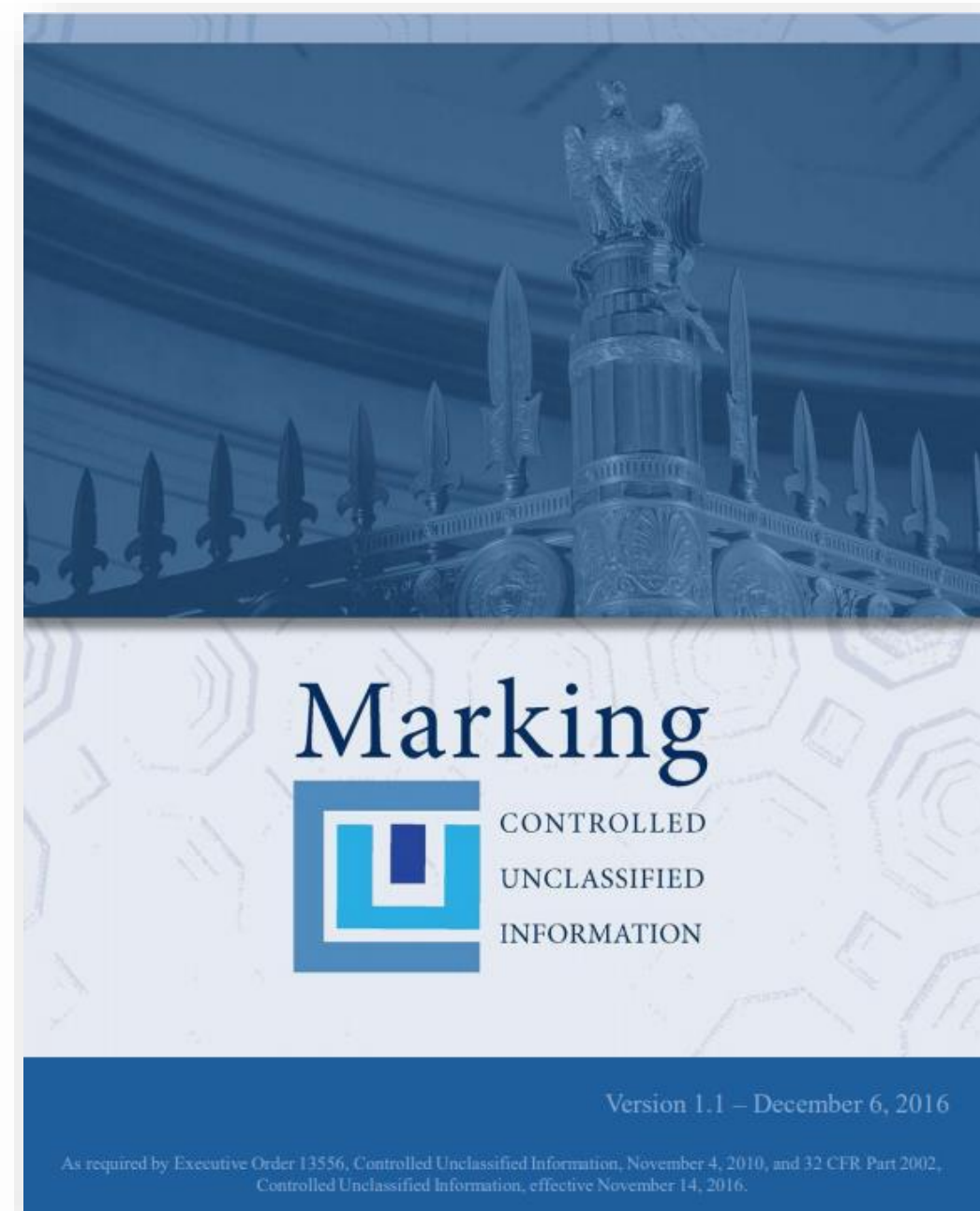


[RESEARCH OUR RECORDS](#)
[VETERANS' SERVICE RECORDS](#)
[EDUCATOR RESOURCES](#)
[VISIT US](#)
[AMERICA'S FOUNDING DOCUMENTS](#)

## Controlled Unclassified Information (CUI)

[Home](#) > [Controlled Unclassified Information \(CUI\)](#)

### Marking Handbook



### CUI Coversheet





# THE CUI REGISTRY(IES)

## DoD CUI PROGRAM

<https://www.dodcui.mil/>



## DoD CUI Registry

Organizational Index Grouping	CUI Categories	Category Abbreviations	Authorities
Defense	Controlled Technical Information	CTI	48 CFR 252.204-7012
	DoD Critical Infrastructure Security Information	DCRIT	10 USC 130e
	Naval Nuclear Propulsion Information	NNPI	42 USC 2013 50 USC 2511
	Unclassified Controlled Nuclear Information - Defense (UCNI)	DCNI	10 USC 128(a) 32 CFR 223
Export Control	Export Controlled	EXPT	50 USC 4614(c) 13 USC 301(g)



# DOD CUI GUIDANCE



## DoD CUI PROGRAM



[HOME](#) ▾ [ABOUT US](#) ▾ [CONTACT](#) ▾ [CMMC](#) ▾

[HOME](#) > [HOME](#) > [TRAINING](#)



CONTROLLED  
UNCLASSIFIED  
INFORMATION

[DoD CUI Awareness Training](#)



**CDSE**  
Center for Development  
of Security Education

[CDSE Home Page](#)  
[CDSE Information Security Page](#)  
[CDSE Current CUI Page](#)



ISOO provides these training videos on YouTube, so some users may be unable to access them from US Government IT systems because of organizational policy.

[The Controlled Unclassified Information Program](#)  
[Controlled Unclassified Information: Lawful Government Purpose](#)  
[Controlled Unclassified Information - Introduction to Marking](#)  
[Controlled Unclassified Information - Marking Commingled Information](#)  
[Controlled Unclassified Information - Controlled Environments](#)  
[Controlled Unclassified Information - Destruction of CUI](#)  
[Controlled Unclassified Information: Unauthorized Disclosure: Prevention and Reporting](#)  
[CUI and the FOIA FAQs](#)



<https://www.dodcui.mil>



# DOD MARKING GUIDE WWW.DODCUI.MIL

The appearance of external hyperlinks does not constitute endorsement by the United States Department of Defense (DoD) of the linked websites, or the information, products or services contained therein. The DoD does not exercise any editorial, security, or other control over the information you may find at these locations.

**CLEARED  
For Open Publication**

Nov 04, 2020

Department of Defense  
OFFICE OF PREPUBLICATION AND SECURITY REVIEW



## Controlled Unclassified Information Markings

October 23, 2020

<https://www.dodcui.mil>

*Markings are for training purposes only*

OUSD(I&S)/DDI(CL&S)  
Information Security

21-S-0209

1



classmgmt.com



# PARAGRAPH/PORTRION MARKINGS

If all the sub-paragraphs or sub-bullet points carry the same classification as the main paragraph or bullet point, portion marking is not required for the sub-paragraphs or sub-bullet points.

However, if any of the sub-paragraphs or sub-bullet points carry different classifications from the main paragraph or bullet point, portion marking is required for all the sub-paragraphs or sub-bullet points as demonstrated here.

