

***Controlling Unclassified  
Information (CUI) Life Cycle  
Short #4: Destroying and  
Decontrolling CUI  
Student Guide***

January 2024

*Center for Development of Security Excellence*

## Contents

-Controlling Unclassified Information (CUI) Life Cycle Short #4: Destroying and Decontrolling CUI .....	1
Introduction .....	3
What is CUI?.....	3
Destroying CUI – Overview .....	4
Temporary and Permanent Records.....	4
Temporary Records .....	4
Permanent Record .....	4
Records Management .....	4
Federal Records Act (44 U.S.C. 31) and Corresponding CFRs – Requirements .....	4
Manner of Destroying CUI .....	5
Paper Destruction .....	5
Electronic Destruction.....	5
Clearing .....	5
Purging .....	6
Destroying .....	6
Consolidating CUI Prior to Destruction .....	6
CUI Destruction or Disposal Bins.....	6
Learning Activity – 1.....	6
Learning Activity – 2.....	6
Learning Activity – 3.....	7
Decontrolling CUI – Overview .....	7
When to Decontrol CUI .....	7
Who Can Decontrol CUI .....	7
Conditions Under Which Decontrol Can Occur.....	8
Learning Activity – 4.....	8
Decontrolling Actions.....	8
Notifications .....	9
Learning Activity – 5.....	9
Public Release Considerations .....	9
Conclusion.....	9
Appendix A: Answer Key .....	1

Learning Activity – 1 ..... 1

Learning Activity – 2 ..... 1

Learning Activity – 3 ..... 1

Learning Activity – 4 ..... 1

Learning Activity – 5 ..... 2

## Introduction

Welcome to the CUI Life Cycle Short #4: Destroying and Decontrolling CUI. This Short will focus on the Decontrol and Destroy steps of the Controlled Unclassified Information (CUI) life cycle. CUI must be protected throughout each step of its life cycle. When CUI no longer requires safeguarding or dissemination controls, the CUI is decontrolled, and when CUI is no longer needed, there are policies in place to determine when and how to destroy it.

At the conclusion of this Short, you will be able to apply the policy requirements outlined in Department of Defense Instruction 5200.48, Controlled Unclassified Information (DODI 5200.48) to decontrol and destroy CUI materials. This Short will also guide you in the creation of a CUI Decontrol and Destroy Workplace Reference document. The template for this guide is located in the [Course Resources](#). You will complete this resource as you proceed through this Short. Once complete, this reference will provide a quick “how-to” guide specific to your agency or workplace.

### Course Objective

- Apply the policy requirements outlined in DODI 5200.48 to decontrol and destroy CUI materials.

### Course Details

- Estimated completion time: 20 minutes
- POC: [dcsa.cdsetraining@mail.mil](mailto:dcsa.cdsetraining@mail.mil)

## What is CUI?

So, what is CUI?

CUI is a standardized safeguarding system for the protection of Unclassified information that allows for, or requires, safeguarding and dissemination controls in accordance with applicable laws, regulations, and government-wide policies.

An authorized holder of CUI is a person or entity that handles CUI, has completed the required CUI training, and is authorized to designate or handle CUI in accordance with regulatory guidance. DOD personnel at all levels are responsible for receiving, handling, creating, safeguarding, disseminating, decontrolling, when applicable, and destroying CUI.

To learn about the previous steps in the CUI life cycle refer to:

- Short #1: Create/Identify and Designate CUI
- Short #2: Safeguarding Part 1 – Marking CUI
- Short #3: Safeguarding Part 2 and Sharing CUI

This Short will start by reviewing the requirements for destroying CUI followed by the requirements for decontrolling it.

## Destroying CUI – Overview

Only authorized holders can destroy CUI. As an authorized holder of CUI, you should destroy it when you no longer need the information. It should also be destroyed when records disposition schedules published by the National Archives and Records Administration (NARA) allow for it to be destroyed.

The NARA Records Schedule provides mandatory instructions (“disposition instructions”) to all NARA staff regarding how to maintain the agency’s operational records and what to do with them when they are no longer needed for current business.

