Controlled Unclassified Information (CUI) Life Cycle Short #1: Create/Identify and Designate CUI

Student Guide

March 2024

Center for Development of Security Excellence

Contents

Introduction

As you know, in order to protect our national security, classified information must be handled with care, but a great deal of Unclassified information also requires safeguarding and dissemination controls. A variety of laws, regulations, and government-wide policies require the careful handling of several specific types of unclassified information – for example, personally identifiable information, or PII, export-controlled information, or law enforcement information, to name just a few.

Collectively, this information is referred to as Controlled Unclassified Information (CUI). DOD personnel at all levels may be responsible for receiving, handling, creating, safeguarding, disseminating, decontrolling, and destroying CUI. Therefore, let's take a few moments to look at how this all begins.

This short will focus on the first step of the CUI life cycle: Create, Identify and Designate CUI.

When you have completed this short, you should be able to apply the policy requirements outlined in Department of Defense Instruction, or DODI 5200.48, Controlled Unclassified Information, when it's time to create, identify and designate CUI.

This short will also guide you in creating the CUI Step 1 Workplace Reference, a quick "how-to" guide specific to your agency or workplace. The template for this guide is located in your Course Resources.

Course Objective

- Apply the policy requirements outlined in DODI 5200.48, Controlled Unclassified Information, to Create/Identify and Designate CUI.

Course Details

- Estimated completion time: 25 minutes
- POC: dcsa.cdsetraining@mail.mil

The CUI Life Cycle

The CUI program standardizes the protection of controlled unclassified information throughout its life cycle.

The CUI life cycle begins by creating or identifying the information and then designating it as a specific CUI category. Once information is designated as CUI, it must be safeguarded, which requires proper marking, handling, and storing. If this information is shared, the sharing must meet specific CUI requirements for dissemination, transmission, and transportation. Finally, decontrolling and destroying CUI must also align with policy requirements.

In this first step of the CUI life cycle, you must determine whether the information you are handling is, in fact, considered CUI. This includes creating and designating new information, as well as identifying whether legacy CUI – that is, information that was formerly marked as For Official Use Only (FOUO); Sensitive But Unclassified (SBU); or one of the other legacy markings – can still be designated as CUI in accordance with DODI 5200.48. As part of this step, once you designate information as CUI, you must also determine the appropriate CUI category in accordance with the DOD CUI Registry.

CUI Background and History

As you just learned, the national CUI program arose to standardize the variety of laws, regulations, and government-wide policies used to manage unclassified information requiring safeguarding or dissemination controls.

So, how did we get here? Let's review a quick history of CUI.

In 2010, national policy was issued through Executive Order, or E.O. 13556. This executive order established a uniform program for managing CUI across the federal government, replacing a variety of agency-specific policies, markings, and procedures that led to inconsistent marking, safeguarding, and sharing of CUI. This executive order also designated the National Archives and Records Administration (NARA) to serve as the Executive Agent (EA) to implement and oversee all federal agency actions to ensure they comply with E.O. 13556. NARA created the CUI Office and appointed the Director of the Information Security Oversight Office (ISOO) to serve as Director of the CUI office to fulfill these responsibilities.

In February 2012, what is now the Under Secretary of Defense for Intelligence and Security (USD(I&S)) released DOD Manual, or DODM, 5200.01, Information Security Program Volume 4, Controlled Unclassified Information. This was the DOD's first effort to align with the national CUI policy issued by E.O. 13556. DODM, 5200.01, Volume 4 identified the DOD CUI controls and markings now known as legacy markings. These include the markings mentioned earlier like FOUO and SBU, among others.

In November 2016 ISOO, as the executive agent for CUI, issued Title 32 of the Code of Federal Regulations, or CFR, Part 2002: Controlled Unclassified Information. This established standards for effectively implementing E.O. 13556 and is known as the implementing directive or Final Rule for CUI.

In response to the implementing directive, in March 2020, USD(I&S) published DODI 5200.48, Controlled Unclassified Information. This Instruction cancelled DODM 5200.01 Volume 4 and established the current DOD CUI Program. The DODI 5200.48 outlines the minimum requirements for CUI.

Your organization may implement additional CUI procedures that you must adhere to, so be sure to check with your security manager or DOD CUI Component Program Manager (CPM).

Take a moment to review the CUI Step 1 Workplace Reference and complete the first section, including your DOD CUI CPM's contact information and any additional guidance issued by your DOD CUI CPM.

CUI Indexes and Categories

Remember that in order to be considered CUI, information must require protection according to a law, Federal regulation, or government-wide policy, also known as an "authority." These authorities, and their respective information types, are cataloged and organized in the National CUI Registry.