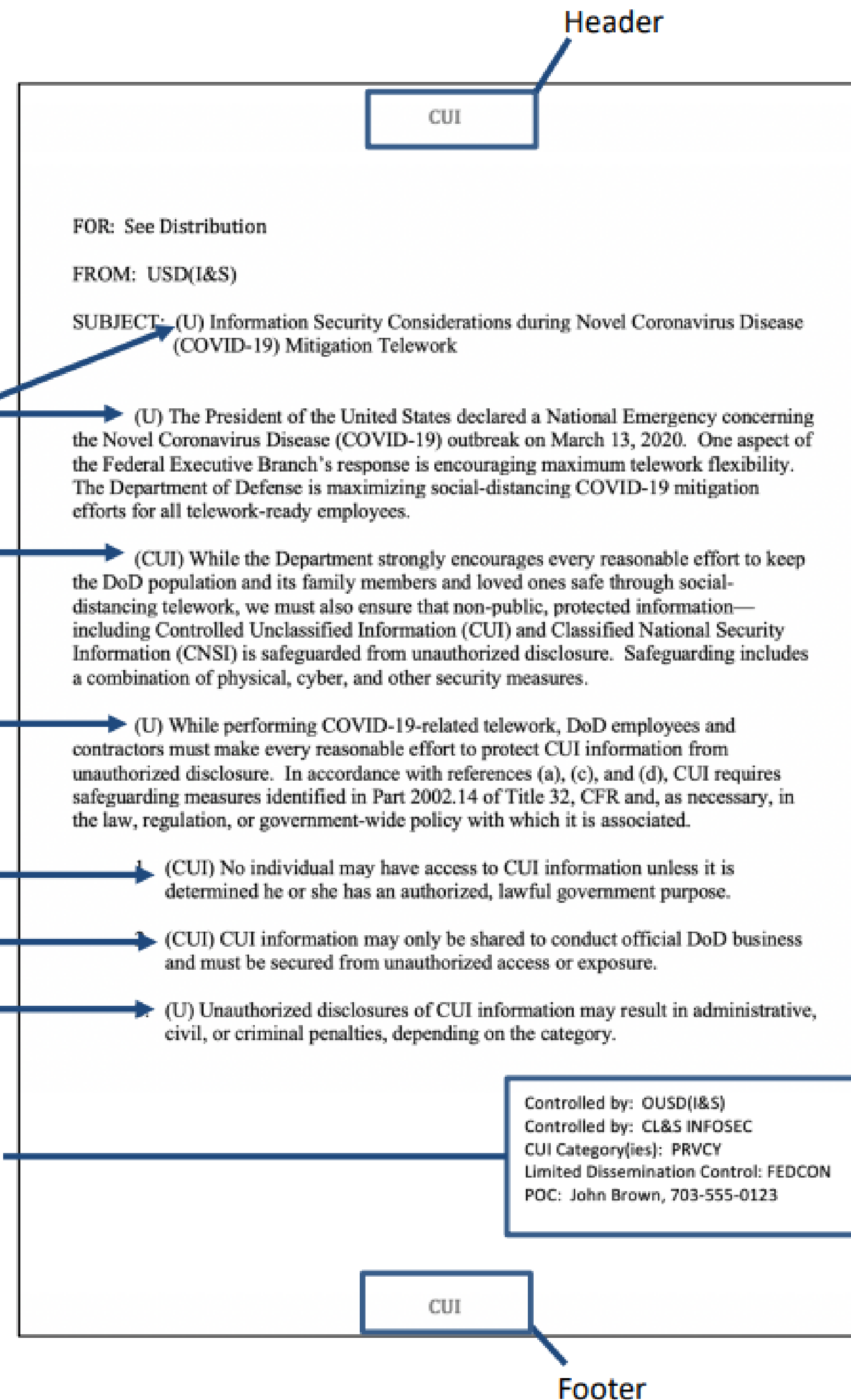
Portions include subjects, titles, paragraphs and sub-paragraphs, bullet points and sub-bullet points, headings, pictures, graphs, charts, maps, reference list, etc.

The CUI designation indicator block does not require a portion mark.

Example of markings on a CUI document with portion markings.

Portion marks

CUI  
Designation  
Indicator





## DOD MARKING GUIDELINES VARY FROM THE ISOO MARKINGS

CUI//NOFORN

### → (U) Marking Requirements for CUI

- → (U) Portion markings.
  - → (CUI//NF) Portion markings are optional. However, if portion markings are annotated, they must be applied to all portions, to include subjects, titles, headings, paragraphs, subparagraphs, bullet points, etc.
  - → (U) Portions containing CUI NOFORN information will be annotated "(CUI//NF)."
- → (U) Banner line.
  - → (CUI) At a minimum, CUI markings for unclassified documents will include the acronym "CUI" at the top and bottom of each page.
  - → (CUI//NF) If there is NOFORN information in the document, this will be reflected in the banner line as shown in this example.

Controlled by: OUSD(I&S)  
Controlled by: CL&S INFOSEC  
CUI Category(ies): NNPI  
Limited Dissemination Controls: NOFORN  
POC: John Brown, 703-555-0123

CUI//NOFORN





# DCSA, CUI COMPLIANCE OVERSIGHT



## John B. Massey

Deputy Assistant Director of Enterprise Security Operations  
Defense Counterintelligence & Security Agency,  
Critical Technology Protection





# DCSA, CUI COMPLIANCE OVERSIGHT

UNCLASSIFIED

## DCSA's CUI Responsibilities



**DCSA assigned eight (8) responsibilities in support of Department CUI program management; focused on CUI associated with classified contracts**

- a. Administers the DOD CUI Program for contractually established CUI requirements for contractors in classified contracts
- b. Assesses contractor compliance with contractually established CUI system requirements in DOD classified contracts associated with the NISP
- c. Establishes a process to notify the DOD CIO, USD(R&E), and USD(A&S) of threats related to CUI
- d. Provides security education, training, and awareness on the required topics identified in Section 2002.30 of 32CFR
- e. Provides security assistance and guidance to the DOD Components on the protection of CUI
- f. Serves as the DOD-lead to report UD's of CUI
- g. Coordinates with the DOD CIO to implement uniform security requirements for NISP contractors
- h. Consolidates DOD Component input on the oversight of CUI protection requirements in DOD classified contracts for NISP contractors

DoDI 5200.48



# DCSA, CUI COMPLIANCE OVERSIGHT

UNCLASSIFIED



## DCSA's CUI Planning

### GOALS

- ☐ Operationalize DCSA CUI responsibilities as outlined in DODI 5200.48.
- ☐ Execute DOD CUI Program Administration and associated responsibilities
- ☐ Expanded perimeter of security beyond cleared industry

### END-STATE

- ☐ Information sharing and collaboration with USG partners
- ☐ Integration into industry oversight processes
- ☐ Avoidance of redundant USG CUI-oversight efforts
- ☐ Near Future: Holistic view of security at NISP facilities
- ☐ Long-Term: Oversight of CUI for the DIB (17 May 2018 USD(I) Memo)

DOD CUI Program Administration  
(responsibilities: a, e, g, h)

UD & Threat Notification Processes  
(responsibilities: c, f)

CUI Security Education & Training  
(responsibilities: d)

Coordination Lead (DOD CIO/Components)  
(responsibilities g, h)

Assess Contractor Compliance  
(responsibilities: b)



# DCSA, CUI COMPLIANCE OVERSIGHT



- Phase 1 officially commenced 1-Oct-21, expected to address eight CUI responsibilities throughout the course of FY2022

**Executive Order  
13556**

November 9, 2010

**32 CFR Part 2002**

September 14, 2016

**DOD Instruction  
5200.48**

March 6, 2020

## DCSA CONTROLLED UNCLASSIFIED INFORMATION (CUI)

### CUI IMPLEMENTATION PHASE 1

On October 1, DCSA will begin operationalizing its eight CUI responsibilities using a phased approach and will be in an initial operating capability throughout fiscal year 2022. Phase 1 starts with the standup of a centralized program administration office (hereafter referred to as the DCSA CUI Program Office), which will begin executing several administrative functions, including developing processes and procedures, engaging Government and Industry stakeholders, and producing tools, training, and resources to support Industry's development, management, and sustainment of CUI programs within their contractor facilities.

