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

Table of Contents

Introduction and Course Logistics *(Running Time 5:53)*

PAGE 1

Audio: Welcome to the Department of Defense (DoD) Mandatory Controlled Unclassified Information (CUI) Training.

On screen:

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

PAGE 2

Audio: If you would like to follow along with a written transcript of this training, you can download a copy by clicking on the Transcript icon located in the lower left corner of the screen, marked by the "T" symbol. You can also download the transcript from the Resources page of this training site. You can access the Resources page by clicking on "Resources" at the top of the screen.

Closed captioning is available for this course and can be activated by clicking on the Closed Captioning icon located in the lower left corner of the screen, marked by the "CC" symbol.

On screen:

(Image of course transcript)

PAGE 3

Audio: Users can access this course via screen reader software. When screen reader mode is enabled, this training course will automatically pause at the end of each screen, allowing time to review all on-screen information before continuing. Detailed instructions on how to take this course with assistive software can be found at the link provided here. You can also access these instructions from the Resources page of this training site.

If you are currently using screen reader software, use the Up and Down arrow keys to activate screen reader mode. Otherwise, click on the "RESUME" button to continue without activating these features.

On screen:

If you do not require assistive software, click here to skip this page.

Users requiring additional assistance can access this course utilizing their screen reader software. This feature is only intended for users who currently have assistive software on their computer.

(Image of "View Screen Reader Instructions" button)

Note: Activating screen reader mode without assistive software will prevent the training from running properly.

(Image of "RESUME" button)

PAGE 4

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

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

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.

On screen:

Welcome

Controlled Unclassified Information

- What is it?
- How will I recognize it?

This course will provide a baseline introduction to CUI.

Note: For Official Use Only (FOUO) is no longer an authorized marking for new documents and materials in the DoD.

PAGE 5

Audio: 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. by selecting the Resources tab at the top right corner of the screen. As you advance through this course, any time a policy or regulation is mentioned, you can select the Resources tab to access the regulatory guidance.

On screen:

Introduction

Controlled Unclassified Information (CUI) **–**

Unclassified information requiring safeguarding and dissemination controls, consistent with applicable law, regulation, or government-wide policy.

(Images of the White House and Executive Order 13556)

PAGE 6

Audio: At 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; and
- State the implementation guidelines.

On screen:

Objectives

- 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

PAGE 7

Audio: During this course of instruction, individual training modules will be presented. We will begin with an overview of the CUI Program. We will then discuss marking CUI, and will conclude with a discussion on procedures for handling CUI.

On screen:

Course Structure

- CUI Program Overview
- Marking CUI
- Handling of CUI

PAGE 8

Audio: Before we begin the training modules, let's discuss the logistics involved in this web-based training.

To accommodate your work schedule, this training provides the ability for you to log out at any time. Your progress will be saved after each page you view. If you log out in the middle of the training, you will resume the training where you left off the next time you log in.

On screen:

Course Logistics

- You may log out at any time during the training
- When you log back in, you will resume training where you left off

PAGE 9

Audio: You must complete each training module in the sequence in which it is presented. However, you will be able to review any previously completed training modules by clicking on "Menu", highlighted here, and then on the training topic.

During the presentation of each training module, you will have the ability to pause the presentation, skip back, and replay the training module again. If you review a module that has already been completed, you will also have the ability to skip ahead.

On screen:

Course Logistics

- Each training module must be completed in the sequence in which it is presented
- You can review previously completed training modules
- During each training module, you may pause, go back, or restart the module

PAGE 10

Audio: During the course of instruction, you will be presented with knowledge checks to ensure your understanding of the information presented to you.

At the end of each module of instruction, click on the "NEXT" button to proceed to the next module.

On screen:

Course Logistics

- You will be presented with knowledge checks to ensure your understanding of the information presented to you
- Upon completion of each training module, click on the "NEXT" button to proceed to the next module

PAGE 11

Audio: After you have completed all of the training modules, you will be presented with a final exam to test your overall knowledge of the information presented to you in this training course. You will be required to achieve a score of 70% in order to complete the training. You will be given three opportunities to pass the exam. If you do not pass after three attempts, you will be required to view the training again from the beginning.

On screen:

Course Logistics

- At the end of the training, you will be presented with a final exam
- You must achieve a score of 70% to complete the training
- You will have three opportunities to pass the exam
- If you do not pass after three attempts, you will be required to view the entire course again

PAGE 12

Audio: Upon successful completion of the course, a Certificate of Completion will be provided for you to print out.

On screen:

(Image of sample course completion certificate)

PAGE 13

Audio: As previously mentioned, a Resources page has been created for this web-based training. In addition to a written transcript of the training, this page contains links to references used throughout the training that you can access at any time for more information regarding the topics being discussed.

On screen:

(Image of course Resources page)

PAGE 14

Audio: Now that you have a feel for how to navigate through this web-based training, let's begin.

Click on the "NEXT" button to start the presentation of the first training module, an overview of the CUI Program.

