CUI TRAINING

TEMPLATE

VERSION 3.0

DCSA CUI training slides are a resource that DOD and Industry may use to provide personnel required to complete annual CUI training. The information contained in this document fulfills DoD CUI training requirements.

IMPORTANT

The FIRST thing you should do BEFORE working with Controlled Unclassified Information (CUI) is to WORK WITH THE GOVERNMENT CONTRACTING ACTIVITY (GCA) (customer, prime, agency, GCA, etc.) to validate contracted CUI safeguarding requirements.

Always obtain clear, written verification and guidance on how to receive, handle, and store material under your contract/customer (i.e., Security Classification Guides (SCG), CUI Marking Guide).

Work with the Cognizant Security Office(s) (CSO) to assist with safeguarding guidance if you are unable to obtain it from the GCA.

BE CAREFUL! Once you start marking things CUI, you now have network and safeguarding requirements you must adhere to.

CONTENTS

- Introduction
- Why?
- Previous Markings
- How and Who Decides?
- CUI Life Cycle
    - **Create/Receive**
    - **Identify/Designate**
    - **Mark/Label**
    - **Storage/Safeguard**
    - **Disseminate**
    - **Decontrol/Destroy**
- Unauthorized Disclosure/Disciplinary Actions
- Wrap Up
- References
- Certificate of Completion

NOTE: The contents of this briefing—including illustrations—are Unclassified

INTRODUCTION

Federal agencies routinely generate, use, store, and share information that requires some level of protection from unauthorized access and release.

Protection may be required for privacy, law enforcement, or other reasons pursuant to and consistent with law, regulation, and/or Government-wide policy.

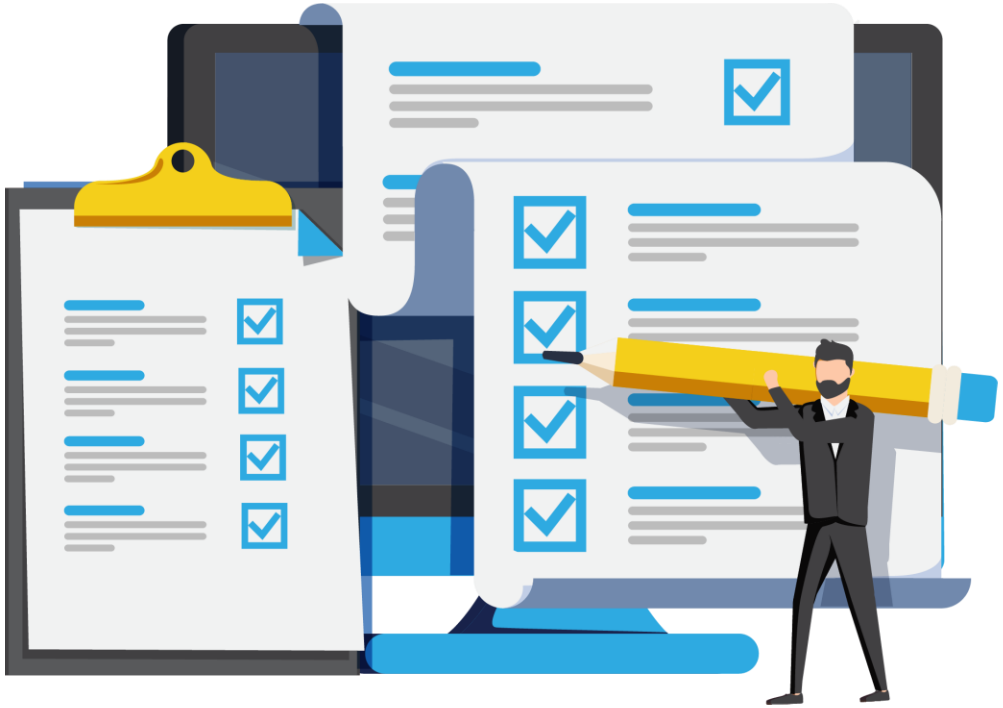
Historically, each DoD Component developed its own practices for safeguarding sensitive unclassified information, resulting in a patchwork of systems.

CUI represents an unprecedented initiative to standardized safeguarding practices.

WHY CUI TRAINING?

