Controlled Unclassified Information (CUI) Life Cycle Short #3: Safeguarding Part 2 & Sharing

Student Guide

January 2024

Center for Development of Security Excellence

Contents

Introduction

Welcome to the CUI Life Cycle Short #3: Safeguarding Part 2 & Sharing Short. This Short will focus on the Safeguard and Share steps of the Controlled Unclassified Information (CUI) Life Cycle. Safeguarding includes marking, handling, and storing CUI.

The Short "Safeguarding Part 1: Marking CUI" reviewed marking requirements. Markings are a critical component of CUI safeguarding, since they ensure that CUI is immediately recognized, and handled and stored appropriately.

In this Short, we will focus on the handling and storage requirements of CUI. In addition, we will review the requirements for Sharing CUI, which includes disseminating, transmitting, and transporting. At the conclusion of this Short, you will be able to apply the policy requirements outlined in DODI 5200.48: Controlled Unclassified Information to safeguard CUI by properly handling, storing, and sharing it.

This short will also guide you in the creation of a CUI 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 Controlled Unclassified Information (CUI) to safeguard CUI by properly handling, storing, and sharing CUI materials.

Course Details

- Estimated completion time: 20 minutes
- POC: dcsa.cdsetraining@mail.mil

What is CUI?

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

DOD personnel at all levels are responsible for receiving, handling, creating, safeguarding, disseminating, decontrolling when applicable, and destroying CUI.

Refer to Short #1 Create/Identify and Designate CUI and Short #2 Safeguarding Part 1 – Marking CUI to learn more about the previous steps in the CUI life cycle.

Safeguarding: Overview

Let's start with Safeguarding.

The CUI program national policy was initially established in 2010 with Executive Order 13556, Controlled Unclassified Information. It was established to standardize the variety of agency-specific policies, procedures, and markings that were previously used to protect Controlled Unclassified Information.

The DOD currently requires safeguarding in accordance with DODI 5200.48, CUI, which was issued in March 2020 to better align with national CUI policy. The phased implementation of the DOD CUI program that is outlined in the DODI 5200.48, requires all CUI materials to carry the minimum required CUI markings. As you just learned, marking is the initial step in safeguarding CUI to ensure it is immediately recognized. The new marking requirements replace For Official Use Only (FOUO) and all other legacy markings. DODI 5200.48 also updates the requirements for secure communication standards of CUI including system configuration requirements and encryption required for electronic transmission.

Once CUI is identified and marked in accordance with new DOD policy requirements, outside of the new requirement for secure communication standards that were also defined with the issuance of DODI 5200.48, the requirements for handling, storage and destruction of CUI did not change.

Handling: Overview

Proper handling is a key part of Safeguarding CUI. CUI must always be kept in a controlled environment. This consists of an area or space with adequate physical or procedural controls to protect CUI from unauthorized access or unauthorized disclosure.

The basic procedures for physical safeguarding when CUI is in the office include maintaining visual and physical control while being careful not to expose CUI to unauthorized users who do not have an authorized, lawful government purpose to access it.

Physical or procedural controls include barriers, managed access controls, and a computer splash screen with a disclaimer or warning. These are all policy requirements. Some best practices include using a Standard Form (SF) 901, Cover Sheet over hardcopy materials and using a privacy screen.

Handling: Scenario

Let's try a scenario. You have some CUI documents properly stored in your office. Today you will need to take them out of storage and reference them throughout the day while working on your current project.

You are working alone in the office all day, except for a couple of meetings in your office.

What special precautions should you take to safeguard the CUI documents during those meetings in your office?

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

- ○ Leave the documents on the desk and conduct meetings in another location
- ○ Place a SF 901 CUI cover sheet over the CUI documents or put them back in storage
- ○ No precautions are needed since you are not sharing the CUI documents

Handling: During Working Hours – At Desk

Let's take a closer look at ways to handle CUI while working at your desk during working hours.