On screen:

Coming up next:

CUI Program Overview

(Image of "NEXT" button)

CUI Program Overview *(Running Time 6:50)*

PAGE 1

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

On screen:

Purpose of the CUI Program

- Federal agencies routinely generate, use, store, and share information
    - Does not meet the threshold for classification as national security or atomic energy information
    - 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
    - Caused confusion throughout the Executive Branch

(Image of Title 32 Code of Federal Regulations (CFR) Part 2002 (CUI))

PAGE 2

Audio: The Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)) released the Department of Defense 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:

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

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

On screen:

Purpose of the CUI Program

(Image of DoD Instruction 5200.48)

- 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)
    - Defense Federal Acquisition Regulation Supplement (DFARS) Section 252.204-7008 and 252.204-7012
- It also established the official DoD CUI Registry, which we will discuss later in the training

PAGE 3

Audio: 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 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.

On screen:

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
    - Records management
- When applied to a contract for non-Federal systems, use DFARS Sections:
    - 252.204-7008
    - 252.204-7012
- 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

PAGE 4

Audio: Let's try a review question.

On screen:

Knowledge Check

Knowledge Check 1

On screen:

Information may be CUI in accordance with:

A. Executive Order 13526

B. Public Affairs guidance

C. **Law, regulation, or government-wide policy**

D. FOIA withholding criteria

PAGE 5

Audio: 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 Resources tab 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.

On screen:

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
    - 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
    - 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
- 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

(Image of Non-Disclosure Agreement)

PAGE 6

Audio: 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 Resources tab to review the regulatory guidance.

On screen:

Responsibilities

- DoDI 5200.48 identifies departmental officials and elements with oversight responsibilities within DoD

(Image of DoD Instruction 5200.48)

PAGE 7

Audio: 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.

Look at the example on the screen. Note the Categories, Markings and Controls sections. You will see a Category List, CUI Markings, Limited Dissemination Controls, Decontrol, and a Registry Change Log.

There is also a section for Policy and Guidance and a Glossary.

Select the Resources tab to see a listing of regulatory guidance and links to the ISOO Registry.

On screen:

ISOO Registry

- 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

(Image of ISOO Registry screen shot – Categories; Markings and Controls; Policy and Guidance; and Glossary links highlighted)

PAGE 8

Audio: 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.

A Common Access Card (CAC) is required to access the DoD Registry and an Intelink account must be created.

The Government Contracting Activities (GCA) will be required to provide CUI Registry information to contractors.

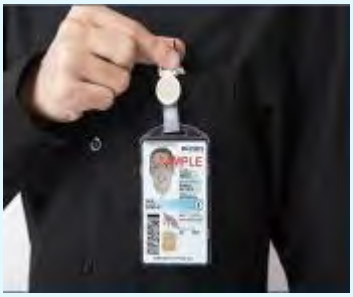
Automatic notifications will not be generated as the DoD CUI Registry changes, so periodically check for updates.

Select the Resources tab for links to Intelink and the DoD CUI Registry.

On screen:

DoD Registry

(Image of Intelink account page screen shot)



(Image of sample CAC)

- The Government Contracting Activities (GCA) will be required to provide CUI Registry information to contractors
- Automatic notifications will not be generated as the DoD CUI Registry changes, so periodically check for updates

PAGE 9

Audio: This concludes this training module. In the next training module, we will discuss marking CUI.

Click on the "NEXT" button to proceed.

On screen:

Coming up next:

Marking CUI

(Image "NEXT" button)

Marking CUI *(Running Time 7:19)*

PAGE 1

Audio: 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 that the underlying authority spells out the controls for CUI Specified (SP) information and does not for CUI Basic information.

During DoD's initial implementation of the CUI Program, DoD personnel are not to use any abbreviation that includes "SP."

On screen:

Marking Requirements – CUI Basis vs. CUI Specified

- CUI Basic – 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) – 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 that the underlying authority spells out the controls for CUI Specified (SP) information and does not for CUI Basic information
    - During DoD's initial implementation of the CUI Program, DoD personnel are not to use any abbreviation that includes "SP"

PAGE 2

Audio: 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 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 as shown on the screen. Do not add the "U," signifying unclassified, to the banner and footer as was required with the previous FOUO marking (for example, U//FOUO).

On screen:

Minimum Marking Requirements – CUI Only

- Before you mark a document as CUI, you must first determine if the information is CUI
- 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)

(Image of document marked as CUI; banner and footer highlighted)

PAGE 3

Audio: 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. Note in the example on the screen that this document was on letterhead so that line was omitted.

The second line must identify the office making the determination. During DoD's initial implementation, this will be the originator of the document.

