Department of Defense (DOD) Mandatory Controlled Unclassified Information (CUI) Training

Welcome

Controlled Unclassified Information. What is it? How will I recognize it?

If these are questions you need answers to, then you are in the right place.

Welcome to the Department of Defense (DOD) Mandatory Controlled Unclassified Information (CUI) training. This course will provide a baseline introduction to CUI. It is important to note that For Official Use Only (FOUO) is no longer an authorized marking for new documents and materials in the DOD.

Introduction

Controlled Unclassified Information (CUI) is unclassified information requiring safeguarding and dissemination controls, consistent with applicable law, regulation, or government-wide policy.

The signing of Executive Order (E.O.) 13556 on November 04, 2010 established CUI. You can access this E.O. from the Course Resources.

Objectives

By the end of this course you will be able to:

- Explain the purpose for the CUI program
- Describe the purpose and location of the Information Security Oversight Office (ISOO) and DOD CUI Registries
- Apply proper initial marking requirements
- Identify decontrol requirements
- Describe safeguarding requirements
- Identify proper destruction methods
- Apply appropriate access and dissemination controls
- Explain the procedures for identifying and reporting security incidents
- State the implementation guidelines for CUI

Purpose of the CUI Program

Federal agencies routinely generate, use, store, and share information, and while it does not meet the threshold for classification as national security or atomic energy information, it does require some level of protection from unauthorized access and release.

Protection is required for privacy, law enforcement, or other reasons pursuant to and consistent with law, regulation, or government-wide policy. In the past, each agency developed its own practices for sensitive unclassified information, resulting in a patchwork of markings across the Executive Branch. This caused confusion throughout the branch.

ISOO published Title 32 Part 2002 (CUI) Code of Federal Regulations (CFR) Final Rule on September 14, 2016. This Final Rule was the "Implementing Guidance" for the CUI Program.

The Office of the Under Secretary of Defense for Intelligence and Security (OUSD (I&S)) released DOD Instruction (DODI) 5200.48, Controlled Unclassified Information, on March 6, 2020. This instruction establishes policy, assigns responsibilities, and prescribes procedures for CUI throughout DOD, in accordance with (IAW):

- E.O. 13556;
- Part 2002 of Title 32 CFR (Final Rule);
- and the Defense Federal Acquisition Regulation Supplement (DFARS) sections 252.204-7008 and 252.204-7012.

It also established the official DOD CUI Registry, which we will discuss later in the training.

CUI Program

The implementation of the DOD CUI Program addresses the designation, handling, and decontrolling of CUI in accordance with DODI 5200.48. This includes CUI identification, sharing, marking, safeguarding, storage, dissemination, destruction, and records management.

When applied to a contract for non-Federal DOD systems use Sections 252.204-7008 and 252.204-7012 of the DFARS.

Unclassified information can only be characterized as CUI if there is a law, regulation, or government-wide policy prescribing safeguarding or dissemination control. Agencies must NOT cite the Freedom of Information Act (FOIA) as a CUI safeguarding or disseminating control authority for CUI.

Knowledge Check

Let's try a review question.

Information may be CUI in accordance with:

a. FOIA withholding criteria

b. Law, regulation, or government-wide policy
c. Executive Order 13526
d. Public Affairs guidance

Answer: b. Law, regulation, or government-wide policy

Impact of CUI

The authorized holder of a document or material is responsible for determining, at the time of creation, whether the information falls into a CUI category. If so, the authorized holder is responsible for applying CUI markings and dissemination instructions accordingly. Each organization within DOD may generate specific guidance.

According to CUI Notice 2020-03 Non-Disclosure Agreement (NDA) Template for CUI, an NDA is optional, however, the Executive Agent (EA) strongly recommends using the CUI NDA to increase standardization across the Executive Branch and in contracts. The Secretary has directed the DOD to issue a DoD CUI NDA. Access the Course Resources to review the CUI NDA.

Every individual at every level, including DOD civilian and military personnel, as well as contractors providing support to the DOD in accordance with contractual requirements, will comply with the requirements in DODI 5200.48.

More information on marking, safeguarding, dissemination and destruction will be provided as you go through the training.

Responsibilities

We've mentioned the responsibilities of the individual with regard to CUI, but what about other responsibilities within the DOD?

DODI 5200.48 identifies departmental officials and elements with oversight responsibilities within DOD. For more information on the responsibilities, access the Course Resources to review the regulatory guidance.

ISOO Registry

So how do you identify what is CUI?

The ISOO CUI Registry is the Government-wide online repository for Federal-level guidance regarding CUI policy and practice. The ISOO CUI Registry is available to all military, civilian, and contractor employees.