- Key initiatives: education and training tools, resources; develop unauthorized disclosure (UD) and threat notification processes

Ref: [https://www.dcsa.mil/Portals/91/Documents/CTP/tools/VOI\\_September2021.pdf](https://www.dcsa.mil/Portals/91/Documents/CTP/tools/VOI_September2021.pdf)



# DCSA, CUI COMPLIANCE OVERSIGHT



- CUI Resources

## Quick Start Guide



## Marking Job Aid



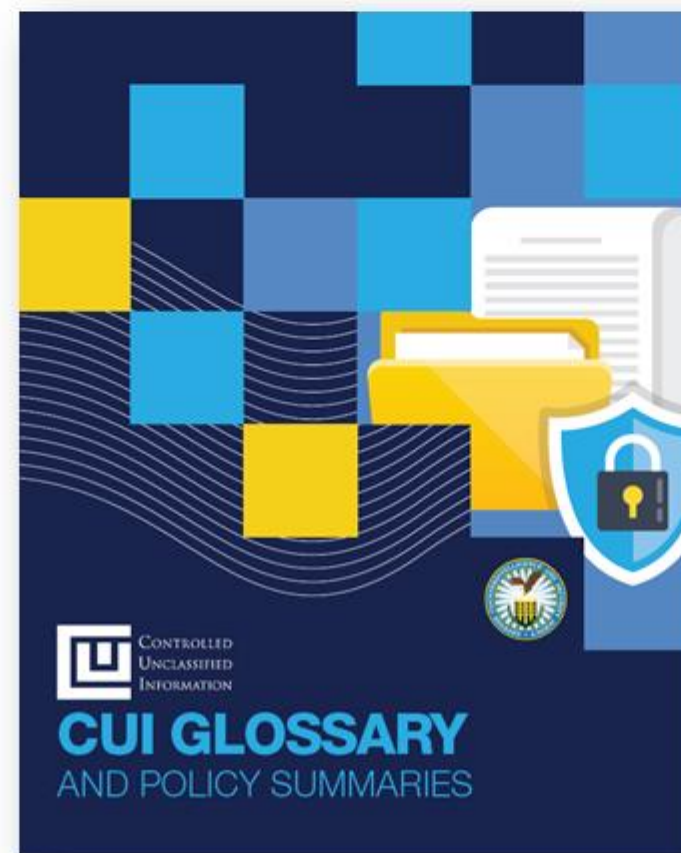
## FAQs



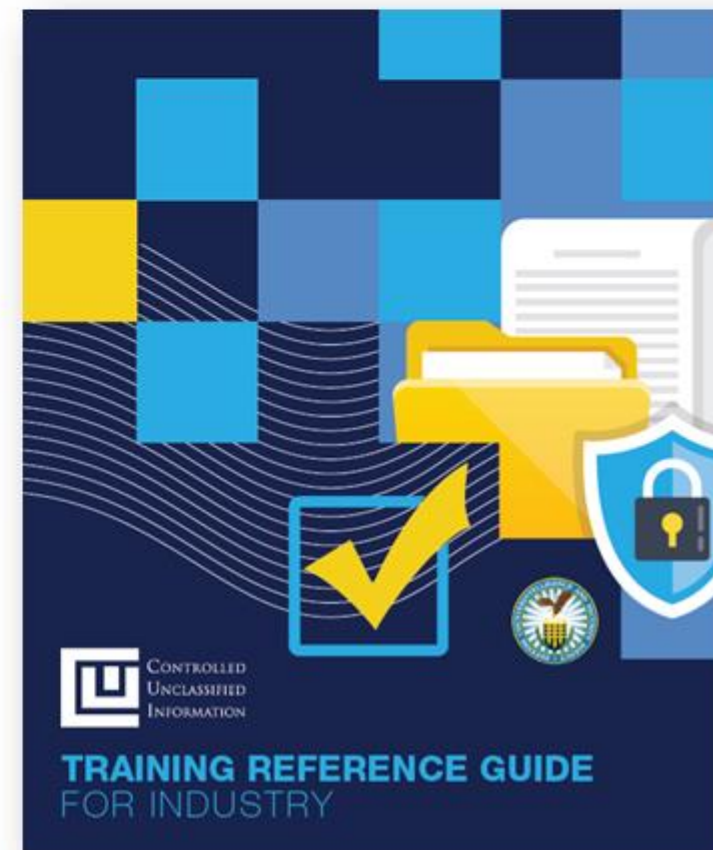


# DCSA, CUI RESOURCES

## CUI Glossary & Policy Summary



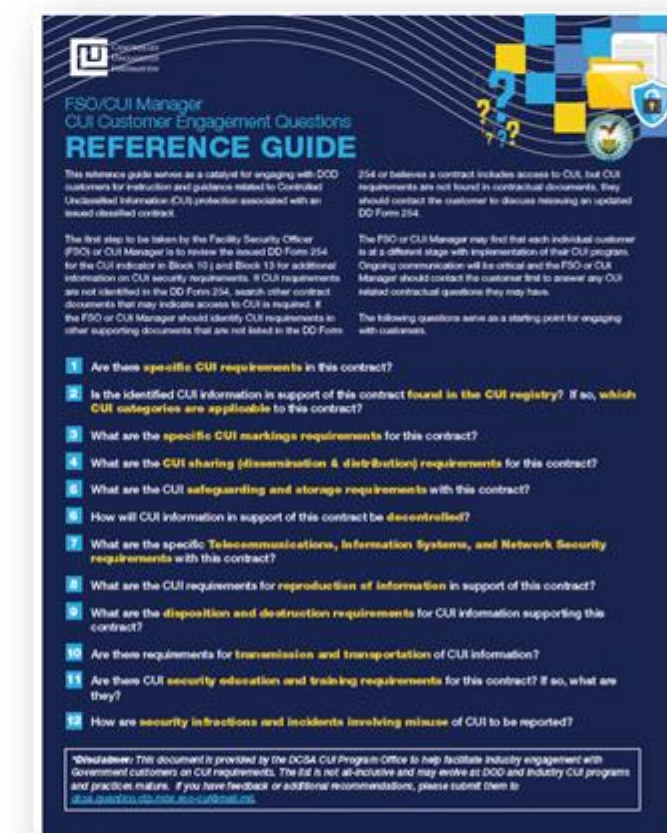
## Training Reference Guide



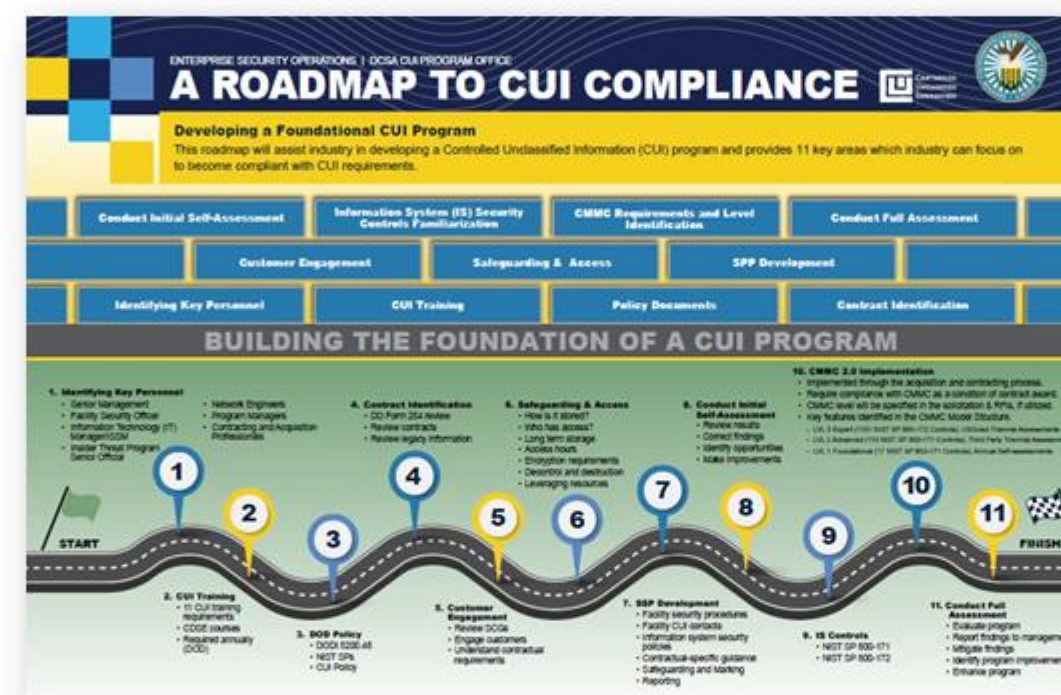
## Baseline Requirements



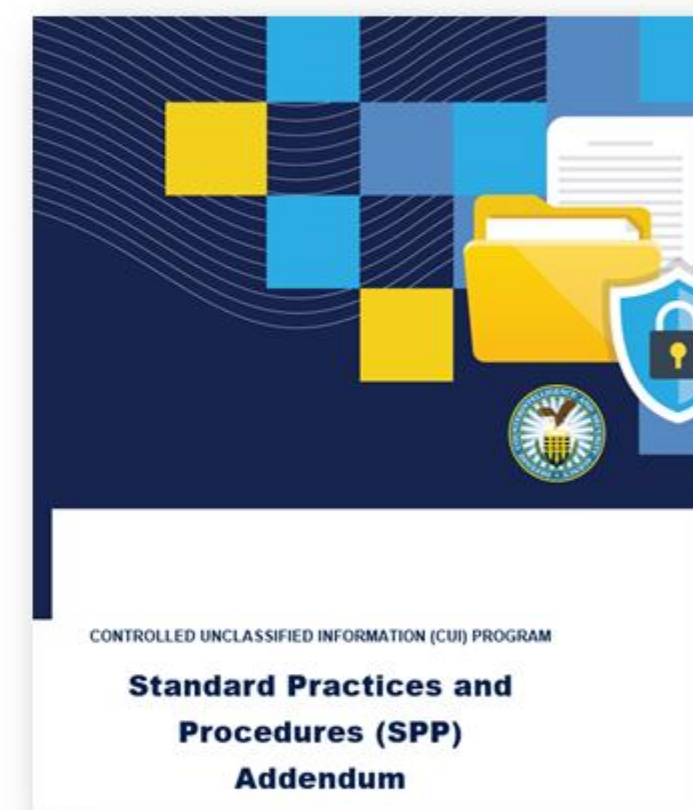
## FSO/CUI Manager Customer Questions



## CUI Roadmap



## SPP Addendum



## CUI Selfie Tool

Below are some considerations for establishing a CUI program. Ensure the CUI Manager implements the following as it relates to CUI Program Management:

Review Item	Yes	No	N/A	Notes
<b>Has the Agency or Component or Cleared Contractor:</b>				
Appointed a CUI Manager or other personnel to manage and implement the CUI Program which implements the provisions of DODI 5200.48? (32 CFR 2002.4.e, DODI 5200.48 (5.3))				
Developed and implemented security guidance necessary for program implementation. (32 CFR 2002.4.e, DODI 5200.48 (5.3))				
Allocated sufficient resources and personnel committed to implement the CUI Program? (32 CFR 2002.4.e, DODI 5200.48 (5.3))				
Conduct CUI oversight review of their contracts that contain Government Contracting Office CUI oversight requirements. (32 CFR 2002.16.5, DODI 5200.48 (5.3))				