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

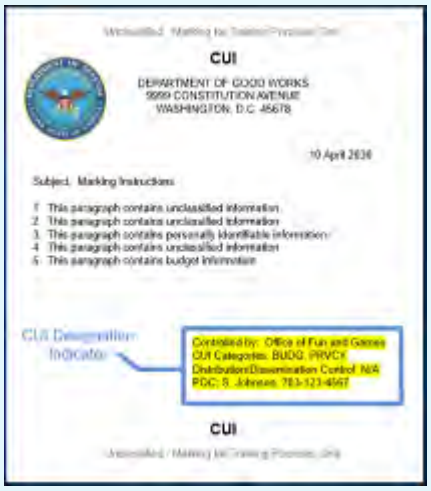
The fourth line must contain the distribution statement or limited dissemination controls. If a distribution statement is required, such as for CTI, the words "Distribution Statement" and the letter are required (for example, Distribution Statement B).

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

On screen:

Minimum Marking Requirements – CUI Only

Add the CUI designation indicator to the first page or cover of any document containing CUI.



(Image of letterhead document marked as CUI; CUI Designation Indicator highlighted)

PAGE 4

Audio: Take a look at the screen. Here is an example of portion marking. 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 markings will only be marked "Unclassified" or "(U)" for unclassified information in accordance with the June 4, 2019 ISOO letter.

Select the Resources tab to view the letter.

On screen:

Portion Markings – CUI Only

Banners, footers, and portion markings will only be marked "Unclassified" or "(U)" for unclassified information in accordance with the June 4, 2019 ISOO letter.

(Image of document marked as CUI; Portion markings highlighted)

PAGE 5

Audio: In this next example, we have a CUI Only document with limited dissemination controls (LDCs). LDCs are utilized within DoD to limit access to certain agency-specific CUI within an organization. Take a look at the third line in the designation indicator. Note that this document has a FED ONLY dissemination control. This LDC will apply to all CUI within a 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.

As a quick review, take a look at the two documents on the screen. The document to the left is marked correctly, while the document to the right is not.

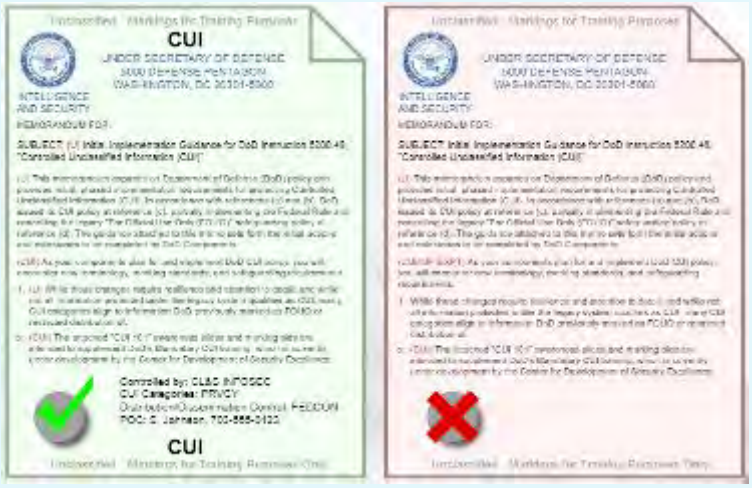
Access the Resources tab to review the CUI Marking Job Aid for additional examples on marking CUI.

On screen:

Limited Dissemination Controls – CUI Only

(Image of document marked as CUI; Distribution/Dissemination highlighted)

- LDCs are utilized within DoD to limit access to certain agency-specific CUI within an organization
- 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



(Images of correctly marked and incorrectly marked documents)

(Image of "RESUME" button)

PAGE 6

Audio: The use of a CUI cover page (as shown on the screen) is optional but encouraged and can be found by selecting the Resources tab.

The label (SF 902) is used to identify and protect electronic and other media that contains CUI.

On screen:

CUI Cover Page and SF 902 Label

(Images of CUI cover page and SF 902 label)

PAGE 7

Audio: Let's try a review question.

On screen:

Knowledge Check

Knowledge Check 1

On screen:

The correct banner marking for UNCLASSIFIED documents with CUI is:

A. Controlled Unclassified Information

B. Controlled

C. Unclassified//CUI

D. **CUI**

PAGE 8

Audio: 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 Resources tab.

On screen:

Marking Requirements – CUI and Classified

(Images of co-mingled classified document with CUI markings; CUI portion markings and designation indicator highlighted)

PAGE 9

Audio: Let's look at some examples of 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.

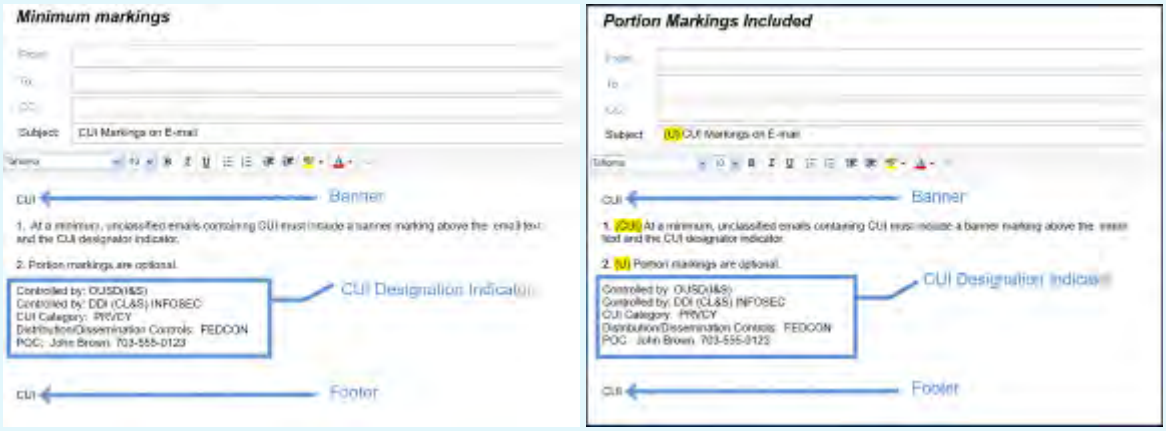
In the second example, you see that portion markings have been included. The banner line and footer and CUI designation indicator are also required.