The ISOO CUI Registry includes a Category List, CUI Markings, Limited Dissemination Controls, Decontrol, and a Registry Change Log.

It also provides Policy and Guidance and a Glossary.

Access the Course Resources for a listing of regulatory guidance and links to the ISOO Registry.

DOD Registry

The DOD CUI Registry is built on the ISOO Registry with the addition of the DOD issuance alignment. There is also a breakout of other types of information which could meet the threshold of CUI, particularly under the OPSEC category.

Automatic notifications will not be generated as the DOD CUI registry changes, so periodically check for updates.

Marking Requirements CUI Basic vs. CUI Specified

There are two designations for CUI – Basic and Specified (SP).

CUI Basic is the subset of CUI for which the authorizing law, regulation, or government-wide policy does not set out specific handling or dissemination controls. Agencies handle CUI Basic according to the uniform set of controls set forth in DODI 5200.48 and the DOD CUI Registry.

CUI Specified (SP) is the subset of CUI in which the authorizing law, regulation, or government-wide policy contains specific handling controls that it requires or permits agencies to use that differ from those for CUI Basic.

The distinction is the underlying authority spells out the controls for CUI Specified (SP) information and does not for CUI Basic information.

During DODs initial implementation of the CUI Program, DOD personnel are **not** to use any abbreviation that includes "SP".

Minimum Marking Requirements – CUI Only

Before you mark a document as CUI, you must first determine if the information is CUI. The first page of the CUI Marking Job aid (available in the Course Resources) provides a flowchart to assist you in the identification process. At initial CUI implementation, the only authorized marking for DOD CUI documents is the acronym "CUI" in the banner and footer of the document. Do not add the "U," signifying unclassified, to the banner and footer as was required with the previous FOUO marking (i.e., U//FOUO).

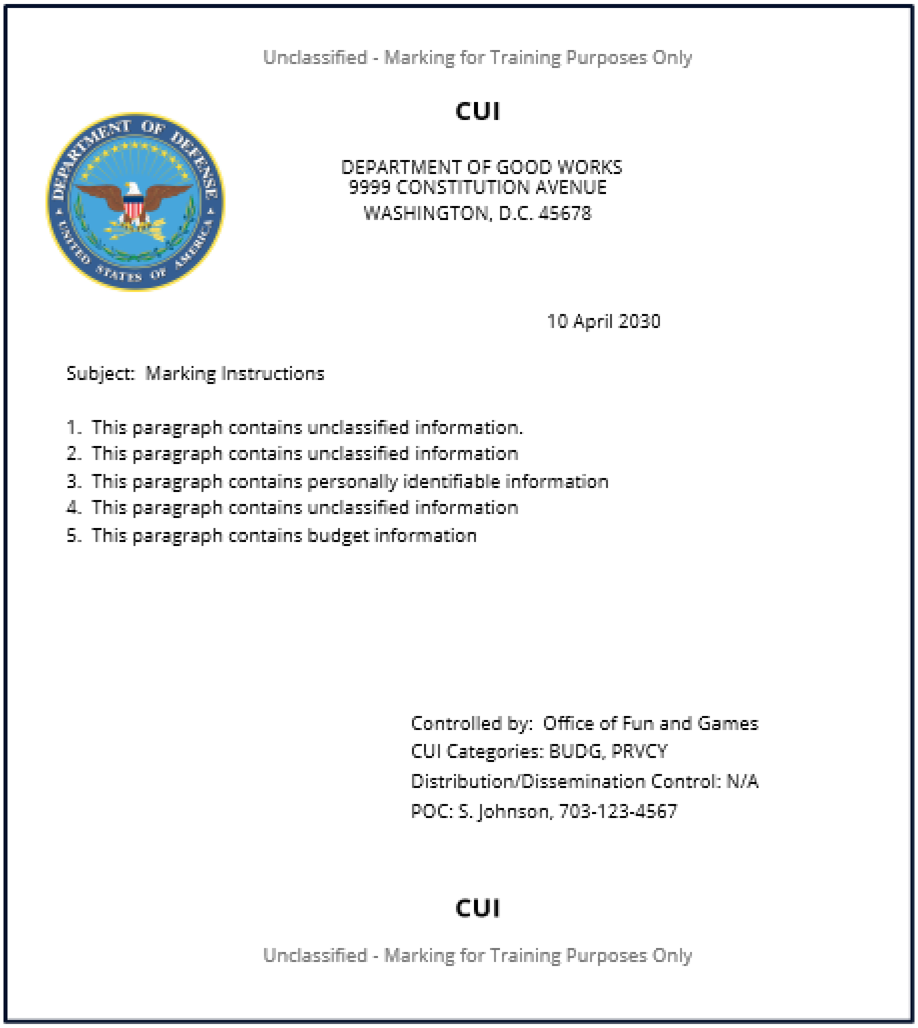
There is a requirement to add the CUI designation indicator to the first page or cover of any document containing CUI. This indicator will be located in the lower right corner and must contain at a minimum the name of the DOD Component determining that the information is CUI. If letterhead is used, this line may be omitted. In the example this document was on letterhead so that line was omitted.