Type of Media	Handling CUI During Working Hours – At Desk
Electronics	Ensure screen cannot be viewed from another person standing or sitting nearby. Approved options include: • Privacy screen • Turning off the monitor • Office dividers or barriers
Hard Copy	Conceal the contents from casual viewing. As an option, you can use a SF 901 cover sheet placed on top of documents to conceal the contents from casual viewing.

Handling: Hardcopy CUI – Scenario

What happens if you need to leave your desk during working hours? For example, let's say you have been working with CUI documents all morning and you plan to leave your desk and go to lunch.

What special precautions should you take to safeguard the CUI documents when you leave your office?

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

- ○ Put it in a paper tray on top of your file cabinet
- ○ Leave it in your office on your desk with a SF 901 CUI cover sheet
- ○ Leave it with your co-worker because you know he is trustworthy
- ○ Bring it with you to keep it under visual control

Handling: Electronic CUI – Scenario

What about electronic CUI?

What special precautions should you take to safeguard the CUI on your computer when you need to step away from your desk?

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

- ○ Remove your access card and ensure the system is locked.
- ○ Ensure your monitor isn't visible to others.
- ○ Leave your computer on but turn off the monitor.
- ○ No special precautions are needed to safeguard the CUI stored on your computer.

Storing: Overview

Now that you are familiar with handling CUI, let's look at storage. When not handling CUI, it must be stored in a controlled environment. This means there are sufficient internal security measures in place to

prevent or detect unauthorized access. When storing CUI under your control, you must provide the appropriate safeguarding measures.

Storage must have at least one physical barrier and reasonably ensure the CUI is protected from unauthorized access and observation. In addition, authorized holders should mark containers used to store CUI. As a best practice to minimize unauthorized access, whether it is during or after working hours, you should NEVER store CUI in a:

- Personal residence
- Hotel room safe, or
- Automobile

You should consult your DOD CUI Component Program Manager, Security Manager, or leadership for exceptions to these storage safeguards while teleworking or traveling.

Storing: During Working Hours – Scenario

Now it's your turn. How should you store CUI in your workspace during and after working hours? Review the following three scenarios and answer each question.

Let's say you have been working on a report all morning while accessing CUI documents for reference. It's early afternoon and you have finally finished it. Before beginning the next report, what should you do with the CUI documents on your desk since you no longer need them for your current report?

Which of the following CUI storage methods is allowable **DURING** working hours?

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

- ☐ Store it in unlocked containers
- ☐ Store it in your unlocked desk
- ☐ Store it in a locked cabinet
- ☐ Store it on your desk without a cover sheet
- ☐ Store it in the desk and lock it
- ☐ Store it in a locked room

Storing: After Working Hours with Security – Scenario

Let's take a closer look at storing CUI after working hours. Previously, when you finished your report, you stored the CUI documents you were referencing in your unlocked desk. Now that it is time to leave for the day you need to find a safe place to store it. Fortunately, the facility where you currently work has security that continuously monitors access to the facility.

Which of the following can you use to physically store CUI AFTER working hours?

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

- ☐ You can store it in an unlocked container
- ☐ You can keep it in the unlocked desk

- ☐ You can store it in your locked cabinet
- ☐ You can store it on your letter tray on your desk
- ☐ You can store it in a locked room

Storing: After Working Hours without Security – Scenario

Let's look at the same scenario but this time, imagine that you work at a facility that **does not have security that continuously monitors access to the facility**.

Which of the following can you use to physically store CUI AFTER working hours?

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

- ☐ On your desk in a folder
- ☐ In a file box in the corner of your office
- ☐ In a locked cabinet
- ☐ In a bin on your desk
- ☐ In an unlocked file cabinet
- ☐ In a locked room

Storing: Electronic Environments

We just addressed ways to physically store hard copy CUI; now let's look at ways you can store it in an electronic environment. CUI may only be digitally stored on an authorized Information Technology (IT) system or application provided the system:

- Is configured at no less than the Moderate Confidentiality impact level,
- Has limited access based on need; and
- Meets DOD's IT Security Policy requirements in accordance with DODI 8500.01, Cybersecurity and 8510.01, Risk Management Framework for DOD systems.