CUI training will be conducted **ANNUALLY** and, at a minimum, must include the following items per DoDI 5200.48:

1. Convey individual responsibilities related to protecting CUI;
2. Identify the categories or subcategories routinely handled by agency personnel and any special handling requirements;
3. Describe the CUI Registry, its purpose, structure, and location (i.e., https://www.dodcui.mil/Home/DoD-CUI-Registry);
4. Describe the differences between CUI Basic and CUI Specified;
5. Identify the offices or organizations with oversight responsibility for the CUI Program;
6. Address CUI marking requirements, as described by agency policy;
7. Address the required physical safeguards and methods for protecting CUI, as described by agency policy;
8. Address the destruction requirements and methods, as described by agency policy;
9. Address the incident reporting procedures, as described by agency policy;
10. Address the methods and practices for properly sharing or disseminating CUI within the agency and with external entities inside and outside the Executive branch; and
11. Address the methods and practices for properly decontrolling CUI, as described by agency policy.



NOTE: Industry organizations may develop their own CUI training.

This presentation captures all 11 categories, but Industry may instead use this training to meet the requirement: DoD CDSE CUI course https://securityhub.usalearning.gov/.

PREVIOUS/ LEGACY MARKINGS

1. **FOUO as a marking identification will no longer be used.**
   - Engage with Authorized Holders that are still using FOUO and reach out to DCSA to assist if needed.
2. **Legacy information (such as FOUO, SBU) does not automatically become CUI**. It must be reviewed by the Authorized Holder to determine if it meets the CUI requirements.
   - Legacy marked information stored on a DoD access-controlled website or database does not need to be re-marked as CUI.
   - When legacy information is incorporated into, or cited in, another document or material, it must be reviewed for CUI and marked accordingly.
3. It is our responsibility to **protect legacy information until such time that the Authorized Holder reviews the information** to determine if the data meets the CUI requirements and re-marks this data accordingly.

Legacy Material Definition

Legacy material is unclassified information that the government marked as restricted from access or dissemination in some way, or otherwise controlled, prior to the CUI Program.

HOW DO THEY DECIDE?

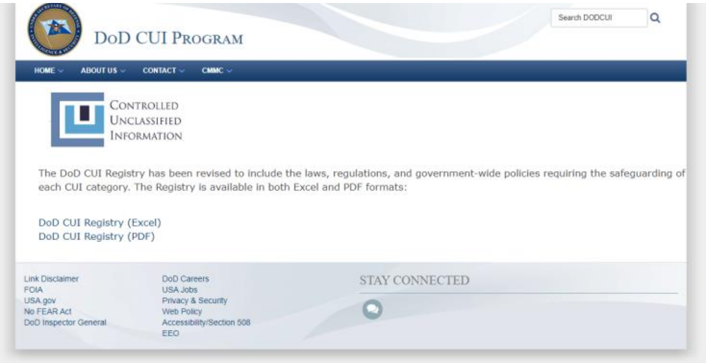
There is a registry for that!

There are TWO registries. The DoD CUI Registry provides an official list of indexes and categories used to identify various types of DoD CUI. While the DoD CUI Registry generally mirrors the Information Security Oversight Office-maintained National CUI Registry, it may provide additional information unique to the Department of Defense. As the CUI Executive Agent, ISOO maintains the National CUI Registry at https://www.archives.gov/cui.

WHAT IS CONSIDERED CUI

In order to be considered CUI, the information must fall within a law, regulation, or government-wide policy.

1 DoD Registry The DoD CUI Registry aligns each Index and Category to DOD issuances.

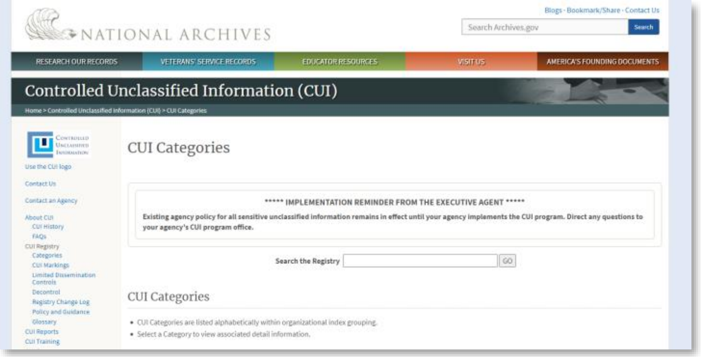


The DoD CUI Registry has been revised to include the laws, regulations, and government-wide policies requiring the safeguarding of each CUI category. The Registry is available in both Excel and PDF formats:

DoD CUI Registry (Excel)
DoD CUI Registry (PDF)

https://www.dodcui.mil/Home/DoD-CUI-Registry

2 ISOO Registry The National CUI Registry contains Indexes and categories for the entire Executive Branch and should be consulted for non-DOD contracts.



***** IMPLEMENTATION REMINDER FROM THE EXECUTIVE AGENT *****

Existing agency policy for all sensitive unclassified information remains in effect until your agency implements the CUI program. Direct any questions to your agency's CUI program office.