Established, implemented, and maintained an effective security education program as required by DODI 5200.48, to include initial mandatory and continuing refresher training for assigned members. (32 CFR 2002.30, DODI 5200.48 (5.3))				
<b>Industry Only:</b> Does the contractor have DOD contracts with CUI requirements? (32 CFR 2002.16.5, DODI 5200.48 (5.3))				
<b>Industry Only:</b> Does the contractor have non-DOD contracts with CUI requirements? (32 CFR 2002.16.5, DODI 5200.48 (5.3))				
Has the CUI Manager completed mandatory CUI training? (32 CFR 2002.30, DODI 5200.48 (5.3))				
Have personnel working with CUI completed mandatory CUI training? (32 CFR 2002.30.b, DODI 5200.48 (5.3))				
Is the CUI manager documenting CUI oversight training? If so, how is it tracked? (32 CFR 2002.30, DODI 5200.48 (5.3))				

## Resource One-Pager



classmgmt.com

Approved for release January 27, 2022



# DCSA, CUI RESOURCES



## John B. Massey

Deputy Assistant Director of Enterprise Security Operations  
Defense Counterintelligence & Security Agency,  
Critical Technology Protection

NCMSLive

VIRTUAL TRAINING SERIES

Reference: NCMSLive 09-Feb-2022  
<https://classmgmt.com/ncmslive.php>

### • 09 FEB 2022 -- "Ask the FSO: CUI Spectacular with DCSA" (General Security NCMSLive Series)

- Presentation Slides
  - Presentation: Ask the FSO: CUI Spectacular with DCSA
- Session Recording
- Session Q and A



classmgmt.com

DCSA CUI Program Office

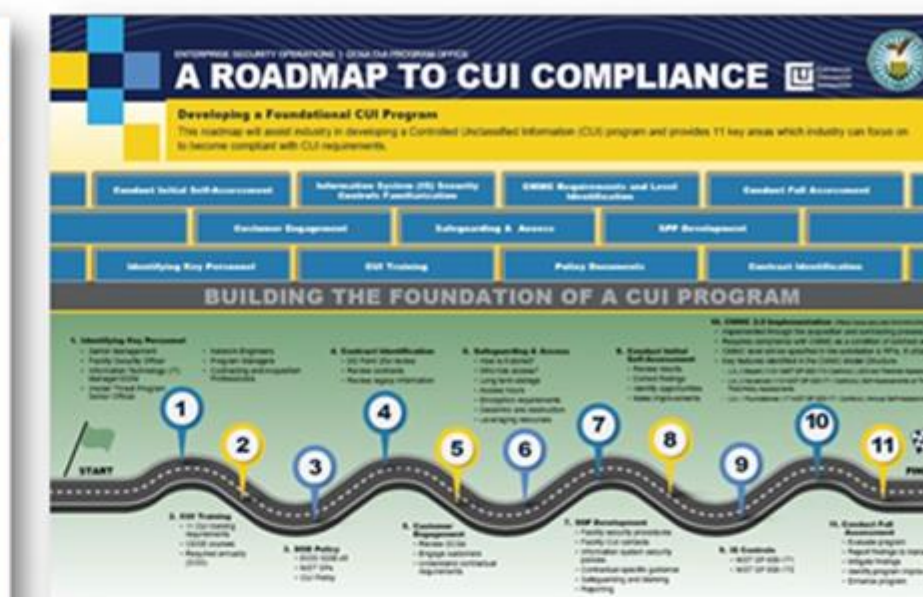
## New Release: CUI Products

The DCSA CUI Program Office has announced the release of *several* new CUI products and resources to support both DoD and Industry in implementation of CUI programs.