Now that you have learned how to handle and store CUI, take a minute to access the Workplace Reference document in the Course Resources. For your personal reference, complete the CUI Component Program Manager, Handling, and Storing sections.

Sharing: Overview

You have just learned ways to safeguard CUI. In this next section we will discuss sharing CUI. Sharing occurs when authorized holders provide access, transmit, or transfer CUI to other authorized holders through internal or external means.

Sharing includes:

- Disseminating CUI in person, for example, through discussions and meetings;
- Transmitting CUI electronically via the web, email, fax, mail, or phone; and
- Transporting CUI by traveling with it, hand- carrying it, or transporting it to meetings.

Sharing: When is Sharing CUI Permitted?

Whether you are disseminating, transmitting, or transporting CUI, access and sharing is permitted if it:

- Complies with the law, regulation, or government-wide policy, collectively referred to as authorities;
- Furthers a lawful government purpose;
- Is not restricted by an authorized Limited Dissemination Control, or LDC; or
- Is not prohibited by one or more authorities.

Sharing: Authorized Government Purpose

Individuals should not have access to CUI unless the person with authorized possession, knowledge, or control of CUI determines there is an authorized, lawful government purpose to share it. Groups that may have lawful government purpose include:

- Members of congress and their staff;
- All levels of government;
- Other federal agencies, government contractors, foreign allies and partner nations, as well as
- Academia.

Sharing: LDCs and Distribution Statements

Remember, sharing CUI may be restricted by authorized LDCs. Per policy, authorized holders can put limits on disseminating CUI using the DOD approved LDCs; however, these controls can only be approved by the originator of the CUI.

Access should be encouraged and allowed for a lawful government purpose; therefore, LDCs should not be used to unnecessarily restrict it. If no LDCs are on the document, then anyone with a lawful government purpose can access and receive it. Access Appendix B: to view the CUI Limited Dissemination Controls.

In addition, the CUI category Controlled Technical Information (CTI) requires the application of Distribution Statements as described in DODI 5230.24 Distribution Statements on DOD Technical Information. This is the only category of CUI authorized to use them. CTI includes Scientific, Technical, Engineering and Export Controlled Technical Information.

Sharing: Requirements When Sharing Legacy Materials

Before we leave the topic of sharing, there are requirements you need to be aware of when sharing legacy materials, unclassified information that was marked as restricted from access or dissemination in some way, prior to the new DOD CUI program.

DOD legacy marked material does not need to be remarked or redacted as long as it remains under DOD control or is accessed online and downloaded for use within the DOD. This is the case even if other agencies and contractors are granted access to such websites or databases. However, if legacy information will be shared outside DOD, or if a new derivative document is created from this material, then the information must be reviewed to ensure it still qualifies as CUI and, if it does, remarked as such.

Sharing: Legacy Materials – Scenario

Consider some legacy information that you have.

You have some DOD legacy documents that you have cause to share with an agency outside the DOD. What do you need to do before you share this material?

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

- ○ You must first review the information to see if it still qualifies as CUI; if so, remark the legacy material in accordance with DOD CUI policy.
- ○ Immediately remark the material as legacy automatically qualifies as CUI.

Transmitting Methods

Now that we've discussed dissemination and who may access CUI, let's address the ways in which CUI may be transmitted. Some common transmission methods include email, mail, fax, telephone, electronic systems, and file sharing. Let's look at ways to safely share CUI using each of these transmission methods.

Email

When conducting official business involving CUI on electronic and cloud-based environments personnel should not use unofficial or personal (e.g., ".net" and ".com") e-mail accounts, messaging systems, servers, or other non-DOD information systems, unless they are approved or authorized government contractor systems.