CUI Categories

- CUI Categories are listed alphabetically within organizational index grouping.
- Select a Category to view associated detail information.

https://www.archives.gov/cui/registry/category-list

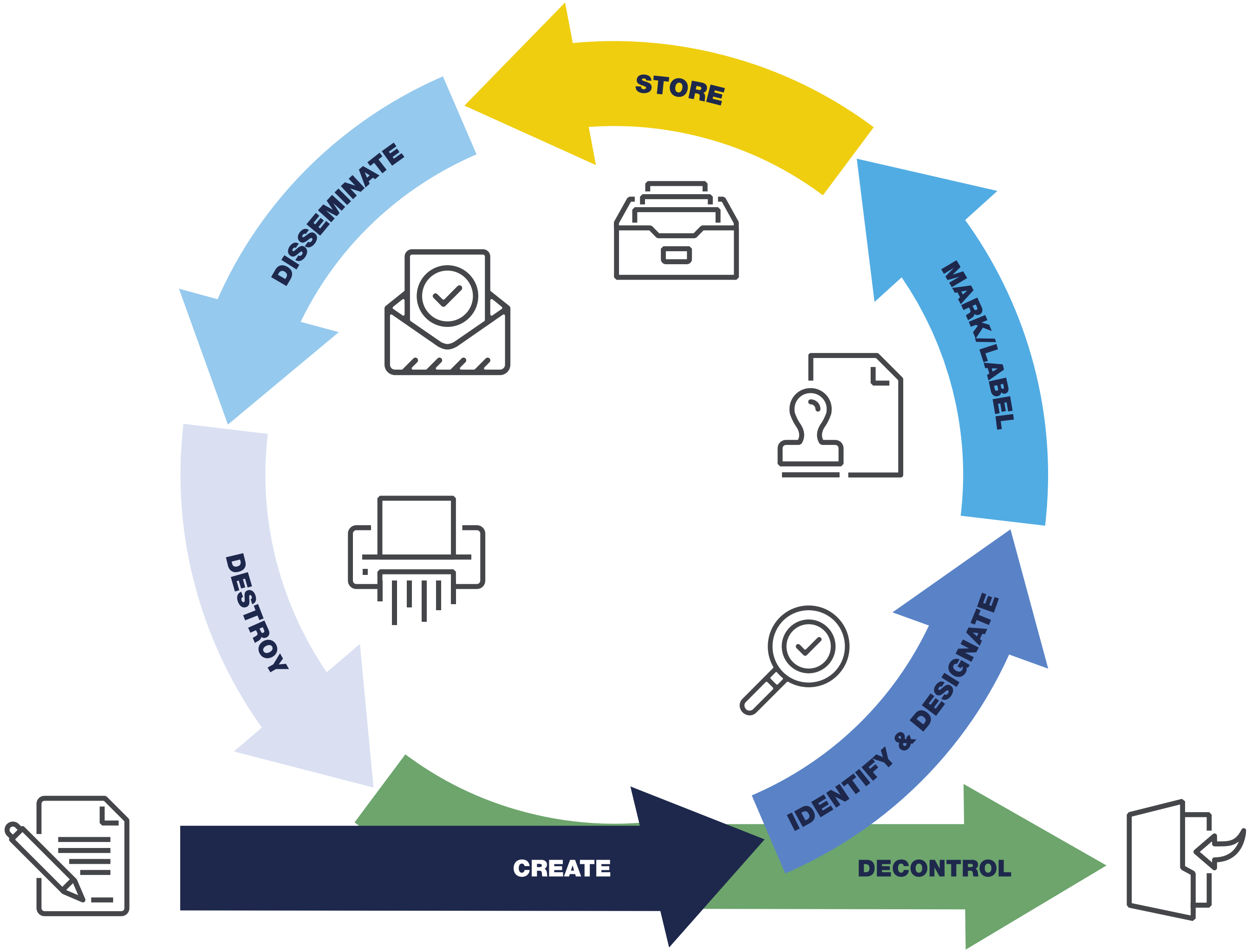
WHO DECIDES?

The **Authorized Holder (AH)** of a document or material is responsible for determining, at the time of creation, whether information in a document or material falls into a CUI category. If so, the authorized holder is responsible for applying CUI markings and dissemination instructions accordingly.