You can find these resources in the NCMS Hub and on the DCSA CUI website: <https://www.dcsa.mil/mc/ctp/cui/>.

DCSA and NCMS encourage you to share these tools within your organizations and professional networks.

**BREAKING**  
**NEWS**



That's a template!



# CUI TRAINING & AWARENESS

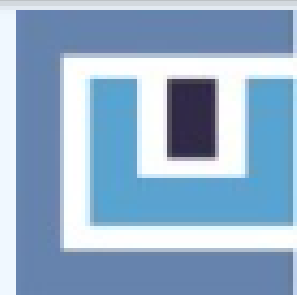
CDSE

An official website of the Center for Development of Security Excellence, Defense Counterintelligence and Security Agency

LEARN. PERFORM. PROTECT.

## SECURITY AWARENESS HUB

*Select eLearning awareness courses for DoD and Industry*



Access the Official DoD CUI Program Website

### DoD Mandatory Controlled Unclassified Information (CUI) Training

This course is mandatory training for all of DoD and Industry personnel with access to controlled unclassified information (CUI). The course provides information on the eleven training requirements for accessing, marking, safeguarding, decontrolling and destroying CUI along with the procedures for identifying and reporting security incidents.

Launch Course

Ref: <https://www.dcsa.mil/mc/ctp/cui/>



# CUI TRAINING & AWARENESS

UNCLASSIFIED

## WHY CUI TRAINING?

CUI training will be conducted **ANNUALLY** and, at a minimum, must include the following items (per [CUI Notice 2016-01](#) and [DoDI 5200.48](#)):

1. Convey individual responsibilities related to protecting CUI;
2. Identify the categories or subcategories routinely handled by agency personnel and any special handling requirements (i.e., for CUI Specified);
3. Describe the CUI Registry, its purpose, structure, and location (i.e., <http://www.archives.gov/cui/>);
4. Describe the differences between CUI Basic and CUI Specified;
5. Identify the offices or organizations with oversight responsibility for the CUI Program;
6. Address CUI marking requirements, as described by agency policy;
7. Address the required physical safeguards and methods for protecting CUI, as described by agency policy;
8. Address the destruction requirements and methods, as described by agency policy;
9. Address the incident reporting procedures, as described by agency policy;
10. Address the methods and practices for properly sharing or disseminating CUI within the agency and with external entities inside and outside the Executive branch; and
11. Address the methods and practices for properly decontrolling CUI, as described by agency policy.



Source:  
DCSA CUI  
Training Template  
Slide 5

<https://www.dcsa.mil/mc/ctp/cui/>



**NOTE:** Industry organizations may develop their own CUI training.

This presentation captures all 11 categories, but Industry may instead use this training to meet the requirement:  
DoD CDSE CUI course  
<https://securityhub.usalearning.gov/>.

UNCLASSIFIED



# CUI TRAINING & AWARENESS

- CUI training, at a minimum (per CUI Notice 2016-01), must include 11 required elements:
  - Convey individual responsibilities related to protecting CUI
  - Identify the categories (or subcategories) routinely handled by agency personnel and any special handling requirements (i.e., LDCs for CUI Specified)
  - Describe the CUI Registry, its purpose, structure, and location (i.e. <http://www.archives.gov/cui/>)
  - Describe the differences between CUI Basic and CUI Specified
  - Identify the offices or organizations with oversight responsibility for the CUI Program
  - Address CUI marking requirements, as described by agency policy
  - Address the required physical safeguards and methods for protecting CUI, per agency policy
  - Address the destruction requirements and methods, per agency policy
  - Address the incident reporting procedures, per agency policy
  - Address the methods and practices for properly sharing or disseminating CUI within the agency and with external entities inside and outside the Executive branch; and
  - Address the methods and practices for properly decontrolling CUI, as described by agency policy.

[https://www.dcsa.mil/Portals/91/Documents/CTP/tools/VOI\\_June\\_2021.pdf](https://www.dcsa.mil/Portals/91/Documents/CTP/tools/VOI_June_2021.pdf)



# CUI TRAINING & AWARENESS



## What Can Industry Do Now?

- Review existing contracts and engage with Government customers to determine which, if any, CUI requirements are applicable to current contracts.
- Review CUI resources and training available on the CDSE website to include the CUI Toolkit and “DOD Mandatory Controlled Unclassified Information (CUI) Training For Contractors (IF141.06.FY21.CTR).”
- Review the CUI Toolkit, which includes training, policy documents, resources, and an FAQ video, which CDSE has made available at: <https://www.cdse.edu/toolkits/cui/current.html>.
- Review the DOD CUI Registry at <https://www.dodcui.mil> to become familiar with CUI organizational index groupings and CUI categories.



# CUI Implementation Timeline

CONTROLLED  
UNCLASSIFIED  
INFORMATION



Agencies must initiate an awareness campaign that informs their entire workforce of the coming transition to the standards of the CUI Program.

**AWARENESS  
CAMPAIGN**

June 30,  
2020



Parent agencies must issue policies that implement the CUI Program.

**POLICY**

December  
31, 2020



Agencies (including any sub-agencies or components) must deploy CUI training to all affected employees.

**TRAINING**

December  
31, 2021



Parent agencies must issue agencies (including any sub-agencies or components) must implement or verify that all physical safeguarding requirements, as described in 32 CFR 2002 and in agency policies, are in place.

**PHYSICAL  
SAFEGUARDING**

December  
31, 2021



Agencies (including any sub-agencies or components) must modify all systems to the standard identified in the 32 CFR 2002.

**INFORMATION  
SYSTEMS**

December  
31, 2021



Senior Agency Officials must submit an annual report on the CUI program to ISOO no later than November 1 that covers the prior fiscal year Program.

**REPORTING**

Every  
Fiscal Year



# STORAGE OF CUI MATERIAL

Storage containers should be marked to indicate that it contains CUI.

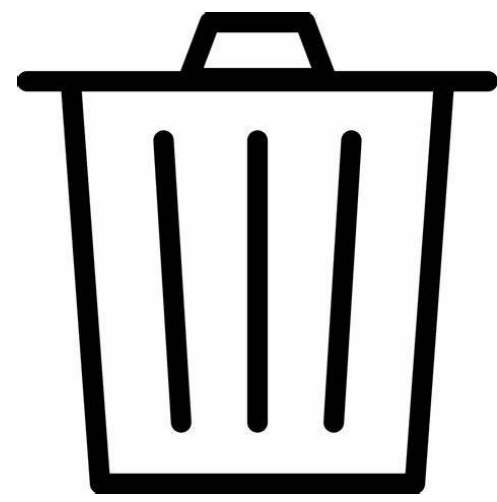


During working hours, steps will be taken to minimize the risk of access by unauthorized personnel, such as not reading, discussing, or leaving CUI information unattended where unauthorized personnel are present.