## Temporary and Permanent Records

Before you can determine whether and how to destroy CUI, it must be identified as a temporary or a permanent records. Individual agencies or departments determine if records have sufficient value to warrant permanent retention. CUI temporary records are retained for a specified period of time, then they are destroyed at the local level while permanent records become part of the National Archives.

Refer to the [Course Resources](#) for more information on Temporary and Permanent Records.

### ***Temporary Records***

Temporary records generally include housekeeping records and administrative files common to most agencies and are not records relating to an activity’s primary function. Examples of temporary records include budget, fiscal, personnel, and supply records and files. Temporary records may also include CUI documents shared during a meeting or a class. Once the meeting or class is over, and the CUI documents are no longer needed, they should be destroyed.

### ***Permanent Record***

Permanent records are designated for retention because they have enduring or lasting value. Permanent records document organizational functions, or contain significant information on personnel, assets, or activity specific issues or conditions. Specifically, permanent records typically reveal information such as agency briefing materials, analytical research, studies, and reports.

## Records Management

If the agency no longer needs the information, and NARA allows for CUI to be destroyed, you must process it through the Records Management Procedures before destroying it. This is required by the Federal Records Act, 44 U.S.C. 31, and corresponding Code of Federal Regulations (CFRs) implemented by DODI 5015.02, Department of Defense Records Management Program.

### ***Federal Records Act (44 U.S.C. 31) and Corresponding CFRs – Requirements***

Record and non-record copies of CUI documents should be disposed of in accordance with Chapter 33 of Title 44, U.S.C. and the DOD Components’ records management directives which require agencies to maintain records documenting their activities, file records for safe storage and efficient retrieval, and dispose of records according to agency schedules. Adhering to standard policies and procedures helps ensure a compliant records management system is maintained.

Keep in mind, this applies to all records and media types, as well as email and text messages. Your organization may have additional policies and procedures in place for records retention, active files, unused files, emails, texts, and several other areas of information management. Consult your CUI Component Program Manager (CUI CPM) to determine if your organization requires you to implement any additional CUI-specific Records Management Procedures.

## Manner of Destroying CUI

Once you have processed CUI through the Records Management Procedures, it can be destroyed. There are two types of CUI media that may need to be destroyed: physical or hard copy media such as paper and electronic media, and soft media such as hard drives, flash drives, USB drives, DVDs, and other kinds of memory drives.

When destroying physical or electronic CUI, it is required that you do so in a manner that leaves it unreadable, indecipherable, and irrecoverable. Approved destruction methods are outlined in the laws, regulations, and Government-wide policies governing CUI, such as DODI 5200.48, 32 CFR Part 2002 Controlled Unclassified Information, and Information Security Oversight Office, or ISOO CUI Notice 2019-03, Destroying Controlled Unclassified Information (CUI) in paper form. Note that any method approved for destroying Classified National Security Information is sufficient to destroy CUI.

## Paper Destruction

There are two common options for destroying paper: the single-step method and the multi-step method. For the single-step paper destruction method, agencies must use cross-cut shredders that produce 0.04 inch x 0.2 inch particles, or smaller; or pulverize or disintegrate paper using disintegrator devices equipped with a 3/32 inch security screen. When possible, equipment approved for destroying CUI should be clearly marked.

With a multi-step paper destruction process, an agency shreds CUI to a lesser standard and then destroys it using an additional destruction method. It is a permitted alternative once your organization has verified and found this method satisfactory.

For more information, refer to the National Institute of Standards and Technology Special Publications, or NIST SP 800 Revision 1, Guidelines for Media Sanitization, Table A-1: Hard Copy Storage Sanitization.

## Electronic Destruction

When destroying CUI stored electronically and on soft media, the authority governing the CUI may specify a required destruction method. If it does not, agencies must use one of the methods identified by the DOD CUI Program and NIST SP 800-88 Revision 1, Guidelines for Media Sanitization. These guidelines outline three suggested practices for electronic destruction clearing, purging, and destroying.