The Authorized Holder includes:

- DoD civilian and military personnel
- DoD Components, Agencies
- Contractors providing support to the DoD pursuant to contractual requirements

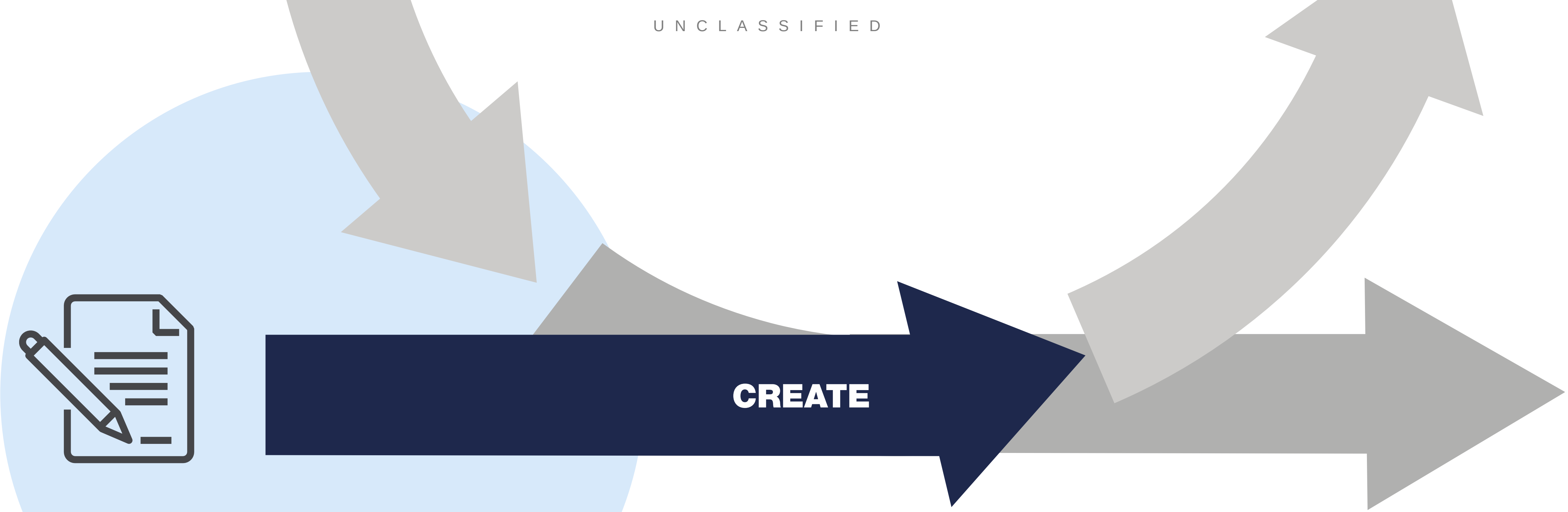
CUI LIFECYCLE



CUI is information created or generated in support of a Government contract.

Whenever CUI is distributed, the **Authorized Holders** (AH) may disseminate CUI as long as it complies with law, regulation, or government-wide policy; furthers a lawful government purpose; is not restricted by Limited Dissemination Control (LDC); and is not otherwise prohibited by any other law, regulation, or government-wide policy.

However, it is everyone's responsibility when sending or receiving, to identify, and safeguard CUI according to law, regulation, or government-wide policy.



CREATE

Controlled Unclassified Information (CUI) is created when information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits safeguarding or dissemination controls.

CREATING CUI

What is CUI?

- **CUI is government created or owned information** that requires safeguarding or dissemination controls consistent with applicable laws, regulations and government wide policies.
- **Anyone can be an Authorized Holder** and create CUI as long as it is generated for, or on behalf of, the government or agency under a contract and it falls into one of the DOD CUI categories. However, in most situations, Industry will be guided by its customer on what is CUI and what isn't.
- **CUI is not classified information. It is not corporate intellectual property** unless created for or included in requirements related to a government contract.
- **Access to CUI is based on having a lawful government purpose** which is similar to the need-to-know concept for access to classified or FOUO type information but intentionally less stringent.
- Material ***should not be marked CUI*** in order to:
  - Conceal violations of the law, inefficiency, or administrative errors.
  - Prevent embarrassment to a person, organization, or agency.
  - Prevent open competition.

WHAT IS *NOT* CUI?

- Classified information or a classification
- Corporate intellectual property (unless created for or included in requirements related to a government contract)
- Publicly available information

CREATING CUI

CUI Category Types

Once the category of CUI is determined then it will then fall under one of these two:

CUI Basic is any category of CUI which a law, regulation, or Government-wide policy says must be protected, but doesn't provide any further information about how to protect it.

CUI Specified has different marking and handling requirements. It is designed to accommodate the specific requirements of certain customers. CUI Specified is NOT a "higher level" of CUI, it is simply different and cannot be ignored or overlooked because of laws, Federal regulations and government-wide policies. Not every category and authority listed in the Registry is applicable to DoD.

CREATING CUI

Receiving CUI

The Defense Industrial Base (DIB) should understand what types of sensitive information they have. A contractor should ensure safeguards for sensitive information also flow down to subcontractors.