The second line must identify the office making the determination. During DODs initial implementation this will be the originator of the document.

The third line must identify all types of CUI contained in the document.

The fourth line must contain the distribution statement or limited dissemination controls. If a distribution statement is required (such as for CTI or Controlled Technical Information), the words “Distribution Statement” and the letter is required, for example Distribution Statement B.

The fifth line must contain the phone number or office mailbox for the originating DOD Component or authorized CUI holder.



Unclassified - Marking for Training Purposes Only

CUI

DEPARTMENT OF GOOD WORKS
9999 CONSTITUTION AVENUE
WASHINGTON, D.C. 45678

10 April 2030

Subject: Marking Instructions

1. This paragraph contains unclassified information.
2. This paragraph contains unclassified information
3. This paragraph contains personally identifiable information
4. This paragraph contains unclassified information
5. This paragraph contains budget information

Controlled by: Office of Fun and Games
CUI Categories: BUDG, PRVCY
Distribution/Dissemination Control: N/A
POC: S. Johnson, 703-123-4567

CUI

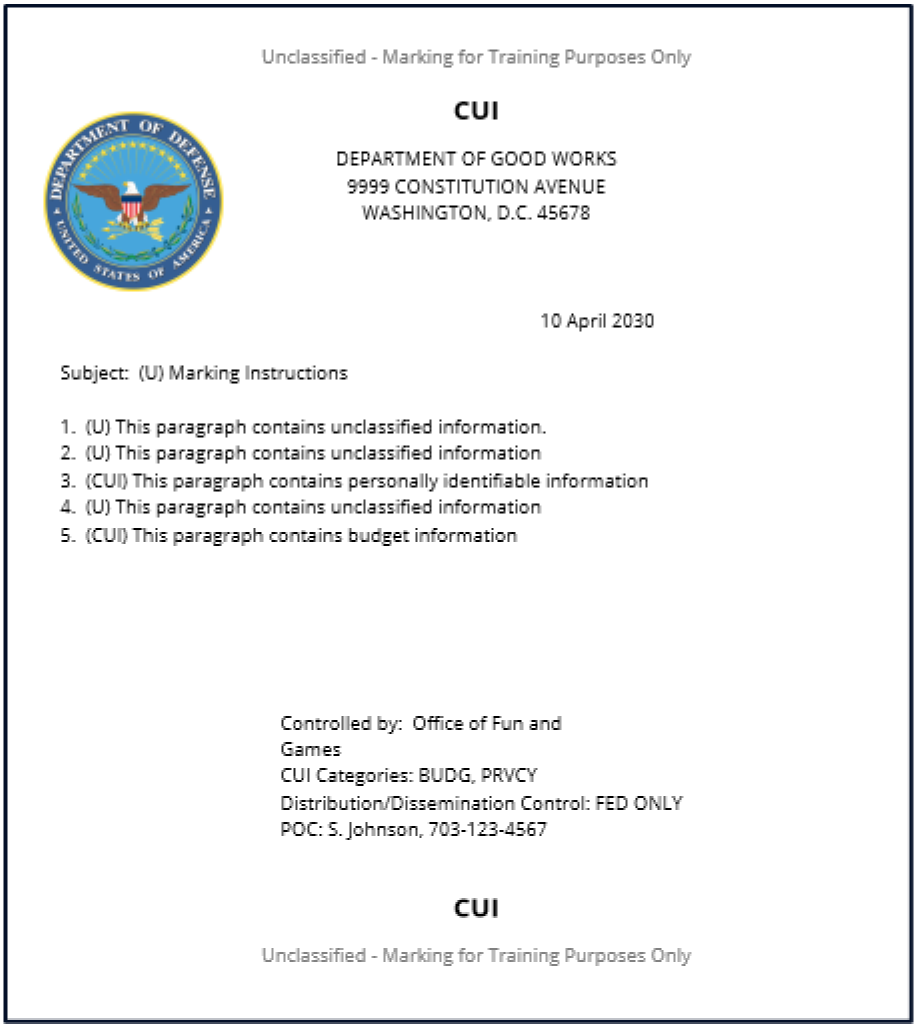
Unclassified - Marking for Training Purposes Only

Portion Markings - CUI Only

Portion markings are not required. If portion markings are selected, then all document subjects and titles, as well as individual sections, parts, paragraphs, or similar portions of a CUI document known to contain CUI, will be portion marked with “(CUI)” in accordance with DODI 5200.48

and additional component guidance. Use of the unclassified marking “(U)” as a portion marking for unclassified information within CUI documents or materials is required.