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

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

On screen:

Marking Requirements – CUI and Classified



(Images of emails containing CUI with minimum markings and with portion markings included; banner, footer, subject, paragraph, and designation indicator highlighted)

PAGE 10

Audio: Let's try a review question.

On screen:

Knowledge Check

Knowledge Check 2

On screen:

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

A. **TOP SECRET**

B. CUI

C. TOP SECRET//CUI

D. SECRET

PAGE 11

Audio: This concludes this training module. In the next training module, we will discuss handling of CUI.

Click on the "NEXT" button to proceed.

On screen:

Coming up next:

Handling of CUI

(Image "NEXT" button)

Handling of CUI (Running Time 10:57)

PAGE 1

Audio: 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. Select the Resources tab for guidance on these procedures.

Agencies must promptly decontrol CUI that has been properly 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.

On screen:

Decontrol

- Decontrolling and releasing CUI records is executed by:
    - Originator of the information
    - Original Classification Authority (OCA), if identified in a Security Classification Guide (SCG)
    - 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
- Agencies must promptly decontrol CUI that has been properly 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

PAGE 2

Audio: Decontrolling CUI through the public release process relieves authorized holders from requirements for handling information in accordance with the CUI program. A pre-publication review must be conducted in accordance with DoDI 5230.09 and DoDI 5230.29 before public release may be authorized. As a reminder, pre-publication review of UNCLASSIFIED information is required prior to public release regardless of whether or not it was ever subject to control.

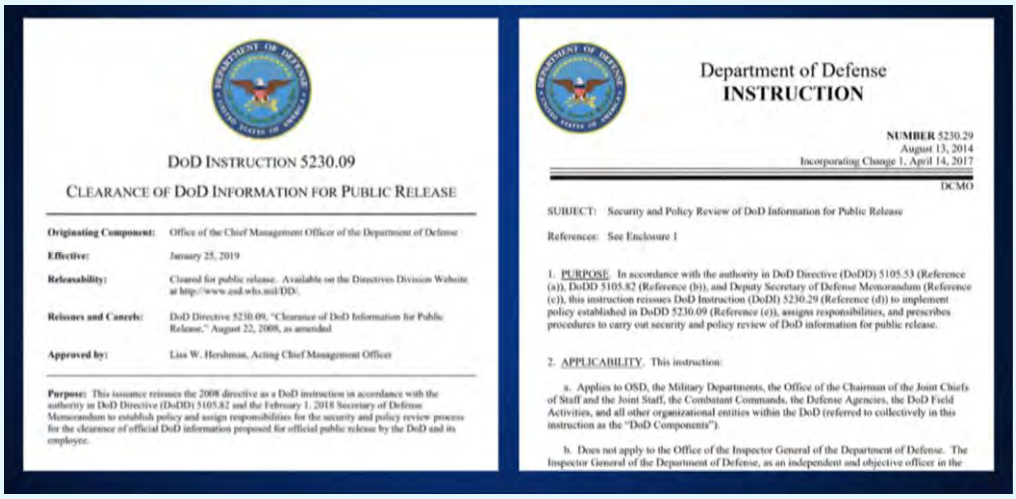
When CUI is decontrolled, all known holders will be notified by email or other means. Upon notification, holders will remove the CUI markings. Holders will not need to retrieve records on file solely for this purpose. Information with a decontrolled CUI status will not be publicly released without review.

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

On screen:

Decontrol

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



DoD INSTRUCTION 5230.09

CLEARANCE OF DoD INFORMATION FOR PUBLIC RELEASE

Originating Component: Office of the Chief Management Officer of the Department of Defense

Effective: January 25, 2019

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

Reissues and Cancels: DoD Directive 5230.09, "Clearance of DoD Information for Public Release," August 22, 2008, as amended

Approved by: Lisa W. Hershman, Acting Chief Management Officer

Purpose: This issuance reissues the 2008 directive as a DoD instruction in accordance with the authority in DoD Directive (DoDD) 5105.82 and the February 1, 2018 Secretary of Defense Memorandum to establish policy and assign responsibilities for the security and policy review process for the clearance of official DoD information proposed for official public release by the DoD and its employee.