### ***Clearing***

Clearing is one method used to sanitize media which works by “clearing” data through standard read and write commands. This process includes overwriting not only the logical storage location of files, but also should include all user-addressable locations. Clearing to sanitize media is typically only recommended for use on magnetic media such as older hard drives. Before relying on clearing to

sanitize media, reference NIST SP 800-88 Rev. 1, Guidelines for Media Sanitization, Table 5-1: Sanitization Methods, or consult your CUI CPM for guidance.

### ***Purging***

Purging uses laboratory techniques that make CUI data impossible to retrieve.

### ***Destroying***

Destroying, like purging, uses laboratory techniques that make CUI data impossible to retrieve. However, it also destroys the media so it can never be used for storage again.

## **Consolidating CUI Prior to Destruction**

Physical security standards for CUI must be adhered to until the information is destroyed in accordance with the standards of the DOD CUI Program. Agencies can use their discretion to determine which safeguarding controls are necessary to meet requirements while CUI materials await destruction.

For example, agencies may consolidate CUI before destroying it via an approved method. Common ways to consolidate CUI include shred bins and burn bags in a controlled environment and interim storage or contractor facilities. If agencies consolidate CUI materials they must protect them in a controlled environment that prevents unauthorized access. This also applies when consolidated CUI is collected and stored at interim storage facilities, or by contractors. Procedures must be put in place to account for consolidated CUI until it is destroyed in accordance with standards of the DOD CUI Program.

### ***CUI Destruction or Disposal Bins***

Mark bins approved for the disposal of CUI and ensure they cannot be tampered with. They must remain locked. In addition, never use a regular trash can or recycle bin to collect or dispose of CUI. Now that you have learned how to destroy CUI, take a moment to access the Workplace Reference document in the [Course Resources](#) and complete the CUI Component Program Manager and the Destroying CUI sections.

## **Learning Activity – 1**

Let's try a scenario. You led a meeting this morning and shared copies of CUI documents. These documents are considered temporary. Are you required to retain and continue to protect the extra documents after the meeting?

*Select yes or no. Check your answer in the Answer Key at the end of this Student Guide.*

- Yes
- No

## **Learning Activity – 2**

Now that your meeting is over, what should you do with the extra CUI documents?

*Select the best response. Check your answer in the Answer Key at the end of this Student Guide.*

- Manually rip the documents so they are difficult to reassemble.

- Use a cross-cut shredder that produces 0.04 in x 0.2 in particles.
- Throw them away in a recycle bin that will eventually be shredded.
- Put them in your file cabinet so you can easily access them for future meetings this week.

### Learning Activity – 3

You have a flash drive containing numerous CUI documents that you need to destroy. The CUI authority did not specify a destruction method. What destruction method can you use?

*Select the best response. Check your answer in the Answer Key at the end of this Student Guide.*

- Clear data by rewriting the flash drive.
- Since no destruction method is specified, dispose of the flash drive by throwing it in the trash bin.
- Use laboratory techniques that make CUI data impossible to retrieve; then completely destroy flash drive so it cannot be used again.
- Delete the files using the delete button.

### Decontrolling CUI – Overview

Now that you are familiar with properly disposing CUI, let's take a look at decontrolling it. Decontrolling means removing any controls designed to safeguard or limit the dissemination of the information. CUI must be decontrolled when the information no longer needs safeguarding. Not all CUI can be decontrolled. Before decontrolling, check with applicable laws and regulations.

### When to Decontrol CUI

So when should CUI be decontrolled? According to DODI 5230.09, Clearance of DOD Information for Public Release, CUI owners must promptly decontrol CUI once they determine the information no longer requires protection or safeguarding from public disclosure. Owners should first ensure that decontrolling it does not conflict with another law, regulation, or government-wide policy.

There are no specific timelines for decontrolling CUI unless specifically required in a law, regulation, or government-wide policy. Unlike classified national security information (CNSI), which is assigned a declassification date when originally classified, CUI is not assigned a set decontrol date and it should be decontrolled as soon as possible.