- FAR 52.204-21 defines 15 safeguarding requirements and procedures to protect FCI.
- The Defense FAR Supplement (DFARS) 252.204-7012 lists the safeguarding controls to protect CUI. The family of controls come from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171.

Current

- September 2020, Interim DFARS rule 2019-D041 imposed new requirements.
- Contractors working with CUI must now conduct an internal self-assessment based on NIST 800-171 .
- Contractors must upload their assessment scores into the Supplier Performance Risk System (SPRS). Before making an award, contracting officers now must verify that the SPRS score is not more than 3 years old.
- The contractor must have a System Security Plan (SSP) for all covered systems. For each control not met, the contractor must address it within a Plan of Action and Milestones (POAM). Here is a CUI plan of action template and a CUI SSP template.

This Medium is
CUI
U.S. Government Property
Protect it from unauthorized
disclosure in compliance with applicable
executive orders, statutes, and regulations.

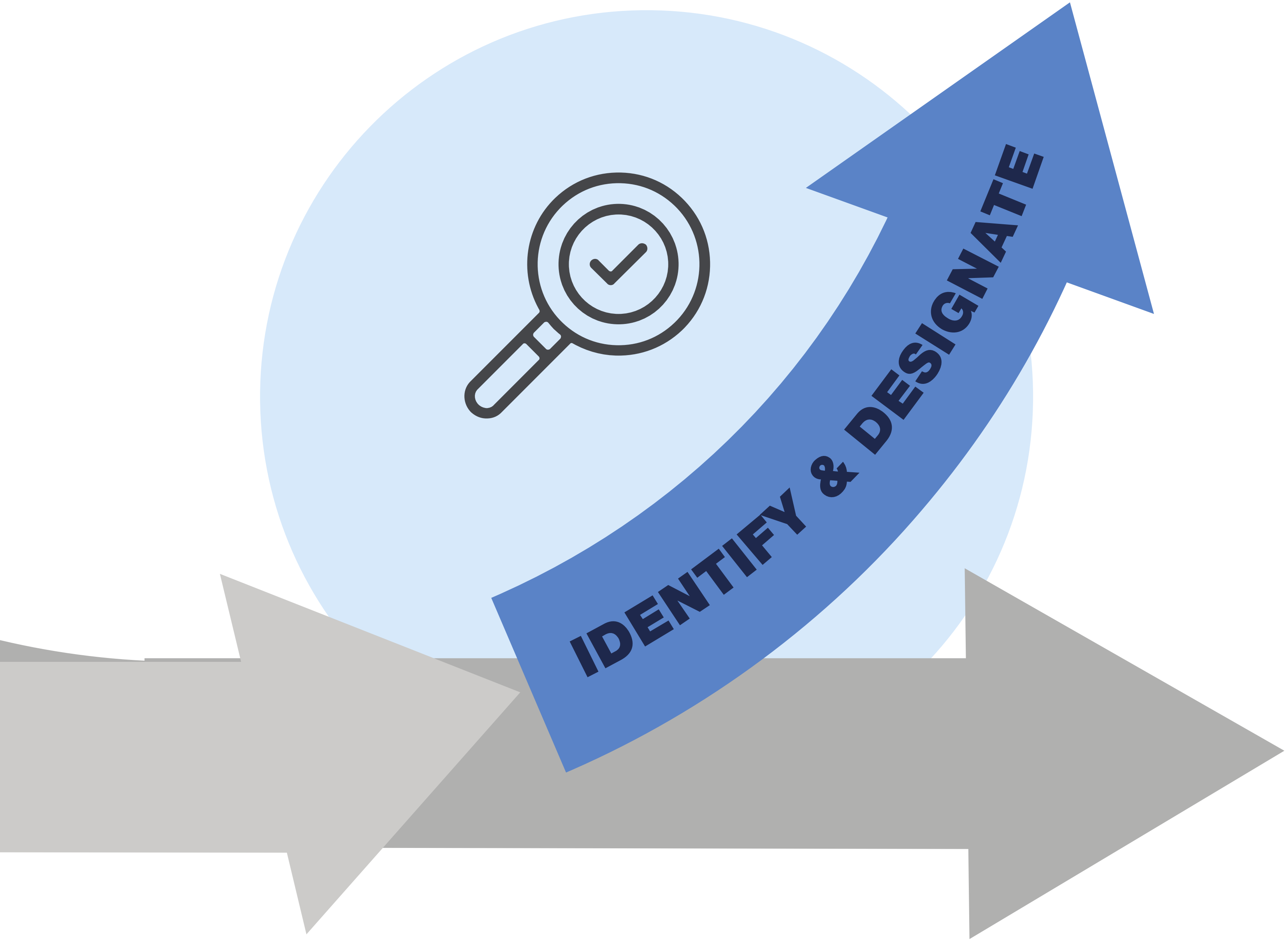
Cybersecurity Maturity Model Certification (CMMC) 2.0