As the CUI Program EA, the ISOO maintains the National CUI Registry. The DOD CUI Registry generally mirrors the national registry; however, it provides DOD personnel with specific information unique to the Department of Defense.

To identify the appropriate authority or authorities – and note that there can be more than one – DOD CUI is grouped into organizational indexes such as defense, privacy, and proprietary, among others.

Each of these indexes is then broken out into a list of associated categories. For example, there are several categories included under the Privacy Index such as Contract Use, Death Records, General Privacy, Health Information, and Personnel Records, to name a few.

By selecting a category, you can find the National and DOD authority or authorities that require the information to be protected as CUI. For example, the protection of General Privacy information as CUI is required by both National and DOD Authorities.

Visit the DOD CUI Registry to explore the indexes and categories in more detail. A link is available in the Course Resources.

What is NOT CUI?

So how do you know whether the information you have is CUI? The first step in identifying or creating CUI is understanding what CUI is *not*.

CUI is *not* classified information. If the information you have meets standards for classification in accordance with DODM 5200.01, Volume 1: DOD Information Security Program, then it is not CUI and you should proceed to the guidance for classified information. Note that because CUI is not classified information, you should never describe it as "classified as CUI." Instead, refer to it as "designated as CUI."

CUI is also not corporate intellectual property, unless that intellectual property was created for or required by government contract, nor is it information that was not created by, for, or under the control of the U.S. Government.

Identify CUI – Scenario

Consider this scenario. Imagine that you are writing an email containing detailed information about counterinsurgency that you obtained from a publicly available academic journal: Journal of Global Security Studies. Is this information CUI?

Is information from a publicly available academic journal article considered CUI?

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

- ○ Yes
- ○ No

What IS CUI?

Once you have excluded information that is *not* CUI, the next step is determining what *is*.

Remember that in order to be considered CUI, the information must fall under the guidance of a law, regulation, or Government-wide policy – one of the "authorities" specified in the DOD CUI or ISOO registries. If the information is not covered by an authority, then it is not CUI, but if it *is* covered then it *is* CUI and must be safeguarded as such.

Create CUI – Scenario

For example, imagine that you are a human resources manager for a DOD agency, reviewing records for a newly created program.

These records contain employee information, including an employee's date of birth and social security number, as well as documents being processed for enrolment in specific health plans. Is this CUI?

You will need to visit the DOD CUI Registry to investigate.

Employee Record:
Jonathan Green
7/27/87
123-45-6789
BCBS Health Plan

Is the information in this record considered CUI?

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

- ○ Yes
- ○ No

DOD CUI Registry

The main DOD CUI Registry screen lists several organizational indexes. Under the Privacy index, observe that Personnel Records is one of the categories. The relevant National and DOD authorities are listed under Personnel Records.

Identify Legacy CUI

Remember, you should use the DOD CUI Registry to determine whether the information you create is CUI.

Reference the CUI Registry to determine whether information with legacy markings is considered CUI. Legacy markings such as FOUO or SBU – among others – must be replaced with the marking CUI in accordance with DODI 5200.48. For example, the marking U//FOUO is no longer an authorized portion or banner marking, but may still be seen on legacy documents that are shared or used within DOD.

Remember, not all legacy information automatically qualifies as CUI! As with any other information, only those information types and categories with a clear authority may be marked as CUI.

So, when should you assess legacy information for CUI?

As long as legacy information remains under DOD control and use, it does not need to be re-marked. However, if that information is shared outside the DOD then it needs to be assessed to determine if it meets criteria for CUI and, if it does, marked accordingly.

If a new document is created with information derived from legacy material, it must also be assessed and marked CUI, assuming it still qualifies.

Take a moment to review the CUI Step 1 Workplace Reference and complete the section on legacy CUI used by your organization.

Legacy vs. CUI

This table contains a summary of the changes from Legacy to CUI Policy.

Legacy Policy	CUI Policy
Unique marking systems, reasoning, and coversheets	An executive branch-wide policy
A system based on Freedom of Information Act (FOIA) exemptions	A system based on laws, regulations, and Government-wide policies
A system with no requirement to mark the underlying FOIA category or information originator	A system with specific documentation requirements
Undefined secure communication requirements	Standardized secure communication requirements

Identify Legacy CUI – Scenario

Now, imagine you're working on updating some documents to better reflect organizational procedures and you come across a Continuity of Operation Planning (COOP) briefing that highlights key changes to include in your emergency plans. The briefing was previously marked FOUO. Does it still meet the criteria to be considered CUI?