When conducting official business involving CUI on electronic and cloud-based environments personnel should send CUI only from a ".mil or .gov" account or government authorized industry email.

Encrypt CUI if sent:

- Via email
- Via NIPRNet
- When in a data at rest state on mobile devices. Data at rest is data that has reached a destination and is not being accessed or used. It typically refers to stored data and excludes data that is moving across a network or is temporarily in computer memory waiting to be read or updated.

Mail

Delivery Services

- Use first class mail, parcel post, or bulk shipments
- As a best practice, use in-transit automated tracking and accountability tools when sending CUI material

Delivery Methods

- Use the following to mail/ship CUI:
- US Postal Service (USPS)
- Any commercial delivery service (FedEx, UPS)
- Interoffice mail delivery/Interagency mail delivery

Packaging

- As a best practice, place SF 901 CUI cover sheet on top of the documents
- Do not place CUI markings on the outside of the packaging
- Address the interior envelope/package to a specific recipient (not to an office or an organization)

Fax/Transmittal

Sender's Role

- The sender is responsible for ensuring that appropriate protection is available at the receiving location before transmission
- FAX is attended by a person authorized to receive CUI
- The FAX machine is located in a controlled environment
- SF 901-fax coversheet is used alerting the recipient of the presence of CUI

Telephone

Type of Connection

- Hard-wired land-line phones are permitted for use
- Avoid wireless telephone transmission of CUI when other options are available

Electronic Systems

Websites

- No CUI is permitted on any public-facing websites

Dedicated Sites

- Your organization should have and maintain dedicated network sites, SharePoint sites, or possibly intranet/extranet sites where only authorized individuals are accessing CUI
- This includes ensuring systems and networks where CUI is stored are compartmentalized and protected according to authorized, lawful government purpose for access

Confidentiality Level

- DOD information systems processing, storing, or transmitting CUI must be categorized at the "moderate" confidentiality impact level and follow the guidance in DODI 8500.01, Cybersecurity and 8510.01, Risk Management Framework for DOD Systems
- Non-DOD information systems processing, storing, or transmitting CUI must provide adequate security, and the appropriate requirements must be incorporated into all contracts, grants, and other legal agreements with non-DOD entities in accordance with DODI 8582.01, Security of Non-DOD Information Systems Processing Unclassified Nonpublic DOD Information and NIST SP 800-171

File Sharing

Approved Services/Systems

- Use approved file sharing service/capability to share files with others
- CUI information may be transmitted electronically via approved secure communication systems or systems utilizing other protective measures such as:
- Public Key Infrastructure or transport layer security (e.g., https)
- DOD SAFE (https://safe.apps.mil). This is a best practice to share large files/videos with DOD and non-DOD recipients and provides users with the ability to encrypt

Transmitting: Sending Email – Scenario

What would you do in this situation?

You are working on a project that requires you to work with CUI documents. Your coworker Sydney, who works out of a different office, was just assigned to work with you on this project. She too is authorized to access these documents.

Which of the following is an approved way for you to email the CUI documents to Sydney?

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

- ○ Use your ".mil or .gov" account; you do not need to encrypt the email.
- ○ Use your personal email account; you do not need to encrypt the email.
- ○ Use your ".mil or .gov" account; you need to encrypt the email.
- ○ Use your personal email account; you need to encrypt the email.

Transporting: Overview

There may be times when you will need to transport CUI to another location. CUI must always be protected, even when traveling. This includes having DOD CUI Program approved CUI markings on printed pages, and an SF 901 CUI cover sheet to clearly identify the information as CUI when transported.

Placing a CUI marked document in a briefcase is also acceptable for transport. There still should be one layer of protection, for example the SF 901 cover sheet, a folder, or envelope protecting the document from plain view.

You should notify the security manager by email or through some other means, such as a sign-out sheet, when removing CUI from the work environment. Refer to CDSE's CUI Toolkit for additional information on transporting CUI.