- To safeguard sensitive national security information, the DoD launched CMMC 2.0, a comprehensive framework to protect the defense industrial base's (DIB) sensitive unclassified information from frequent and increasingly complex cyber attacks. With its streamlined requirements, CMMC 2.0:
  - Simplifies compliance by allowing self-assessment for some requirements
  - Applies priorities for protecting DoD information
  - Reinforces cooperation between the DoD and industry in addressing evolving cyber threats

What can Industry do now?

1. Educate people on cyber threats
2. Implement access controls
3. Authenticate users
4. Monitor your physical space
5. Update security protections

More information about CMMC can be found at: https://dodcio.defense.gov/CMMC/ -



The **Authorized Holder** of the CUI material is responsible for marking the material before distributing so that anyone receiving the CUI can properly identify it.

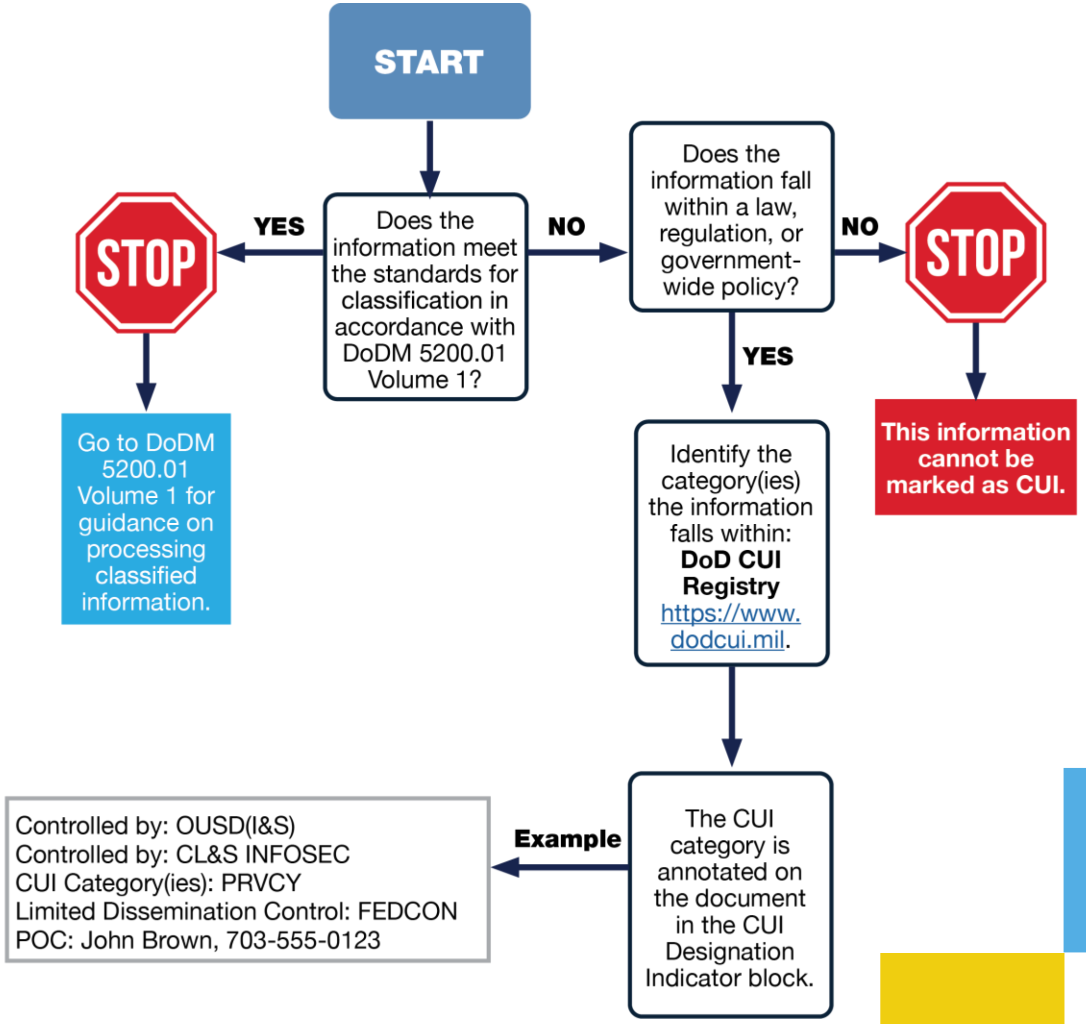
IDENTIFY & DESIGNATE

Identification

- The identification of CUI is critical in determining what sensitive information needs to be protected.
- CUI is generated for or on behalf of the department under a contract and determines if the information falls into one of the many categories found in the DoD CUI Registry.