You will need to visit the DOD CUI Registry to investigate.

When you're ready, make your determination.

Is the information in this document considered CUI?

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

- ○ Yes
- ○ No

DOD CUI Registry

Again, go to the DOD CUI Registry. Under the Critical Infrastructure index, and the Emergency Management category, Continuity of Operations, or COOP, is one of the examples.

The registry also shows applicable National and DOD authorities.

Designate CUI

Once you know that your information is CUI, the next step is to determine which CUI Registry category or categories apply, and then annotate that category in the CUI Designation Indicator (DI) block.

The DI block is a marking that must appear on all CUI. It contains the following information:

- Controlled by
- CUI Category
- Limited Dissemination Control (LDC)
- Point of Contact (POC)

The DI block is similar to the Classification Authority Block (CAB) that appears on the face of all classified documents.

If you think you have CUI, but there is no corresponding category in the registry, there is a CUI request form on the DOD CUI Program Page.

Take a moment to review the CUI Step 1 Workplace Reference and add the categories and CUI abbreviations that you typically work with.

Designate CUI – Scenario

Remember the employee information that you handled earlier? You determined that this information was CUI. Now, what category or categories should you include in the DI block?

You will need to visit the DOD CUI Registry to make this determination.

When you're ready, make your determination.

Employee Record:
Jonathan Green
7/27/87
123-45-6789
BCBS Health Plan

What category(ies) should you include in the DI block?

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

- ☐ PERS
- ☐ PRVCY
- ☐ NUC
- ☐ AIV

DOD CUI Registry

The category abbreviation that you should include in the DI block is available on each registry category screen.

Limited Dissemination Controls (LDCs)

CUI should only be disseminated for a lawful government purpose, but in some cases, additional limits may be placed on the dissemination of specific CUI categories. When CUI requires dissemination or

access controls in accordance with DODI 5200.48, a Limited Dissemination Control (LDC) must be included in the designation indicator block. LDCs can be used to limit the audience that may lawfully access the CUI but must not be used to restrict access unnecessarily.

The list of approved CUI LDC's is available on the DOD CUI Program Page. Keep in mind LDCs should not be implemented unless they are authorized and required by a specific law, regulation, or government-wide policy. Additionally, LDCs should only be applied when the agency designating the information as CUI approves. Remember, not all CUI includes LDCs. When LDCs are absent, anyone with a lawful government purpose may access the information.

One category of CUI – Controlled Technical Information, or CTI – is also authorized to use distribution, or DISTRO, Statements. This is the only category of CUI that uses DISTRO statements, as authorized by the Defense Federal Acquisition Regulation Supplement, or DFARS. If you handle this type of information, reference DODI 5230.24, Distribution Statements on DOD Technical Information, for specific guidance.

Take a moment to review the CUI Step 1 Workplace Reference and complete the section on dissemination controls.

Warning Statements

The DOD CUI Registry also lists warning statements when applicable for specific categories of CUI. For example, Export Controlled information must be marked with a warning statement, per DODD 5230.25, Withholding of Unclassified Technical Data From Public Disclosure.

Note that when CUI is comingled with classified information a warning statement must be included on the first page to alert readers that CUI is present in a classified DOD document.

LDCs – Scenario 1

Consider again the personnel record you created earlier. According to the registry, do you need to apply any LDCs or Warning Statements?

You may need to visit the DOD CUI Registry to make this determination.

Keep in mind that, as the owner of the CUI, your organization may require additional controls beyond the registry requirements.

Employee Record:
Jonathan Green
7/27/87
123-45-6789
BCBS Health Plan

Are LDCs or Warning Statements required for this information per the DOD CUI Registry?

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

- ○ Yes, an LDC is required.
- ○ Yes, a Warning Statement may be required.

- ○ No LDCs or Warning Statements are required.

DOD CUI Registry

Remember that the list of approved LDCs is available on the DOD CUI Registry. It is also available in the course resources. You may also want to check the applicable category screens for required Warning Statements.

LDCs – Scenario 2

Next, you notice that some of the information you are reviewing is associated with naval nuclear propulsion plants and the control of radiation.

Are LDCs or Warning Statements required for this information?

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

- ○ Yes, an LDC is required.
- ○ Yes, a Warning Statement may be required.
- ○ No LDCs or Warning Statements are required.

DOD CUI Registry

Recall that if LDCs or Warning Statements are required, it will be stated in the CUI Registry.

CUI Control Levels

On the National ISOO CUI Registry, you may see a reference to two control levels for CUI: CUI Basic and CUI Specified that align with different CUI categories.