Banners, footers, and portion marking will only be marked “Unclassified” or “(U)” for unclassified information in accordance with the June 4, 2019 ISOO letter. Access the Course Resources to view the letter.



Unclassified - Marking for Training Purposes Only

CUI

DEPARTMENT OF GOOD WORKS
9999 CONSTITUTION AVENUE
WASHINGTON, D.C. 45678

10 April 2030

Subject: (U) Marking Instructions

1. (U) This paragraph contains unclassified information.
2. (U) This paragraph contains unclassified information
3. (CUI) This paragraph contains personally identifiable information
4. (U) This paragraph contains unclassified information
5. (CUI) This paragraph contains budget information

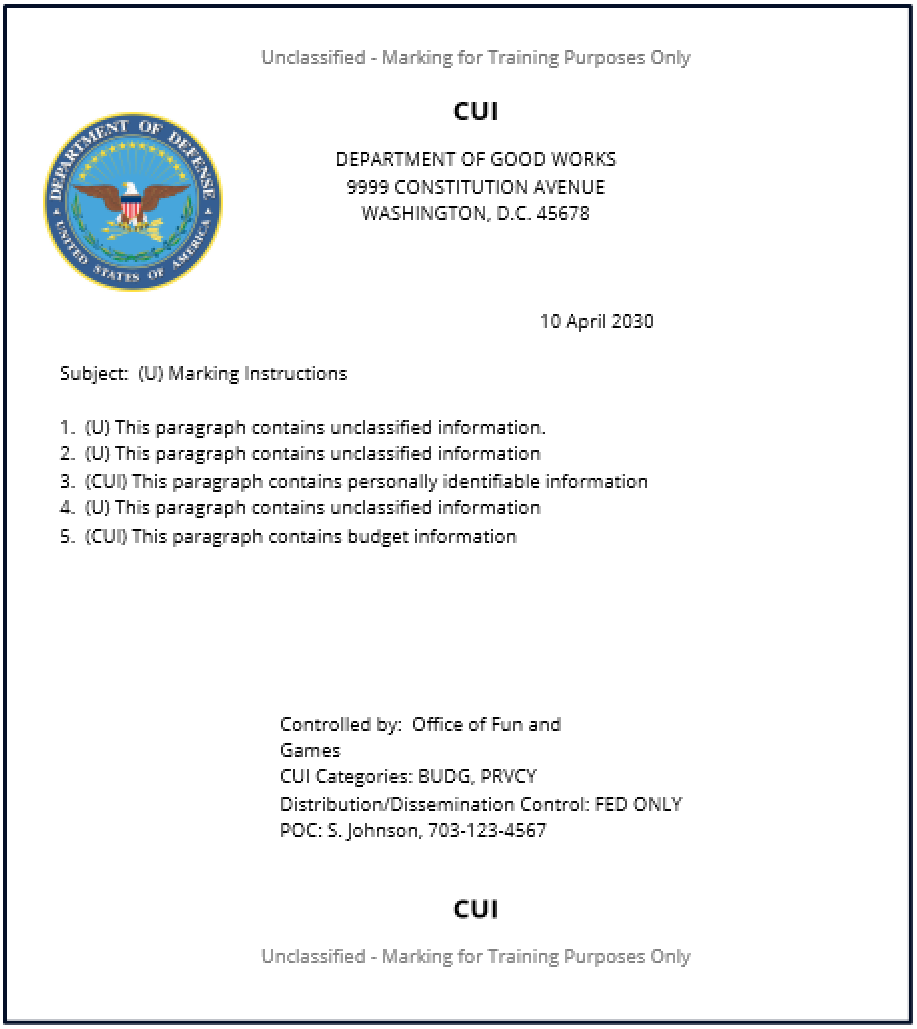
Controlled by: Office of Fun and
Games
CUI Categories: BUDG, PRVCY
Distribution/Dissemination Control: FED ONLY
POC: S. Johnson, 703-123-4567

CUI

Unclassified - Marking for Training Purposes Only

Limited Dissemination Controls (LDCs) - CUI Only

In this example, we have a CUI only document with limited dissemination controls (LDC). LDCs are utilized within DOD to limit access to certain agency-specific CUI within an organization. The third line of the designation indicatory. This LDC applies to all CUI within the document. For each individual portion, prior to secondary dissemination, authorized holders must contact the originator of the information to determine the applicability of the LDC to that specific portion.