Department of Defense
INSTRUCTION

NUMBER 5230.29
August 13, 2014
Incorporating Change 1, April 14, 2017
DCMO

SUBJECT: Security and Policy Review of DoD Information for Public Release

References: See Enclosure 1

1. PURPOSE. In accordance with the authority in DoD Directive (DoDD) 5105.53 (Reference (a)), DoDD 5105.82 (Reference (b)), and Deputy Secretary of Defense Memorandum (Reference (c)), this instruction reissues DoD Instruction (DoDI) 5230.29 (Reference (d)) to implement policy established in DoDD 5230.09 (Reference (e)), assigns responsibilities, and prescribes procedures to carry out security and policy review of DoD information for public release.

2. APPLICABILITY. This instruction:

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 Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this instruction as the "DoD Components").

b. Does not apply to the Office of the Inspector General of the Department of Defense. The Inspector General of the Department of Defense, as an independent and objective officer in the

(Images of DoDI 5230.09 and DoDI 5230.29)

- 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

PAGE 3

Audio: Let's try a review question.

On screen:

Knowledge Check

Knowledge Check 1

On screen:

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

A. True

B. **False**

PAGE 4

Audio: 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 cover sheets, 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 are sufficient internal security measures in place to prevent or detect unauthorized access to CUI. For DoD, an open storage environment meets these requirements.

On screen:

Safeguarding

- 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 cover sheets, 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 are sufficient internal security measures in place to prevent or detect unauthorized access to CUI

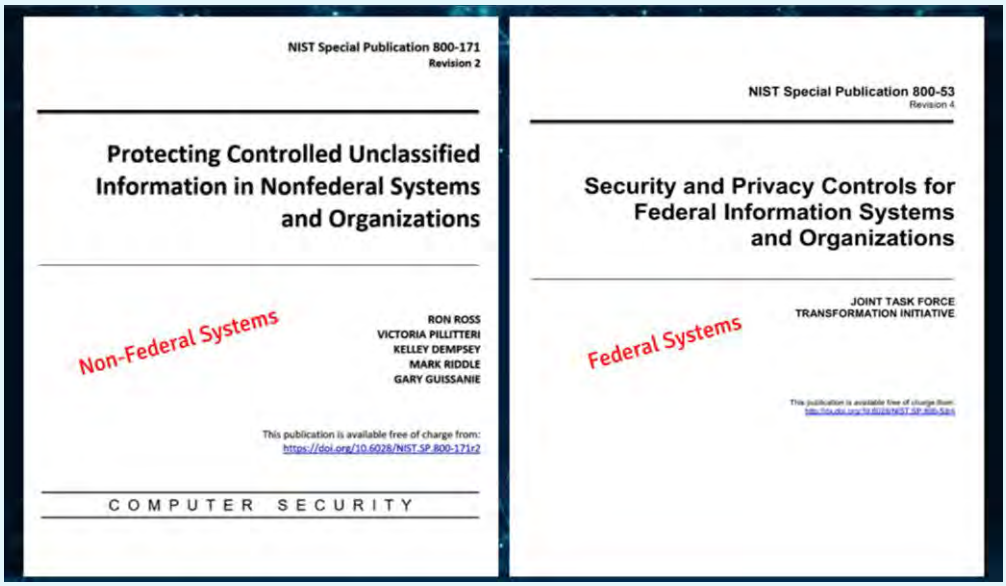
PAGE 5

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

On screen:

Safeguarding – System and Network Requirements

For Information Systems, the basic system and network configuration is Moderate Confidentiality.



(Images of NIST SP 800-171(Non-Federal Systems) and NIST SP 800-53 (Federal Systems))

PAGE 6

Audio: CUI material may be transmitted via first-class mail, parcel post, or bulk shipments. When practical, CUI may be transmitted electronically (for example, data, website, or email), via approved secure communications systems, or systems utilizing other protective measures, such as Public Key Infrastructure (PKI) or transport layer security (for example, 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 (for example, a facsimile machine attended by a person authorized to receive CUI or a facsimile machine located in a controlled government environment).

On screen:

CUI Transmission

- CUI material may be transmitted via:
    - First-class mail
    - Parcel post
    - Bulk shipments
    - Electronically (e.g., data, website, or email)
    - Approved secure communications systems
    - 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
    - Sender is responsible for determining whether appropriate protection will be available at the receiving location before transmission
    - Examples:
        - A facsimile machine attended by a person authorized to receive CUI
        - A facsimile machine located in a controlled government environment

PAGE 7

Audio: You've 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 unrecoverable. 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 DoDM 5200.01 Volume 3 and CUI Notice 2019-03.

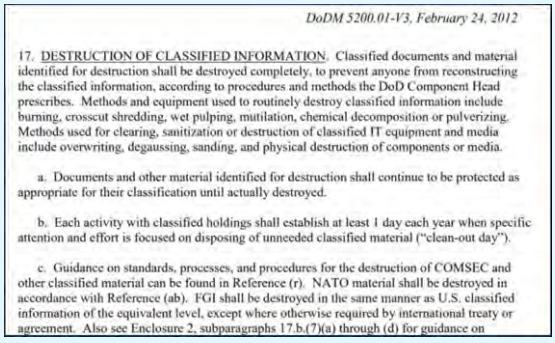
CUI documents and materials will be formally reviewed in accordance with DoDI 5230.09 and DoDI 5200.48 before approved disposition authorities are applied, including destruction.