WHAT IS *NOT* CUI?

- Classified information or a classification
- Corporate intellectual property (unless created for or included in requirements related to a government contract)
- Publicly available information



START

Does the information meet the standards for classification in accordance with DoDM 5200.01 Volume 1?

YES

STOP

Go to DoDM 5200.01 Volume 1 for guidance on processing classified information.

NO

Does the information fall within a law, regulation, or government-wide policy?

NO

STOP

This information cannot be marked as CUI.

YES

Identify the category(ies) the information falls within: **DoD CUI Registry** https://www.dodcui.mil.

The CUI category is annotated on the document in the CUI Designation Indicator block.

Example

Controlled by: OUSD(I&S)
Controlled by: CL&S INFOSEC
CUI Category(ies): PRVCY
Limited Dissemination Control: FEDCON
POC: John Brown, 703-555-0123

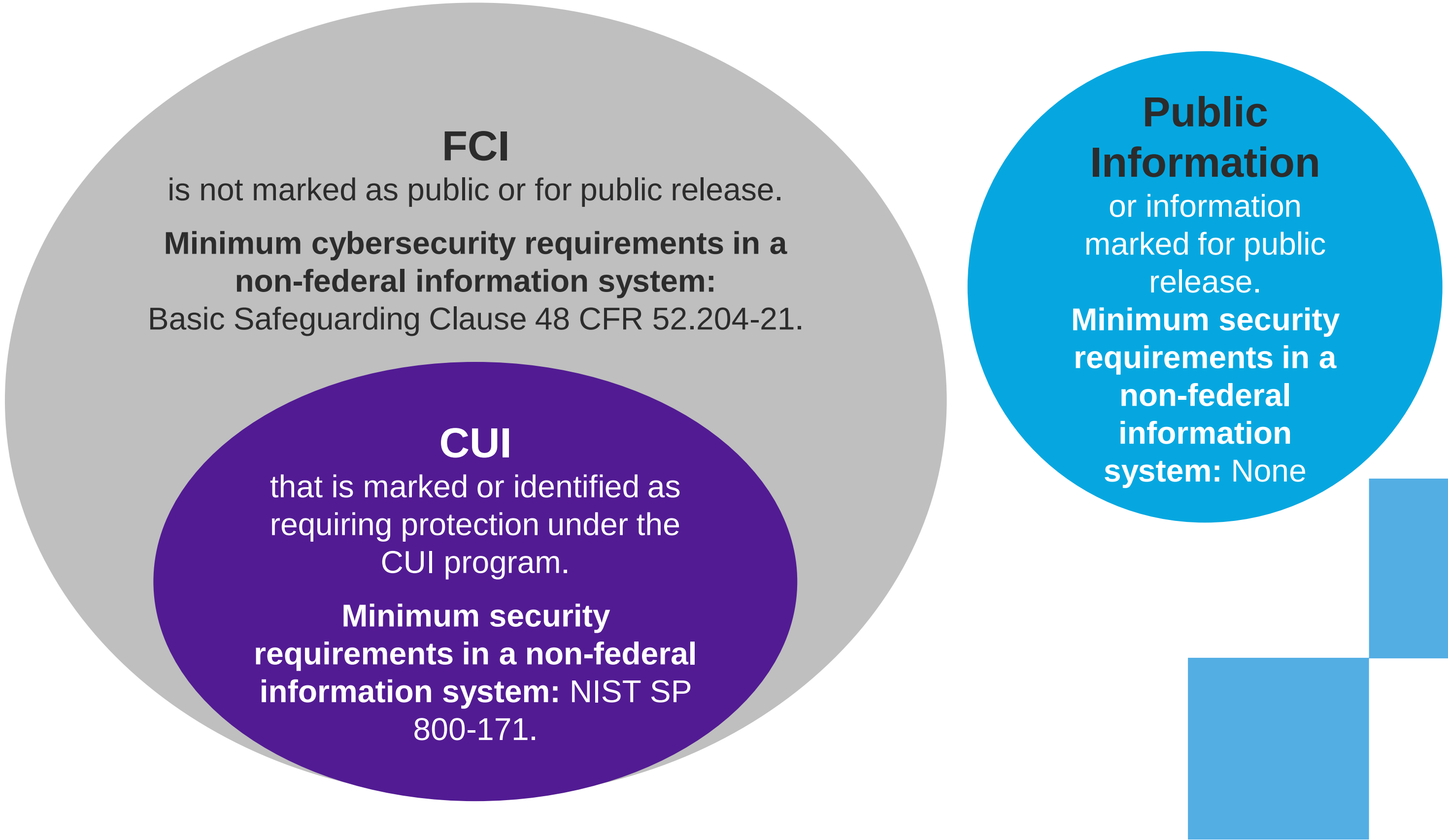
IDENTIFY & DESIGNATE

Federal Contract Information (FCI)

Federal Contract Information (FCI) *(48 CFR 52.204-21)* is not intended for public release and is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.