Now that you have learned how to share CUI, take a minute to access the Workplace Reference document in the Course Resources. For your personal reference, complete the Sharing section.

Teleworking: Overview

Safeguarding measures are not only used in the office. When teleworking or traveling with CUI each person must provide the appropriate safeguarding measures identified in the DODI 5200.48. The requirements for handling, storing, and file sharing are the same whether you are working in an office or teleworking.

Teleworking: Equipment

Let's take a closer look at ways to handle CUI while teleworking.

Telephone

- Use of a conventional wired landline or Voice over Internet Protocol (VOIP) is recommended
- Avoid discussions on wireless devices when possible. However, when no other option is available:
- Ensure government-furnished equipment and personal devices are updated with the latest updates and security patches
- Ensure passwords are responsibly managed, and encryption and signatures are applied to emails
- Do not use untrusted or public Wi-Fi or internet connections

Printer

- Keep documents under direct control of an authorized holder and protect them with the SF 901 cover sheet
- All CUI hard copy materials should be secured at all times, in such a manner, to protect from unauthorized access
- Ensure an authorized holder is available at the printer when sending CUI to the printer
- CUI should not sit unattended on a printer where unauthorized personnel could have access to it
- When possible, use a printer requiring a code, CAC, or other access credentials
- Ensure when reproducing CUI documents on equipment such as printers, copiers, scanners, or fax machines, that the equipment does not retain data, or the agency must otherwise sanitize it in accordance with NIST SP 800–53

Then take a minute to access the Workplace Reference document in the Course Resources and complete the Telework Considerations section for your personal reference.

Teleworking: Scenario

Let's try one last scenario. Although you typically work in the office, today you are working from home due to very icy road conditions outside. As you finish up your 9:00 am Zoom call, you realize you need to return some business calls that you received while you were in your meeting, many from people outside of your office.

During these business calls you will be discussing CUI.

Which method should you use to make these calls?

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

- ○ Using your personal cell phone
- ○ Using a wired landline phone
- ○ Using government furnished phone without recent security updates
- ○ Using an internet connection

Conclusion

Congratulations on completing the Safeguarding Part 2 & Sharing Short. In this Short you learned about safeguarding CUI through proper handling and storing as well as properly sharing CUI via disseminating, transmitting, and transporting it.

You should now be able to apply the policy requirements outlined in DODI 5200.48 to safeguard CUI by properly handling, storing, and sharing CUI materials. In addition, you should now have a completed Workplace Reference document customized for your workplace.

Course Objective

- Apply the policy requirements outlined in DODI 5200.48 to safeguard CUI by properly handling, storing, and sharing CUI materials.

Appendix A: Answer Key

Handling: Scenario

You have some CUI documents properly stored in your office. Today you will need to take them out of storage and reference them throughout the day while working on your current project.

You are working alone in the office all day, except for a couple of meetings in your office.

What special precautions should you take to safeguard the CUI documents during those meetings in your office?

Select the best response.

- ○ Leave the documents on the desk and conduct meetings in another location
- ⦿ Place a SF 901 CUI cover sheet over the CUI documents or put them back in storage (correct response)
- ○ No precautions are needed since you are not sharing the CUI documents

***Feedback**: Since you will have a couple of meetings in your office throughout the day, CUI may be exposed to others in the office who do not have an authorized, lawful government purpose to access the CUI. Physical safeguarding will be needed.*

Handling: Hardcopy CUI – Scenario

What happens if you need to leave your desk during working hours? For example, let's say you have been working with CUI documents all morning and you plan to leave your desk and go to lunch.

What special precautions should you take to safeguard the CUI documents when you leave your office?

Select the best response.