Select the Resources tab for access to the regulatory guidance for destruction and Records Management procedures.

On screen:

Destruction Requirements

- Before any CUI can be destroyed, it must be processed through the Records Management procedures
- When destroying CUI, including in electronic form, agencies must do so in a manner making it unreadable, indecipherable, and unrecoverable
- Two approved methods for destroying paper-based CUI are:
    - Cross-cut shredding that produces 1 mm x 5 mm particles (or smaller)
    - Pulverizing



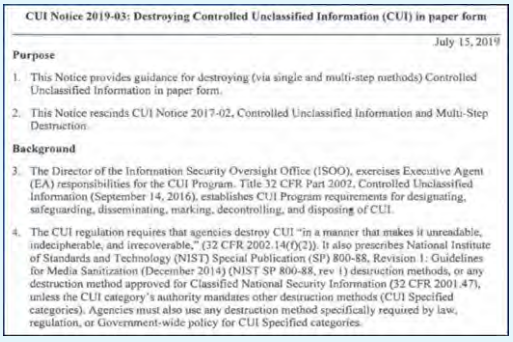
DoDM 5200.01-V3, February 24, 2012

17. DESTRUCTION OF CLASSIFIED INFORMATION. Classified documents and material identified for destruction shall be destroyed completely, to prevent anyone from reconstructing the classified information, according to procedures and methods the DoD Component Head prescribes. Methods and equipment used to routinely destroy classified information include burning, crosscut shredding, wet pulping, mutilation, chemical decomposition or pulverizing. Methods used for clearing, sanitization or destruction of classified IT equipment and media include overwriting, degaussing, sanding, and physical destruction of components or media.

a. Documents and other material identified for destruction shall continue to be protected as appropriate for their classification until actually destroyed.

b. Each activity with classified holdings shall establish at least 1 day each year when specific attention and effort is focused on disposing of unneeded classified material ("clean-out day").

c. Guidance on standards, processes, and procedures for the destruction of COMSEC and other classified material can be found in Reference (r). NATO material shall be destroyed in accordance with Reference (ab). FGI shall be destroyed in the same manner as U.S. classified information of the equivalent level, except where otherwise required by international treaty or agreement. Also see Enclosure 2, subparagraphs 17.b.(7)(a) through (d) for guidance on



CUI Notice 2019-03: Destroying Controlled Unclassified Information (CUI) in paper form

July 15, 2019

Purpose

1. This Notice provides guidance for destroying (via single and multi-step methods) Controlled Unclassified Information in paper form.
2. This Notice rescinds CUI Notice 2017-02, Controlled Unclassified Information and Multi-Step Destruction.

Background

3. The Director of the Information Security Oversight Office (ISOO), exercises Executive Agent (EA) responsibilities for the CUI Program. Title 32 CFR Part 2002, Controlled Unclassified Information (September 14, 2016), establishes CUI Program requirements for designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI.
4. The CUI regulation requires that agencies destroy CUI "in a manner that makes it unreadable, indecipherable, and irrecoverable," (32 CFR 2002.14(f)(2)). It also prescribes National Institute of Standards and Technology (NIST) Special Publication (SP) 800-88, Revision 1: Guidelines for Media Sanitization (December 2014) (NIST SP 800-88, rev 1) destruction methods, or any destruction method approved for Classified National Security Information (32 CFR 2001.47), unless the CUI category's authority mandates other destruction methods (CUI Specified categories). Agencies must also use any destruction method specifically required by law, regulation, or Government-wide policy for CUI Specified categories.

(Images of DoDM 5200.01 Volume 3 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

PAGE 8

Audio: 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); and
- Is not otherwise prohibited by any other law, regulation, or government-wide policy.

On screen:

Access and Dissemination

- 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

PAGE 9

Audio: 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.

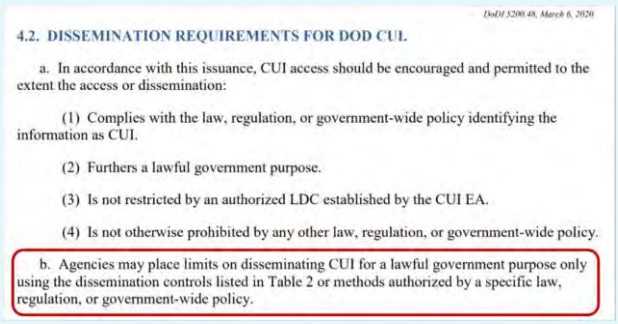
LDCs or distribution statements CANNOT unnecessarily restrict CUI access.

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 Resources tab for information on LDCs.