Unclassified - Marking for Training Purposes Only

CUI

DEPARTMENT OF GOOD WORKS
9999 CONSTITUTION AVENUE
WASHINGTON, D.C. 45678

10 April 2030

Subject: (U) Marking Instructions

1. (U) This paragraph contains unclassified information.
2. (U) This paragraph contains unclassified information
3. (CUI) This paragraph contains personally identifiable information
4. (U) This paragraph contains unclassified information
5. (CUI) This paragraph contains budget information

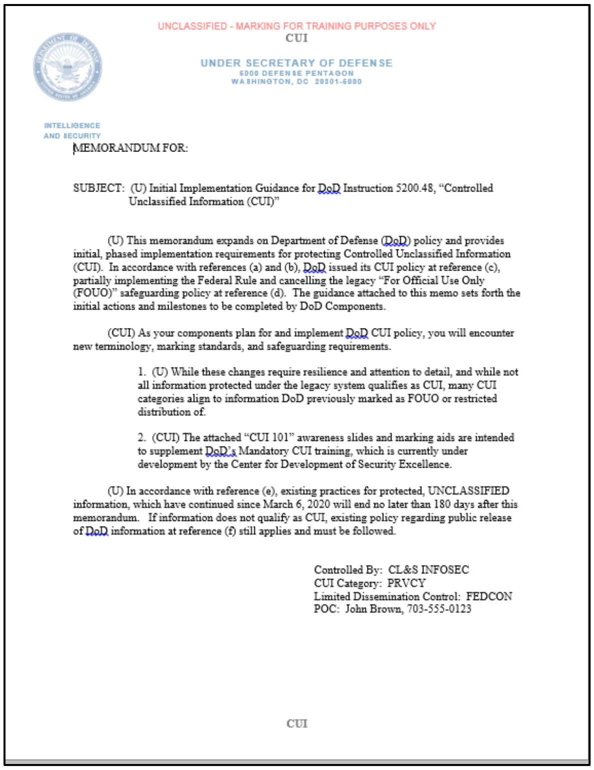
Controlled by: Office of Fun and Games
CUI Categories: BUDG, PRVCY
Distribution/Dissemination Control: FED ONLY
POC: S. Johnson, 703-123-4567

CUI

Unclassified - Marking for Training Purposes Only

Knowledge Check

As a quick review, below are two documents. The left one is marked correctly, while the right one is not.



UNCLASSIFIED - MARKING FOR TRAINING PURPOSES ONLY

CUI

UNDER SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

INTELLIGENCE
AND SECURITY

MEMORANDUM FOR:

SUBJECT: (U) Initial Implementation Guidance for DoD Instruction 5200.48, "Controlled Unclassified Information (CUI)"

(U) This memorandum expands on Department of Defense (DoD) policy and provides initial, phased implementation requirements for protecting Controlled Unclassified Information (CUI). In accordance with references (a) and (b), DoD issued its CUI policy at reference (c), partially implementing the Federal Rule and cancelling the legacy "For Official Use Only (FOUO)" safeguarding policy at reference (d). The guidance attached to this memo sets forth the initial actions and milestones to be completed by DoD Components.

(CUI) As your components plan for and implement DoD CUI policy, you will encounter new terminology, marking standards, and safeguarding requirements.

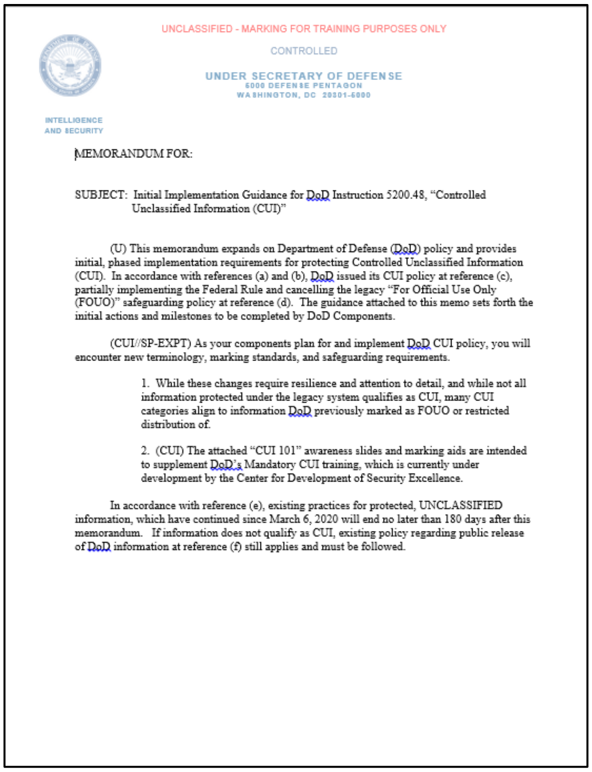
1. (U) While these changes require resilience and attention to detail, and while not all information protected under the legacy system qualifies as CUI, many CUI categories align to information DoD previously marked as FOUO or restricted distribution of.