All CUI decontrol actions must also align with DOD records management requirements per DODI 5015.02 and DODI 5200.48. This includes the requirement to formally review the information before decontrolling it or releasing it to the public.

### Who Can Decontrol CUI

Who can decontrol and release CUI records? In accordance with DODI 5200.48, three parties can decontrol CUI: the originator or creator of the information, the Original Classification Authority if the CUI is identified in a Security Classification Guide, designated offices for decontrolling, or another authorized organization or individual can decontrol the CUI. For a contractor or nonfederal stakeholder to decontrol CUI, decontrol provisions would have to be outlined in the contract or agreement.



## Conditions Under Which Decontrol Can Occur

Now let's look at the specific conditions which prompt decontrolling CUI in accordance with Chapter 20 of Title 32 Part 2002. In some situations, the authorized holder automatically decontrols CUI according to relevant agency policies and procedures. Automatic decontrol can occur when specified by a law, regulation, or government-wide policy. When the designating agency decides to release the information to the public, they can then automatically decontrol the CUI. Additionally, when disclosure is in accordance with an applicable information statute such as the Freedom of Information Act or the Privacy Act automatic, decontrol would also be prompted.

In contrast, designating agencies may act to decontrol CUI through proactive action. For example, they may decontrol CUI in response to a request by an authorized holder to decontrol it. Or they may decontrol it when the CUI no longer requires safeguarding or dissemination controls unless explicitly prohibited by law, regulation, or government-wide policy.

Lastly, they may decontrol it concurrently with any declassification action under Executive Order 13526 or any predecessor or successor order. These orders may cause agencies to decontrol any associated CUI or comingled CUI, but only if that CUI no longer requires controls under laws, regulations or government-wide policies.

### Learning Activity – 4

You are currently holding an analysis report, and this report contains CUI. Which of the following conditions would prompt the decontrol of this CUI document?

*Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.*

- The CUI document has been processed through the Records Management Procedures.
- Laws, regulations/government-wide policies indicate the document can be decontrolled.
- The analysis report was released to the public without a prepublication review.
- A designating agency decides to release the information to the public.

### Decontrolling Actions

After a decontrol decision is made, no immediate marking action is required. However, there are a few conditions that would prompt the need for you to remove or strike through markings on decontrolled CUI. If CUI is reused, restated, or paraphrased in a newly created document this would require you to redact or strike through the CUI markings.

When CUI in your possession is publicly released through an official agency policy or procedure, you would need to redact or strike through the CUI markings. Likewise, if CUI you are holding has been donated to a private institution this would also require you to remark or strike through the CUI markings. In these situations, the CUI materials should have the CUI banner and footer markings lined through and replaced with "DECONTROLLED." You should do this on the first page, the cover page, and the first page of any attachment.

Additionally, the CUI Designation Indicator, or DI Block should have a diagonal line at a 45-degree angle drawn through it. The person decontrolling the information should be sure to record the date of decontrol and their name next to the crossed out DI Block.

## Notifications

When CUI is decontrolled, all known holders should be notified by email or other means. As already noted, authorized holders do not need to immediately retrieve records on file solely to remark or strike through CUI markings after being notified of decontrol. However, they do need to be aware of the circumstances discussed that do require prompt removing or striking through of CUI markings.

## Learning Activity – 5

You are the originator of a CUI document. A regulation change prompted the automatic decontrol of CUI according to agency policies and procedures. Which markings should you strike through on the CUI document?

*Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.*

- Draw a line through the CUI banner and footer markings and replace it with the word “DECONTROLLED.”
- Draw a diagonal line (45-degree angle) through the CUI DI Block with the name of the person and date of decontrol
- Draw a line through the CUI DI Block and write “DECONTROLLED” across the top of the document.
- Draw a vertical line (90-degree angle) through the CUI DI Block and write “DECONTROLLED.”