On screen:

Access and Dissemination



DoDI 5200.48, March 6, 2020

4.2. DISSEMINATION REQUIREMENTS FOR DOD CUI.

a. In accordance with this issuance, CUI access should be encouraged and permitted to the extent the access or dissemination:

(1) Complies with the law, regulation, or government-wide policy identifying the information as CUI.

(2) Furthers a lawful government purpose.

(3) Is not restricted by an authorized LDC established by the CUI EA.

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

b. Agencies may place limits on disseminating CUI for a lawful government purpose only using the dissemination controls listed in Table 2 or methods authorized by a specific law, regulation, or government-wide policy.

(Image of DoDI 5200.48, paragraph (b.) highlighted)

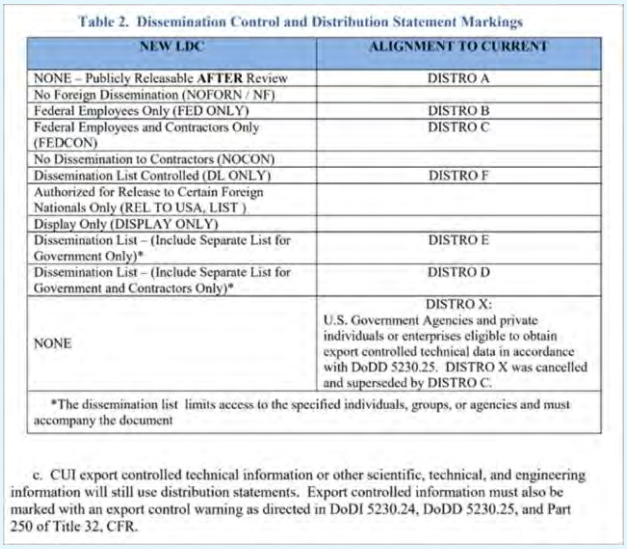


Table 2. Dissemination Control and Distribution Statement Markings

NEW LDC	ALIGNMENT TO CURRENT
NONE – Publicly Releasable **AFTER** Review	DISTRO A
No Foreign Dissemination (NOFORN / NF)	
Federal Employees Only (FED ONLY)	DISTRO B
Federal Employees and Contractors Only (FEDCON)	DISTRO C
No Dissemination to Contractors (NOCON)	
Dissemination List Controlled (DL ONLY)	DISTRO F
Authorized for Release to Certain Foreign Nationals Only (REL TO USA, LIST)	
Display Only (DISPLAY ONLY)	
Dissemination List – (Include Separate List for Government Only)*	DISTRO E
Dissemination List – (Include Separate List for Government and Contractors Only)*	DISTRO D
NONE	DISTRO X: U.S. Government Agencies and private individuals or enterprises eligible to obtain export controlled technical data in accordance with DoDD 5230.25. DISTRO X was cancelled and superseded by DISTRO C.

*The dissemination list limits access to the specified individuals, groups, or agencies and must accompany the document

c. CUI export controlled technical information or other scientific, technical, and engineering information will still use distribution statements. Export controlled information must also be marked with an export control warning as directed in DoDI 5230.24, DoDD 5230.25, and Part 250 of Title 32, CFR.

(Image of DoDI 5200.48, Table 2. Dissemination Control and Distribution Statement Markings)

Example: Raw data, information, or products must be processed and analyzed before determining if further dissemination is required or permitted.

PAGE 10

Audio: Let's try a review question.

On screen:

Knowledge Check

Knowledge Check 2

On screen:

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**

PAGE 11

Audio: 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.

On screen:

Security Incidents

- 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
    - Incidents potentially placing CUI at risk of UD
- For UD of CUI, no formal security inquiry or investigation is required unless disciplinary action will be taken against the individual(s) responsible
- UD of certain CUI, such as export-controlled technical data, may also result in potential civil and criminal sanctions against responsible persons
- 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)
- Notify the appropriate Military Department Counterintelligence (CI) organization of all incidents

PAGE 12

Audio: When will I be required to implement CUI requirements?

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

On screen:

Implementation Schedule

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

PAGE 13

Audio: 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; and
- State the implementation guidelines for CUI.

On screen:

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

PAGE 14

Audio: Now you will be presented with a final exam to test your overall knowledge of the information presented to you in this training course. Click on the "NEXT" button to proceed to the final exam.

On screen:

Coming up next:

Final Exam

(Image of "NEXT" button)

Final Exam

On screen:

1. To begin the Final Exam, click the button below.
2. Questions may be completed in any order. Use the icons on the left to jump to a different question.
3. You may return to previous questions to change your answer.
4. If you need to review course material, a link to jump to that part of the course will be provided.
5. Once all questions are answered, you will be able to proceed to final grading.
6. Failure to achieve a score of 70% or higher after three attempts will require you to restart this course.

(Please note: The Final Exam questions on the training site will appear in random order.)

Final Exam Question 1

On screen:

Who is responsible for applying CUI markings and dissemination instructions?