2. (CUI) The attached "CUI 101" awareness slides and marking aids are intended to supplement DoD's Mandatory CUI training, which is currently under development by the Center for Development of Security Excellence.

(U) In accordance with reference (e), existing practices for protected, UNCLASSIFIED information, which have continued since March 6, 2020 will end no later than 180 days after this memorandum. If information does not qualify as CUI, existing policy regarding public release of DoD information at reference (f) still applies and must be followed.

Controlled By: CL&S INFOSEC
CUI Category: PRVCY
Limited Dissemination Control: FEDCON
POC: John Brown, 703-555-0123

CUI



UNCLASSIFIED - MARKING FOR TRAINING PURPOSES ONLY

CONTROLLED

UNDER SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

INTELLIGENCE
AND SECURITY

MEMORANDUM FOR:

SUBJECT: Initial Implementation Guidance for DoD Instruction 5200.48, "Controlled Unclassified Information (CUI)"

(U) This memorandum expands on Department of Defense (DoD) policy and provides initial, phased implementation requirements for protecting Controlled Unclassified Information (CUI). In accordance with references (a) and (b), DoD issued its CUI policy at reference (c), partially implementing the Federal Rule and cancelling the legacy "For Official Use Only (FOUO)" safeguarding policy at reference (d). The guidance attached to this memo sets forth the initial actions and milestones to be completed by DoD Components.

(CUI//SP-EXPT) As your components plan for and implement DoD CUI policy, you will encounter new terminology, marking standards, and safeguarding requirements.

1. While these changes require resilience and attention to detail, and while not all information protected under the legacy system qualifies as CUI, many CUI categories align to information DoD previously marked as FOUO or restricted distribution of.

2. (CUI) The attached "CUI 101" awareness slides and marking aids are intended to supplement DoD's Mandatory CUI training, which is currently under development by the Center for Development of Security Excellence.

In accordance with reference (e), existing practices for protected, UNCLASSIFIED information, which have continued since March 6, 2020 will end no later than 180 days after this memorandum. If information does not qualify as CUI, existing policy regarding public release of DoD information at reference (f) still applies and must be followed.

CUI Cover Page and SF902 Label

The use of a CUI cover page is optional, but encouraged, and can be found by selecting the course resources.

The label (SF902) is used to identify and protect electronic and other media that contains CUI.

Knowledge Check

Let's try a review question.

The correct banner marking for UNCLASSIFIED documents with CUI is:

a. UNCLASSIFIED//CUI
b. CONTROLLED
c. CONTROLLED UNCLASSIFIED INFORMATION
d. CUI

Answer: d. CUI

Marking Requirements – CUI and Classified

The CUI markings in a co-mingled ***classified*** document will appear in paragraphs or subparagraphs known to contain **only CUI** and must be portion marked with “(CUI).” “CUI” **will not** appear in the banner or footer.

An **acknowledgement** must be added to the warning box on the first page of multi-page documents to alert readers to the presence of CUI in a ***classified*** DOD document.

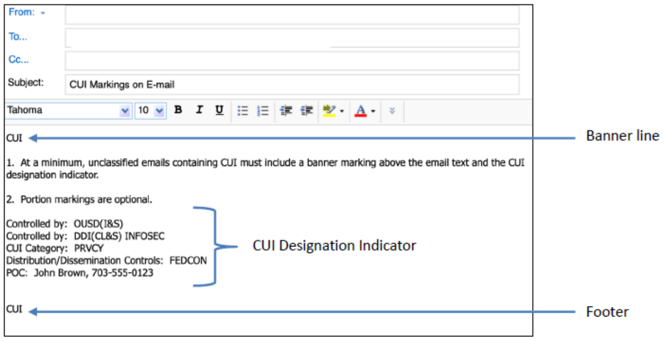
As mentioned in the previous examples, there is a requirement to add the CUI designation indicator to the first page of the document in the lower right corner.