## Public Release Considerations

Remember, decontrol does not equal public release. Decontrolling CUI relieves authorized holders from handling the information in accordance with the DOD CUI Program, but it does not authorize the information for public release. Agencies should have specific processes in place to ensure procedures for public release of CUI are adhered to.

Public release requires pre-publication of the content in accordance with DODI 5230.09, Clearance of DOD Information for Public Release. CUI must be decontrolled and publicly released in accordance with applicable laws and policies. Once CUI is properly processed for public release according to specific agency policy, that CUI is automatically decontrolled across agencies and organizations. A crucial point to remember here is when information is decontrolled this does not equate to authorization for public release – it must go through mandatory pre-publication review!

Now that you have learned how to decontrol CUI, take a moment to access the Workplace Reference document in **Error! Reference source not found.** and complete the Decontrolling CUI section.

## Conclusion

Congratulations on completing the CUI Life Cycle Short #4: Destroying and Decontrolling CUI. You should now be able to apply the policy requirements outlined in DODI 5200.48 to decontrol and destroy CUI

materials. In addition, you should now have a completed Workplace Reference document customized for your workplace.

## Appendix A: Answer Key

### Learning Activity – 1

You led a meeting this morning and shared copies of CUI documents. These documents are considered temporary. Are you required to retain and continue to protect the extra documents after the meeting?

- Yes
- No (correct response)

**Feedback:** Since these CUI documents are temporary, you do not need to retain them after the meeting. They can be destroyed.

### Learning Activity – 2

Now that your meeting is over, what should you do with the extra CUI documents?

- Manually rip the documents so they are difficult to reassemble.
- Use a cross-cut shredder that produces 0.04 in x 0.2 in particles. (correct response)
- Throw them away in a recycle bin that will eventually be shredded.
- Put them in your file cabinet so you can easily access them for future meetings this week.

**Feedback:** When destroying CUI, it must be unreadable, indecipherable, and irrecoverable. Using a cross-cut shredder that produces 0.04 in x 0.2 in particles will accomplish this.

### Learning Activity – 3

You have a flash drive containing numerous CUI documents that you need to destroy. The CUI authority did not specify a destruction method. What destruction method can you use?

- Clear data by rewriting the flash drive.
- Since no destruction method is specified, dispose of the flash drive by throwing it in the trash bin.
- Use laboratory techniques that make CUI data impossible to retrieve; then completely destroy flash drive so it cannot be used again. (correct response)
- Delete the files using the delete button.

**Feedback:** You can clear data by using laboratory techniques that make CUI data impossible to retrieve, and then completely destroying the flash drive so it cannot be used again.

### Learning Activity – 4

You are currently holding an analysis report, and this report contains CUI. Which of the following conditions would prompt the decontrol of this CUI document?

- The CUI document has been processed through the Records Management Procedures.

- Laws, regulations/government-wide policies indicate document can be decontrolled. (correct response)
- The analysis report was released to the public without a pre-publication review.
- A designating agency decides to release the information to the public. (correct response)

**Feedback:** *The following are conditions under which CUI documents may be decontrolled: Laws, regulations/government-wide policies indicate document can be decontrolled and a designating agency decides to release the information to the public. Unauthorized disclosure does not constitute a proper method of decontrol.*

### **Learning Activity – 5**

You are the originator of a CUI document. A regulation change prompted the automatic decontrol of CUI according to agency policies and procedures. Which markings should you strike through on the CUI document.

- Draw a line through the CUI banner and footer markings and replace it with the word “DECONTROLLED.” (correct response)
- Draw a diagonal line (45-degree angle) through the CUI DI Block with the name of the person and date of the decontrol. (correct response)
- Draw a line through the CUI DI Block and write “DECONTROLLED” across the top of the document.
- Draw a vertical line (90-degree angle) through the CUI DI Block and write “DECONTROLLED.”

**Feedback:** *You will draw a line through the CUI banner and footer markings and replace it with the word “DECONTROLLED.” In addition, you will draw a diagonal line (45-degree angle) through the CUI DI Block with the name of the person and date of decontrol.*