A. Authorized Common Access Card (CAC) holder

B. Authorized system access administrator

C. Authorized NIPRnet (non-classified Internet Protocol Router (IP) network) system

D. **Authorized holder of the information at the same time of creation**

Reference: CUI Program Overview, Page 5

Final Exam Question 2

On screen:

At the time of creation of CUI material, the authorized holder is responsible for determining:

A. CUI category, CUI labeling, and destruction instructions

B. **CUI category, CUI markings, and dissemination instructions**

C. CUI category, CUI Registry designations, and CUI downgrading instructions

Reference: CUI Program Overview, Page 5

Final Exam Question 3

On screen:

What is the purpose of the ISOO CUI Registry?

A. DoD secure communications between Adjudications, Security Officers, and Component Adjudicators in support of eligibility and access management

B. **A government-wide online repository for Federal-level guidance regarding CUI policy and practice**

C. A government-wide database of privacy information used to identify individuals' Personally Identifiable Information (PII)

D. A DoD online repository for foreign guidance regarding CUI policy and practice

Reference: CUI Program Overview, Page 7

Final Exam Question 4

On screen:

It is mandatory to include a banner marking at the top of the page to alert the user that CUI is present.

A. **True**

B. False

Reference: Marking CUI, Page 2

Final Exam Question 5

On screen:

What is Controlled Unclassified Information (CUI)?

A. Unclassified information requiring classified markings pursuant to good order and discipline

B. **Unclassified information requiring safeguarding and dissemination controls, pursuant to and consistent with applicable laws, regulations, and government-wide policies**

C. Controlled information requiring a subset of markings pursuant to the Director of National Intelligence

D. Information always requiring a Freedom of Information Act (FOIA) element to ensure application of Title 32 Code of Federal Regulations (CFR) Part 3012.56

Reference: Introduction and Course Logistics, Page 5

Final Exam Question 6

On screen:

Administrative, civil, or criminal sanctions may be imposed if there is an Unauthorized Disclosure (UD) of CUI.

A. **True**

B. False

Reference: Handling of CUI, Page 11

Final Exam Question 7

On screen:

What level of system and network configuration is required for CUI?

A. Advanced confidentiality

B. Basic confidentiality

C. **Moderate confidentiality**

D. Enhanced confidentiality

Reference: Handling of CUI, Page 5

Final Exam Question 8

On screen:

CUI documents must be reviewed according to which procedures before destruction?

A. Safeguarding

B. Transmission

C. **Records Management**

D. Marking

Reference: Handling of CUI, Page 7

Final Exam Question 9

On screen:

What is the goal of destroying CUI?

A. Make it unreadable

B. Make it indecipherable

C. Make it unrecoverable

D. **All of the above**

E. None of the above

Reference: Handling of CUI, Page 7

Final Exam Question 10

On screen:

What is CUI Specified?

A. The subset of CUI for which the law, regulation, or government-wide policy does not set out specific handling or dissemination controls

B. The subset of CUI requiring DoD personnel to submit and obtain information for entries into SF 86c

C. The subset of CUI requiring DoD contractors to provide the information needed for the completion of DD Form 254

D. **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**

Reference: Marking CUI, Page 1

Final Exam Question 11

On screen:

What is CUI Basic?

A. The subset of CUI requiring DoD personnel to submit and obtain information for entries into SF 86c

B. The subset of CUI requiring DoD contractors to provide the information needed for the completion of DD Form 254

C. 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

D. **The subset of CUI for which the authorizing law, regulation, or government-wide policy does not set out specific handling or dissemination controls**

Reference: Marking CUI, Page 1

Final Exam Question 12

On screen:

What marking (banner and footer) acronym (at a minimum) is required on a DoD document containing controlled unclassified information?

A. FOUO

B. UNCLASSIFIED

C. **CUI**

D. IAW

Reference: Marking CUI, Page 2

Final Exam Question 13

On screen:

Who can decontrol CUI?

A. OCA, if in a Security Classification Guide

B. Designated office for decontrolling

C. **Both of the above**

Reference: Handling of CUI, Page 1

Final Exam Question 14

On screen:

What DoD Instruction implements the DoD CUI program?

A. DoDI 5205.08, Access to Classified Cryptographic Information

B. **DoDI 5200.48, Controlled Unclassified Information**

C. DoDI 5200.39, Critical Program Information Identification and Protection Within Research, Development, Test, and Evaluation

D. DoDI 5200.01, DoD Information Security Program and Protection of Sensitive Compartmented Information

Reference: CUI Program Overview, Page 3

Final Exam Question 15

On screen:

Who is responsible for protecting CUI?

A. DoD contractors only

B. DoD civilians only

C. **DoD military, civilians, and contractors**

D. DoD military only

Reference: CUI Program Overview, Page 5

Conclusion

Audio: This concludes the DoD Mandatory Controlled Unclassified Information (CUI) Training.

Thank you for participating.

Please wait while your record is updated.

On screen:

Congratulations!

You have completed the Final Exam.

(Check mark displayed on screen.)

Thank you for participating!

Please wait while your record is updated.

To receive credit for this training, please contact your local training coordinator.