For more information on markings for classified documents, please reference DODM 5200.01 Volume 2 available in the Course Resources.

Marking Emails

Let’s review the markings for an email. In the first example, note that the minimum marking required is “CUI” in the banner line and footer. The email must also contain the CUI designation indicator.

Minimum markings



From:
To...
Cc...
Subject: CUI Markings on E-mail

CUI

1. At a minimum, unclassified emails containing CUI must include a banner marking above the email text and the CUI designation indicator.

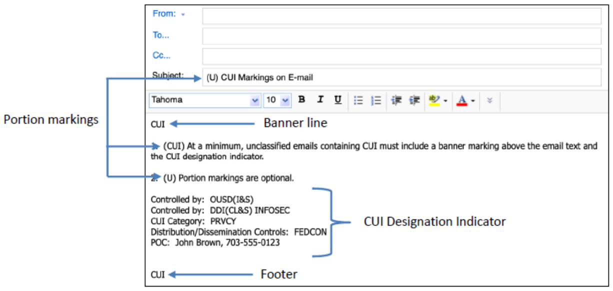
2. Portion markings are optional.

Controlled by: OUSD(I&S)
Controlled by: DDI(CL&S) INFOSEC
CUI Category: PRVCY
Distribution/Dissemination Controls: FEDCON
POC: John Brown, 703-555-0123

CUI

In the second example below you see that portion markings have been included. The banner line and footer and CUI designation indicator are also required.

Portion markings included



From:
To...
Cc...
Subject: (U) CUI Markings on E-mail

CUI

(CUI) At a minimum, unclassified emails containing CUI must include a banner marking above the email text and the CUI designation indicator.

(U) Portion markings are optional.

Controlled by: OUSD(I&S)
Controlled by: DDI(CL&S) INFOSEC
CUI Category: PRVCY
Distribution/Dissemination Controls: FEDCON
POC: John Brown, 703-555-0123

CUI

For additional information and examples, a CUI Marking Job Aid is available in the Course Resources.

If you have questions or need additional guidance on marking, contact your Security Manager or

Component Program Manager.

Knowledge Check

Let's try a review question.

The correct banner marking for a co-mingled document containing TOP SECRET, SECRET, and CUI is:

a. TOP SECRET//CUI
b. CUI
c. SECRET
d. TOP SECRET

Answer: d. TOP SECRET

How and When is CUI Decontrolled?

So how and when is CUI decontrolled?

Decontrolling and releasing CUI records is executed by the originator of the information, the Original Classification Authority (OCA), if identified in a Security Classification Guide (SCG), or designated offices for decontrolling.

There are no specific timelines to decontrol CUI unless specifically required in a law, regulation, or government-wide policy. Decontrol will occur when the CUI no longer requires safeguarding and will follow DOD records management procedures. Access the Course Resources for guidance on these procedures.

Agencies must promptly decontrol CUI properly when determined by the CUI owner to no longer require safeguarding or dissemination controls, unless doing so conflicts with the related law, regulation, or government-wide policy.

Decontrolling CUI through the public release process relieves authorized holders from requirements for handling information in accordance with the CUI program.

Decontrol CUI

A prepublication review must be conducted in accordance with DODI 5230.09 and DODI 5230.29 before public release may be authorized. As a reminder, prepublication review of UNCLASSIFIED information is required prior to public release regardless of whether or not it was ever subject to control.

When CUI is decontrolled, all known holders will be notified by email or other means. Upon notification, holders will remove the CUI markings. Holders will not need to retrieve records on file solely for this purpose. Information with a decontrolled CUI status will not be publicly released without review.

Review the CUI Marking Job Aid for an example of a decontrolled document.

Knowledge Check

Let's try a review question.

I don't have a security clearance, so I don't have to get a pre-publication review.
True
False

Answer: False

Safeguarding

We have discussed recognizing, marking and decontrolling CUI, but how do you safeguard it?

All DOD information will be protected 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, take steps to 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, as mentioned earlier, is optional.

After working hours, CUI will be stored in unlocked containers, desks, or cabinets if the government or government-contract building provides security for continuous monitoring of access. 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. For DOD, an open storage environment meets these requirements.

Safeguarding – System and Network Requirements

For Information Systems, the basic system and network configuration is Moderate Confidentiality, in accordance with the guidelines of the National Institute of Standards and Technology (NIST) SP 800-171 for non-Federal systems and NIST SP 800-53 for Federal systems special publications.