During the initial implementation of DOD's CUI program, all DOD information will be safeguarded in accordance with CUI Basic, as outlined in DODI 5200.48. Therefore, these controls will not initially be aligned with categories in the DOD CUI Registry. The DOD will outline specific distinctions and requirements for these two control levels in forthcoming guidance.

Consult your DOD CUI CPM for any additional guidance or agency-specific requirements regarding use of CUI controls within your agency. Components or organizations may have additional requirements.

For additional guidance on creating the DI block and LDC markings, reference CUI Short #2 Marking.

For additional guidance on implementing LDCs and other controls reference the CUI #3 Short Safeguarding Part 2 and Handling.

Conclusion

Congratulations on completing the first CUI Life Cycle Short: Create/Identify and Designate CUI.

In this Short you learned how to use the DOD CUI Registry to determine whether the information you have qualifies as CUI and, if so, designate the appropriate CUI category. You also learned how to

determine if other necessary controls, such as LDCs or warning statements, apply to specific CUI category designations.

You should now be able to apply the policy requirements outlined in DODI 5200.48 to Create/Identify and Designate CUI. You should also now have a completed Workplace Reference document customized for your workplace.

Course Objective

- Apply the policy requirements outlined in DODI 5200.48 to Create/Identify and Designate CUI.

Appendix A: Answer Key

Identify CUI – Scenario

Imagine that you are writing an email containing detailed information about counterinsurgency that you obtained from a publicly available academic journal: Journal of Global Security Studies. Is this information CUI?

Is information from a publicly available academic journal article considered CUI?

- ○ Yes
- ◉ No

***Feedback**: This information was not created by, nor is it under the control of, the U.S. Government. It is not CUI.*

Create CUI – Scenario

Imagine that you are a human resources manager for a DOD agency, reviewing records for a newly created program.

These records contain employee information, including an employee's date of birth and social security number, as well as documents being processed for enrolment in specific health plans. Is this CUI?

Employee Record:
Jonathan Green
7/27/87
123-45-6789
BCBS Health Plan

Is the information in this record considered CUI?

- ◉ Yes
- ○ No

***Feedback**: Personnel Records and General Privacy are all considered CUI. Visit the DOD CUI Registry to note the relevant authorities for each category.*

Identify Legacy CUI – Scenario

Imagine you're working on updating some documents to better reflect organizational procedures and you come across a Continuity of Operation Planning (COOP) briefing that highlights key changes to include in your emergency plans. The briefing was previously marked FOUO. Does it still meet the criteria to be considered CUI?

Is the information in this document considered CUI?

- ◉ Yes
- ○ No

***Feedback**: Continuity of Operations Plans, or COOP, fall under Emergency Management. They are covered by DOD and Federal authorities and therefore meet the criteria for CUI.*

Remember, if you are not disseminating this information outside the DOD or creating a new document then you do not need to update the markings.

Designate CUI – Scenario

Remember the employee information that you handled earlier? You determined that this information was CUI. Now, what category or categories should you include in the DI block?

Employee Record:
Jonathan Green
7/27/87
123-45-6789
BCBS Health Plan

What category(ies) should you include in the DI block?

- ☑ PERS
- ☑ PRVCY
- ☐ NUC
- ☐ AIV

***Feedback**: The Category Abbreviation for Personnel Records is PERS. Because the record includes the employee's social security number, full name, and birthdate, it also needs the category PRVCY, according to authorities.*

LDCs – Scenario 1

Consider again the personnel record you created earlier. According to the registry, do you need to apply any LDCs or Warning Statements?

Keep in mind that, as the owner of the CUI, your organization may require additional controls beyond the registry requirements.

Employee Record:
Jonathan Green
7/27/87
123-45-6789
BCBS Health Plan

Are LDCs or Warning Statements required for this information per the DOD CUI Registry?

- ○ Yes, an LDC is required.
- ⦿ Yes, a Warning Statement may be required.
- ○ No LDCs or Warning Statements are required.

***Feedback**: In accordance with the DOD CUI Registry, the category General Privacy may require a Privacy Act Statement (PRVCY). Check with your Security Manager or CUI CPM for guidance.*

LDCs – Scenario 2

Next, you notice that some of the information you are reviewing is associated with naval nuclear propulsion plants and the control of radiation.

Are LDCs or Warning Statements required for this information?

- ⦿ Yes, an LDC is required.
- ○ Yes, a Warning Statement may be required.
- ○ No LDCs or Warning Statements are required.

***Feedback**: The LDC: NOFORN must be included in the DI block for naval nuclear testing information*.