After working hours, if building security is not provided, the information will be stored in locked desks, file cabinets, bookcases, locked rooms, or similarly secured areas.

The concept of a controlled environment means there is sufficient internal security measures in place to prevent or detect unauthorized access to CUI.





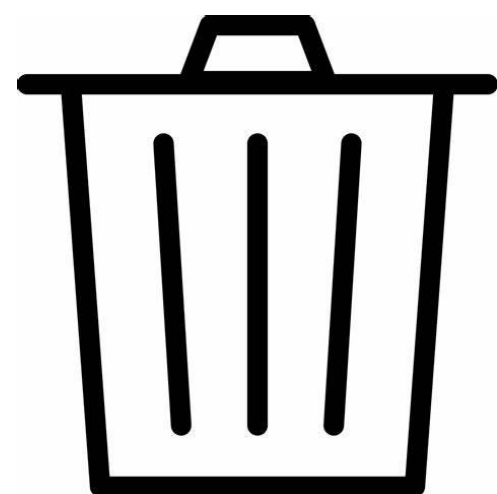
## 5200.01 DESTRUCTION GUIDANCE

FOUO documents may be destroyed by any of the means approved for the destruction of classified information or by any other means that would make it difficult to recognize or reconstruct the information.



**FOUO Destruction**





# 5200.48 DESTRUCTION GUIDANCE

Record and non-record CUI documents may be destroyed by means approved for destroying classified information or by any other means making it unreadable, indecipherable, and unrecoverable the original information such as those identified in NIST SP 800-88 and in accordance with Section 2002.14 of Title 32, CFR.



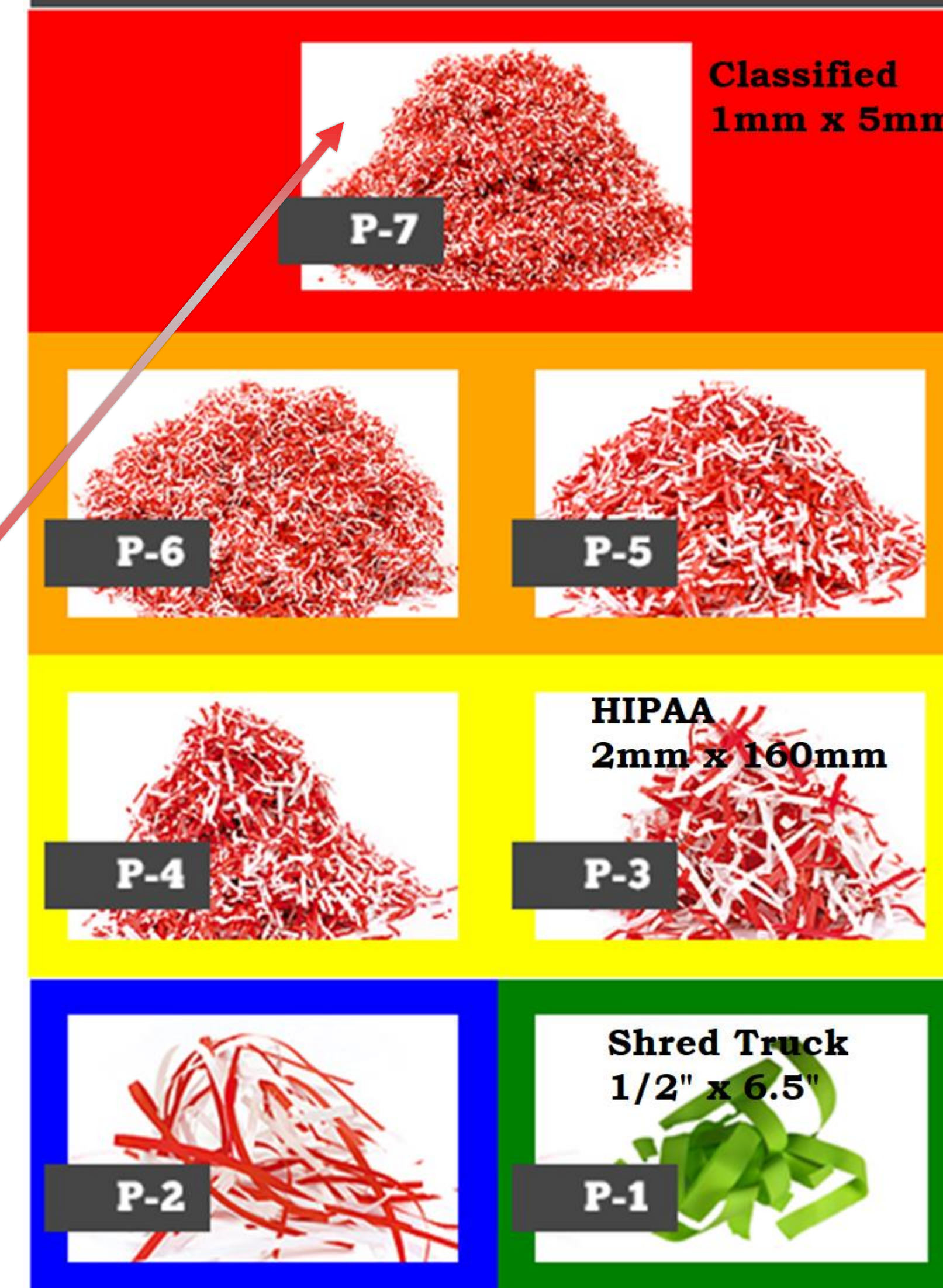
Table A-1: Hard Copy Storage Sanitization

## Hard Copy Storage

### Paper and microforms

Clear:	N/A, see Destroy.
Purge:	N/A, see Destroy
Destroy:	<p>Destroy paper using cross cut shredders which produce particles that are 1 mm x 5 mm (0.04 in. x 0.2 in.) in size (or smaller), or pulverize/disintegrate paper materials using disintegrator devices equipped with a 3/32 in. (2.4 mm) security screen.</p> <p>Destroy microforms (microfilm, microfiche, or other reduced image photo negatives) by burning.</p>
Notes:	When material is burned, residue must be reduced to white ash.