CUI Transmission

CUI material may be transmitted via first class mail, parcel post, or bulk shipments. When practical, CUI may be transmitted electronically (e.g., data, website, or e-mail), via approved secure communications systems or systems utilizing other protective measures such as Public Key Infrastructure (PKI) or transport layer security (e.g., https).
Avoid wireless telephone transmission of CUI when other options are available.

CUI transmission via facsimile machine is permitted; however, the sender is responsible for determining whether appropriate protection will be available at the receiving location before transmission (e.g., facsimile machine attended by a person authorized to receive CUI; facsimile machine located in a controlled government environment).

Destruction Requirements

You have learned how to mark, safeguard and decontrol CUI, but now it needs to be destroyed. What do you do?

Before any CUI can be destroyed, it must be processed through the Records Management procedures. It must be identified as temporary or permanent and handled accordingly.

When destroying CUI, including in electronic form, agencies must do so in a manner making it unreadable, indecipherable, and irrecoverable. If the law, regulation, or government-wide policy specifies a method of destruction, agencies must use the method prescribed. Two approved methods for destroying paper based CUI are cross-cut shredding that produces 1 mm x 5 mm particles (or smaller) or pulverizing. Additional guidance for destroying CUI documents and materials is provided in DODI 5200.48 and CUI Notice 2019-03.
CUI documents and materials will be formally reviewed in accordance with DODI 5230.09 and DODI 5200.48, before approved disposition authorities are applied, including destruction.

Access the Course Resources for access to the regulatory guidance for destruction and records management procedures.

Access and Dissemination

Who can access CUI?

Access to CUI is based on having a lawful government purpose, unlike the need-to-know (NTK) required for access to classified information. CUI access should be encouraged and permitted to the extent the access or dissemination:

- Complies with the law, regulation, or government-wide policy identifying the information as CUI
- Furthers a lawful government purpose
- Is not restricted by an authorized Distribution Statement or Limited Dissemination

Control (LDC)
- Is not otherwise prohibited by any other law, regulation, or government-wide policy

Agencies may place limits on disseminating CUI for a lawful government purpose only using the dissemination controls identified in DODI 5200.48, or methods authorized by a specific law, regulation, or government-wide policy. LDCs or distribution statements CANNOT unnecessarily restrict CUI access.

Since DOD Components need to retain certain agency-specific CUI within their organizations, DOD Components may use the LDCs to limit access to those on an accompanying dissemination list. For example, raw data, information, or products must be processed and analyzed before determining if further dissemination is required or permitted.

Access the CUI Marking Job Aid from the Course Resources for information on LDC's.

Knowledge Check

Let's try a review question.

In order to obtain access to CUI, an individual must first have:

a. A Need-to-Know
b. Approval from their Supervisor
c. Approval from their Security Manager
d. A lawful government purpose

Answer: d. A lawful government purpose

Security Incidents

What happens if CUI is misused, disclosed without authorization, or improperly marked?

The DOD Components' Senior Agency Official (CSAO) and Component Program Manager (CPM) will establish procedures to ensure prompt and appropriate management action to take in cases of CUI misuse, including unauthorized disclosure (UD) of CUI, improper CUI designation and marking, violation of DODI 5200.48, and incidents potentially placing CUI at risk of UD. Such actions will focus on correcting or eliminating the conditions contributing to the incident.

For UD of CUI, no formal security inquiry or investigation is required unless disciplinary action will be taken against the individual(s) responsible. In such cases, a preliminary inquiry is appropriate. UD of certain CUI, such as export-controlled technical data, may also result in potential civil and criminal sanctions against responsible persons based on the procedures codified in the relevant law, regulation, or government-wide policy. The DOD Component originating the CUI is informed of any UD.

Administrative, civil, or criminal sanctions may be imposed based on the category of CUI.

Reporting or accounting for UD of CUI shall be done in accordance with DODI 5200.48. Report misuse, mishandling, or UD of CUI to the UD Program Management Office (PMO). In addition, notify the appropriate Military Department Counterintelligence (CI) organization of all incidents.

Implementation Schedule

When will I be required to implement CUI requirements?

Refer to your Component Program Manager for implementation guidance and other questions regarding CUI.

Summary

Now that you have completed this training, you should be able to:

- Explain the purpose for the CUI program
- Describe the purpose and location of the ISOO and DOD CUI Registries
- Apply proper initial marking requirements
- Identify decontrol requirements
- Describe safeguarding requirements
- Identify proper destruction methods
- Apply appropriate access and dissemination controls
- Explain the procedures for identifying and reporting security incidents
- State the implementation guidelines for CUI