- ○ Put it in a paper tray on top of your file cabinet
- ⦿ Leave it in your office on your desk with a SF 901 CUI cover sheet (correct response)
- ○ Leave it with your co-worker because you know he is trustworthy
- ○ Bring it with you to keep it under visual control

***Feedback**: CUI may be left on your desk provided it is covered or at least turned over to prevent casual viewing. You can also store the CUI documents in locked or unlocked containers, desk drawers, or cabinets until you return from lunch. You should not take the CUI with you to lunch.*

Handling: Electronic CUI – Scenario

What special precautions should you take to safeguard the CUI on your computer when you need to step away from your desk?

Select the best response.

- ⦿ Remove your access card and ensure the system is locked. (correct response)
- ○ Ensure your monitor isn't visible to others.
- ○ Leave your computer on but turn off the monitor.
- ○ No special precautions are needed to safeguard the CUI stored on your computer.

***Feedback**: The system must be secured by removing the access card and ensuring the system is locked.*

Storing: During Working Hours – Scenario

Let's say you have been working on a report all morning while accessing CUI documents for reference. It's early afternoon and you have finally finished it. Before beginning the next report, what should you do with the CUI documents on your desk since you no longer need them for your current report?

Which of the following CUI storage methods is allowable **DURING** working hours?

Select all that apply.

- ☑ Store it in unlocked containers (correct response)
- ☑ Store it in your unlocked desk (correct response)
- ☑ Store it in a locked cabinet (correct response)
- ☐ Store it on your desk without a cover sheet
- ☑ Store it in the desk and lock it (correct response)
- ☑ Store it in a locked room (correct response)

***Feedback**: During working hours, you can store your CUI in either locked or unlocked containers, cabinets, or desks as well as a locked room. You cannot store CUI on your desk without a cover sheet.*

Storing: After Working Hours with Security – Scenario

Previously, when you finished your report, you stored the CUI documents you were referencing in your unlocked desk. Now that it is time to leave for the day you need to find a safe place to store it. Fortunately, the facility where you currently work has security that continuously monitors access to the facility.

Which of the following can you use to physically store CUI AFTER working hours?

Select all that apply.

- ☑ You can store it in an unlocked container (correct response)
- ☑ You can keep it in the unlocked desk (correct response)

- ☑ You can store it in your locked cabinet (correct response)
- ☐ You can store it on your letter tray on your desk
- ☑ You can store it in a locked room (correct response)

***Feedback**: Correct. Locked or unlocked containers, desks, and cabinets as well as a locked room can be used to physically store CUI after hours when the facility provides security for continuous monitoring. You cannot store it in the open on the letter tray on your desk.*

Storing: After Working Hours without Security – Scenario

You work at a facility that **does not have security that continuously monitors access to the facility**.

Which of the following can you use to physically store CUI AFTER working hours?

Select all that apply.

- ☐ On your desk in a folder
- ☐ In a file box in the corner of your office
- ☑ In a locked cabinet (correct response)
- ☐ In a bin on your desk
- ☐ In an unlocked file cabinet
- ☑ In a locked room (correct response)

***Feedback**: A locked cabinet, desk, or room can be used to physically store CUI when the facility does NOT provide security for continuous monitoring. After working hours, the CUI storage areas must be locked.*

Sharing: Legacy Materials – Scenario

You have some DOD legacy documents that you have cause to share with an agency outside the DOD. What do you need to do before you share this material?

Select the best response.

- ⦿ You must first review the information to see if it still qualifies as CUI; if so, remark the legacy material in accordance with DOD CUI policy. (correct response)
- ○ Immediately remark the material as legacy automatically qualifies as CUI.

***Feedback**: If legacy documents are being shared with external agency(s), information must first be reviewed to determine if it meets the requirements to still be considered CUI and if so, must be marked in accordance with the new CUI requirements.*

Transmitting: Sending Email – Scenario

You are working on a project that requires you to work with CUI documents. Your coworker Sydney, who works out of a different office, was just assigned to work with you on this project. She too is authorized to access these documents.

Which of the following is an approved way for you to email the CUI documents to Sydney?

Select the best response.