## Shred Level Security Pyramid





# PER DOD 5200.48... ISOO CUI NOTICE 2019-03

## Single-step paper destruction standard:

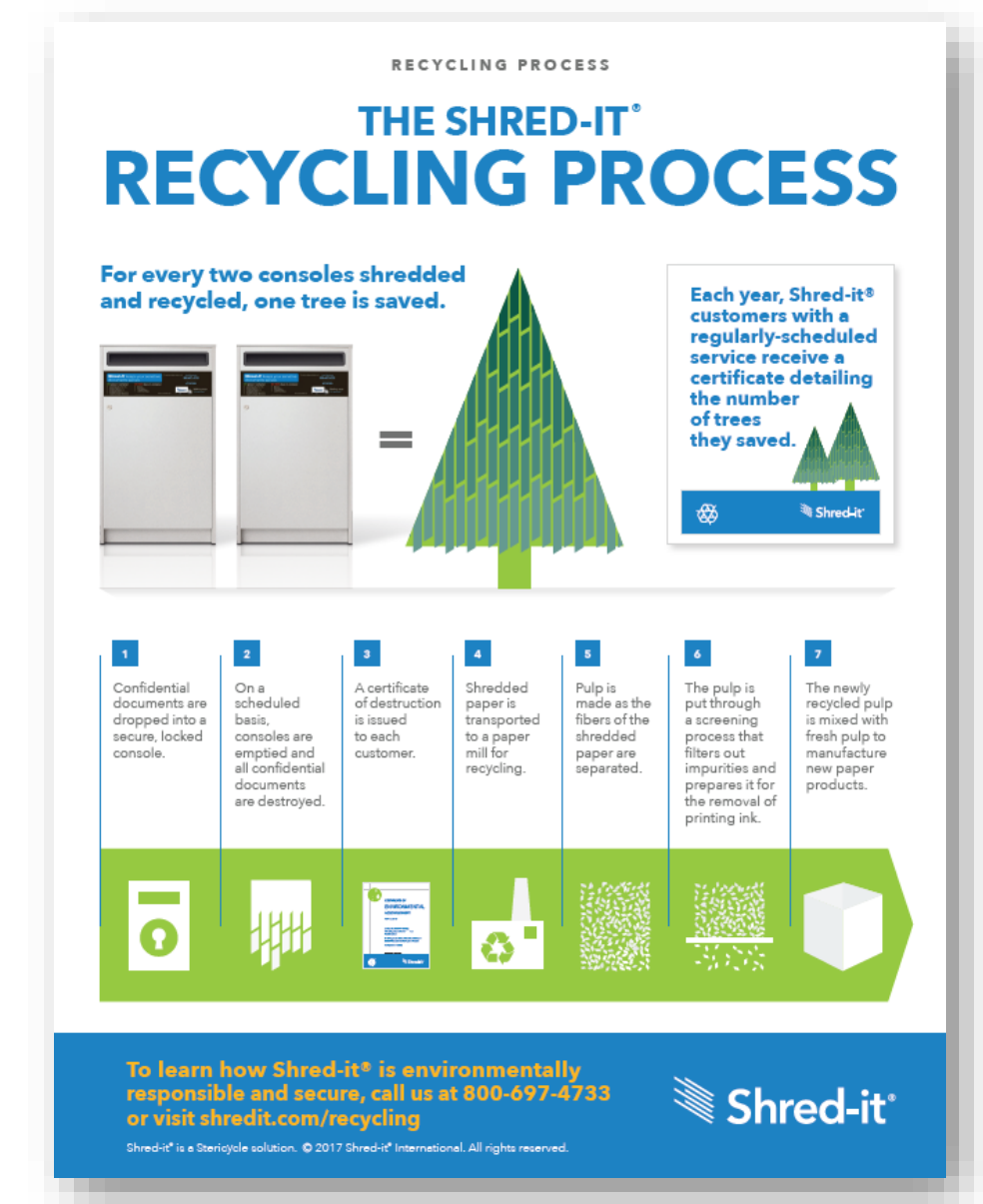
For the single-step paper destruction method agencies must:

- a. Use cross-cut shredders that produce 1mm x 5mm (0.04"x 0.2") particles (or smaller); or
- b. Pulverize/disintegrate paper using disintegrator devices equipped with a 3/32" (2.4 mm) security screen. (source: NIST SP 800-88, rev 1, Table A-1: Hard Copy Storage Sanitization)

## Multi-step paper destruction standard:

**A multi-step destruction process in which an agency shreds CUI to a degree that doesn't meet the Table A-1 standards, and then recycles or destroys it (or has a contractor or shared service provider shred and/or recycle/destroy), is a permitted alternative once your organization has verified and found this method satisfactory.** Agencies that use a multi-step destruction process must follow the guidelines in this Notice and the attached document, and the process must result in CUI that is unreadable, indecipherable, and irrecoverable.

**Recycling hard copy (paper) satisfies CUI destruction requirements** as part of a multi-step destruction process **only if the process recycles the CUI into new paper**. Recycling processes that convert paper into **other products** do not always render the CUI unreadable, indecipherable, and irrecoverable, and thus **may not meet the CUI Program's standards**.





# WHAT ACTIONS SHOULD YOU TAKE?

There are six things you need to do starting 30 Nov 2020:

- Conduct a self-assessment in accordance with the NIST SP 800-171 "DoD Assessment Methodology" (110 controls).
- Register on the Supplier Performance Risk System (SPRS) <https://www.sprs.csd.disa.mil/> or email results to [webptsmh@navy.mil](mailto:webptsmh@navy.mil)
- Produce and maintain a System Security Plan (SSP) and Plan of Action and Milestones (POA&M) for each system.
- Produce and maintain policy, process, and system documentation / evidence of compliance.
- Enter the self-assessment score into SPRS prior to award, option exercise, or extension of a contract, task order, or delivery order. Note that this will affect more than new contract awards. Contract extensions and new task orders will also trip this requirement.
- Ensure all sub-contractors also perform the above.





# Guiding the DoD in Responsible Acquisition Decisions

<https://www.sprs.csd.disa.mil/>



- Login/Register  
(via PEE)
- NIST SP 800-171  
Vendor Help posting  
Basic Assessments
- F  
A  
Q
- NIST SP 800-171  
Information
- Vendor Threat  
Mitigation
- Enhanced Vendor  
Profile
- SPRS Reports ▾

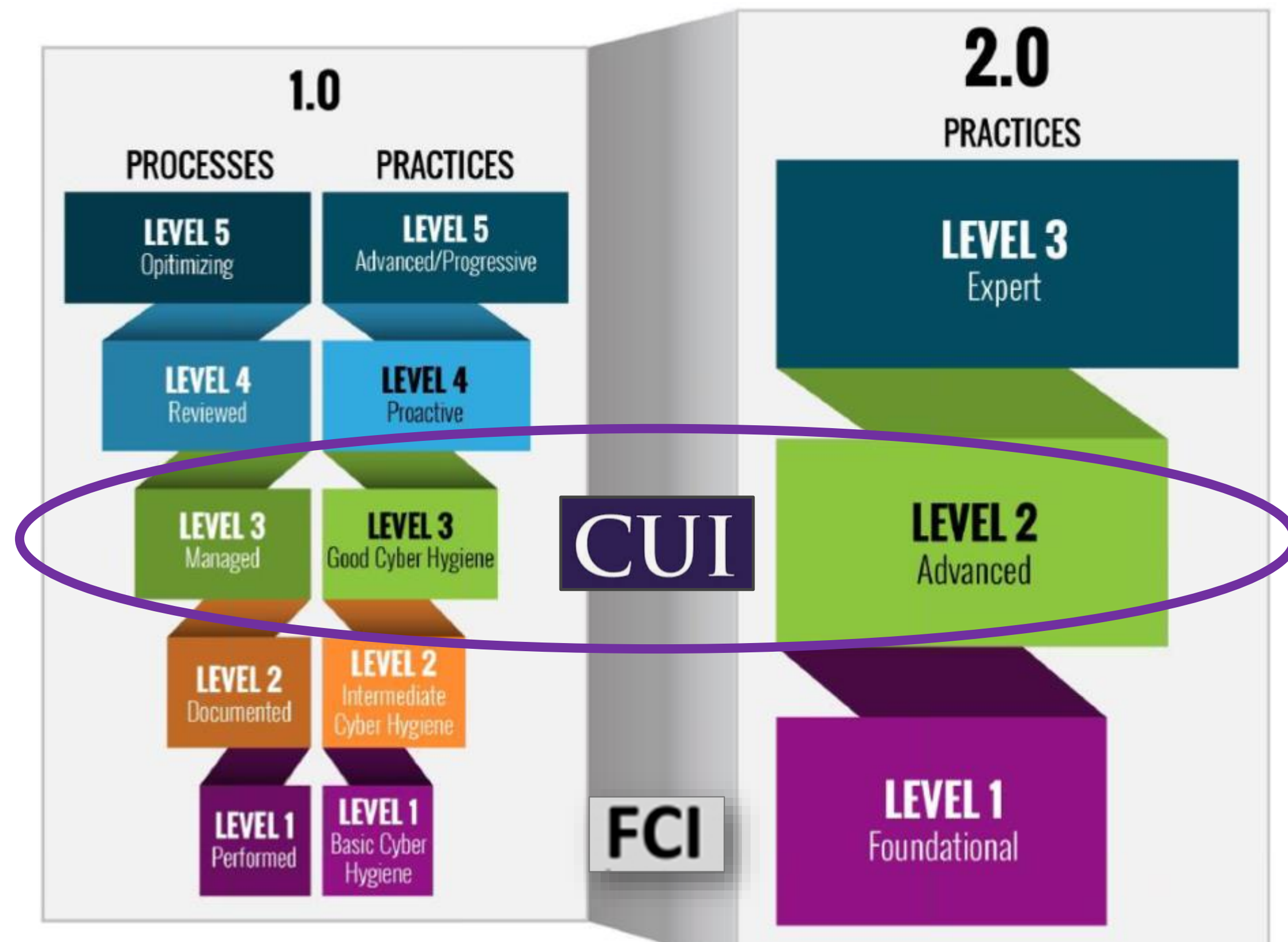
	09/30/2020	110	BASIC	NIST SP 800-171		ENTERPRISE	NJ USA 23386 THALES DEFENSE & SECURITY, INC 22605 GATEWAY CENTER DR, CLARKSBURG MD USA 6UQP0 THALES VISIONIX, INC 22605 GATEWAY CENTER DRIVE, CLARKSBURG MD USA	09/30/2020
---	------------	-----	-------	-----------------	--	------------	--	------------



# “CMMC 2.0” ANNOUNCED

Nov 4, 2021

## CMMC Model Structure



### Summary of Major Changes:


- 3 Levels of certification (was 5)
- Level 1 includes the same 17 requirements originally prescribed, but 3rd party certification no longer needed; instead, a senior company official will need to sign annual affirmations to SPRS
- CUI remains TDSI focus: Former level 2 & 3 combined into new Level 2 "Advanced" – includes all 110 controls prescribed in NIST SP 800-171 for CUI safeguarding
- Most program maturity measurements have been removed
- Some self-attestation allowed for Level 2, rather than required 3rd party assessment
- Levels 4 & 5 have been combined into new Level 3 for select projects (TBD)



# “CMMC 2.0” ANNOUNCED Nov 4, 2021

## Updates the program structure and the requirements to streamline and improve implementation of the CMMC program. Modifications include:

- DoD announced the new “strategic direction” of CMMC today after a months-long review that delayed its planned implementation
- Eliminates levels 2 and 4 and removes CMMC-unique practices and all maturity processes from the CMMC Model;
- Allowing annual self-assessments with an annual affirmation by DIB company leadership for CMMC Level 1;
- Bifurcating CMMC Level 3 requirements to identify prioritized acquisitions that would require independent assessment, and non-prioritized acquisitions that would require annual self-assessment and annual company affirmation;
- CMMC Level 5 requirements are still under development;
- Development of a time-bound and enforceable Plan of Action and Milestone process; and
- Development of a selective, time-bound waiver process, if needed and approved.



This document is scheduled to be published in the Federal Register on 11/05/2021 and available online at [federalregister.gov/d/2021-24160](https://www.federalregister.gov/d/2021-24160), and on [govinfo.gov](https://www.govinfo.gov)

**BILLING C**

**DEPARTMENT OF DEFENSE**

**Office of the Secretary**

**32 CFR Chapter I**

**Defense Acquisition Regulations System**

**48 CFR Chapter 2**

**Cybersecurity Maturity Model Certification (CMMC) 2.0 Updates and Way Forward**

**AGENCY:** Office of the Under Secretary of Defense for Acquisition and Sustainment, Department of Defense (DoD).

**ACTION:** Advanced notice of proposed rulemaking.

**SUMMARY:** This document provides updated information on DoD’s way forward for the approved CMMC program changes, designated as “CMMC 2.0.” CMMC 2.0 builds upon the initial Cybersecurity Maturity Model Certification (CMMC) framework to dynamically enhance DIB cybersecurity against evolving threats. Under the CMMC program, Defense Industrial Base (DIB) contractors will be required to implement certain cybersecurity protection standards, and, as required, obtain Cybersecurity Maturity Model Certification as a condition of DoD contract award. The CMMC framework is designed to protect sensitive unclassified information that is shared by the Department with its contractors and subcontractors and provide assurance that Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) will be

Source: [www.federalregister.gov/d/2021-24160](https://www.federalregister.gov/d/2021-24160)



- Reduces maturity levels, consolidating the levels under CMMC from five tiers to just three: **foundational, advanced and expert**
- CMMC 2.0 changes eliminate the need for the vast majority of 300,000 DIB contractors to need third-party assessments
- Contractors who only handle FCI and not the more sensitive CUI (level one “foundational” requirements) — will only be required to perform annual self-assessments
- Limited waiver process; “limited circumstances” will allow companies to make Plans of Action and Milestone (POA&Ms) to achieve certification
- **CMMC 2.0 endorsed by the CMMC Accreditation Body**

Source:

<https://federalnewsnetwork.com/defense-main/2021/11/pentagon-strips-down-cmmc-program-to-streamline-industry-cyber-assessments/>



**CMMC**  
**ACCREDITATION BODY**  
Cybersecurity Maturity Model Certification

MAIN MENU

## CMMC Accreditation Body Endorses Pentagon's Proposed Implementation Changes in CMMC 2.0



**CMMC Accreditation Body Endorses Pentagon's Proposed Implementation Changes in CMMC 2.0**

*Anticipated improvements will address cost, clarity, and scalability concerns*

(Bethesda, MD, Nov 4, 2021) - The [CMMC Accreditation Body](#) (CMMC-AB) expressed its support for the proposed changes to the implementation of the Cybersecurity Maturity Model Certification (CMMC) initiative that were revealed by the Department of Defense



# LINKS

Full wording of the interim DFARS rule:

<https://www.federalregister.gov/documents/2020/09/29/2020-21123/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of>

CMMC Model Information:

<https://www.acq.osd.mil/cmmc/draft.html>

CMMC Accreditation Body:

<https://www.cmmcab.org/>

NIST 800-171 DOD Self-Assessment Methodology:

<https://www.acq.osd.mil/dpap/pdi/cyber/docs/NIST%20SP%20800-171%20Assessment%20Methodology%20Version%201.2.1%20%206.24.2020.pdf>

Supplier Performance Risk System (SPRS) <https://www.sprs.csd.disa.mil/> or email results to [webptsmh@navy.mil](mailto:webptsmh@navy.mil)



# THANK YOU!

## Questions?

**Curtis.Chappell@thalesdsi.com**

**(240) 864-7362**

**classmgmt.com**

**For the lawyers: "...the opinions expressed by Curtis Chappell are his own and not necessarily those of NCMS or Thales Defense & Security, Inc."**