- ○ Use your ".mil or .gov" account; you do not need to encrypt the email.
- ○ Use your personal email account; you do not need to encrypt the email.
- ⦿ Use your ".mil or .gov" account; you need to encrypt the email. (correct response)
- ○ Use your personal email account; you need to encrypt the email.

***Feedback**: You should only send CUI from a ".mil or .gov" account for authorized industry email. Encrypt CUI if sending via email, NIPRNet, or Non-classified Internet Protocol (IP) Router Network, and when in a data at rest state, typically stored data, on your mobile devices.*

Teleworking: Scenario

Although you typically work in the office, today you are working from home due to very icy road conditions outside. As you finish up your 9:00 am Zoom call, you realize you need to return some business calls that you received while you were in your meeting, many from people outside of your office.

During these business calls you will be discussing CUI.

Which method should you use to make these calls?

Select the best response.

- ○ Using your personal cell phone
- ⦿ Using a wired landline phone (correct response)
- ○ Using government furnished phone without recent security updates
- ○ Using an internet connection

***Feedback**: Use of a conventional wired landline or Voice over Internet Protocol (VOIP) is recommended. Avoid discussions on wireless devices and untrusted or public Wi-Fi or internet connections.*

Appendix B: CUI Limited Dissemination Controls

Control	Marking	Description
Federal Employees Only *	FED ONLY	Dissemination authorized only to employees of the U.S. Government executive branch agencies or armed forces personnel of the U.S. or Active Guard and Reserve.
Federal Employees and Contractors Only *	FEDCON	Includes individuals or employees who enter into a contract with the U.S. to perform a specific job, supply labor and materials, or for the sale of products and services, so long as dissemination is in furtherance of the contractual purpose.
No Dissemination to Contractors	NOCON	Intended for use when dissemination is not permitted to federal contractors, but permits dissemination to state, local, or tribal employees.
Dissemination List Controlled **	DL ONLY	Dissemination authorized only to those individuals, organizations, or entities included on an accompanying dissemination list.
Releasable by Information Disclosure Official	RELIDO	A permissive foreign disclosure and release marking used to indicate that the originator has authorized a Senior Foreign Disclosure and Release Authority (SFDRA) to make further sharing decisions for uncaveated intelligence material (intelligence with no restrictive dissemination controls) in accordance with existing procedures, guidelines, and implementation guidance. Note: Only agencies that are eligible to use RELIDO in the intelligence community (IC) classified information context may use this LDC on CUI. It is defined and applied in the same manner as in the IC context.
No Foreign Dissemination	NOFORN	Information may not be disseminated in any form to foreign governments, foreign nationals, foreign or international organizations, or non-U.S. citizens.
Authorized for Release to Certain Foreign Nationals Only	REL TO USA, [LIST]	Information has been predetermined by the designating agency to be releasable only to the foreign country(ies) or international organization(s) indicated, through established foreign disclosure procedures and channels. It is NOFORN to all foreign countries/international organizations not indicated in the REL TO marking. See list of approved country codes.
Display Only	DISPLAY ONLY	Information is authorized for disclosure to a foreign recipient, but without providing them a physical copy for retention to the foreign country(ies) or international organization(s) indicated, through established foreign disclosure procedures and channels.

Control	Marking	Description
Attorney Client	ATTORNEY-CLIENT	Dissemination of information beyond the attorney, the attorney's agents, or the client is prohibited, unless the agency's executive decision makers decide to disclose the information outside the bounds of its protection.
Attorney Work Product	ATTORNEY-WP	Dissemination of information beyond the attorney, the attorney's agents, or the client is prohibited, unless specifically permitted by the overseeing attorney who originated the work product or their successor.

* The use of this LDC does not prevent the sharing of information with Congress and other oversight organizations e.g. GAO.

** DL ONLY is used when you have a specific organization or list of individuals authorized to receive the document and none of the other LDCs apply. The list must be on or attached to the document, or a link to the list annotated on the document.

April 29, 2022