Remember that FCI can be CUI, but not all FCI is CUI.

[Click this link for more on FCI.]()



FCI
is not marked as public or for public release.

Minimum cybersecurity requirements in a non-federal information system:
Basic Safeguarding Clause 48 CFR 52.204-21.

CUI
that is marked or identified as requiring protection under the CUI program.

Minimum security requirements in a non-federal information system: NIST SP 800-171.

Public Information
or information marked for public release.
Minimum security requirements in a non-federal information system: None

All physical and digital media must be **marked** or **labeled** to alert individuals to the presence of CUI.

At minimum, CUI markings for unclassified DoD documents will include the acronym “CUI” in the banner and footer of the document.

MARK/LABEL

Marking Documents

Required

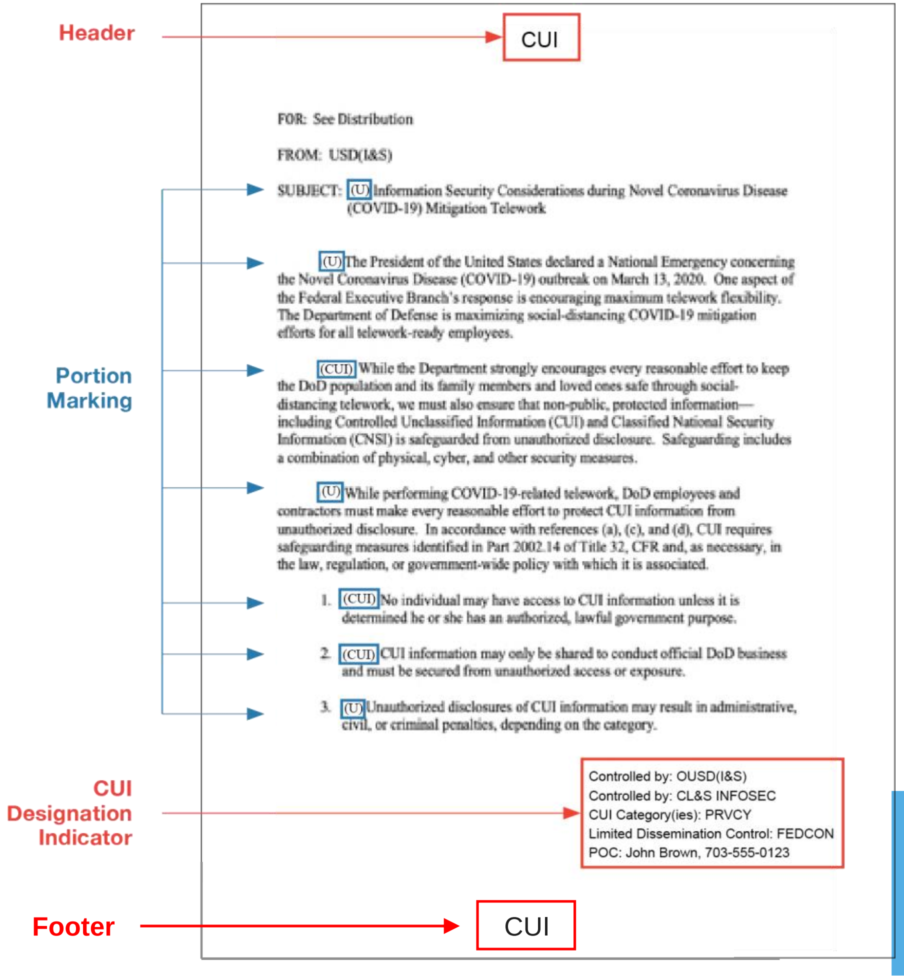
- Header/top/banner and Footer/bottom of document has “CUI” in bold letters
- ***Designation Indicator (5 items)***

Not required/optional

- Portion marking *(If you use portion marking, you must portion mark everything. Subjects, titles, individual sections, parts, paragraphs, or similar portions known to contain CUI, will be portion marked with “(CUI)” and everything else will have a “(U)” in front of the sentence).*
- CUI coversheet
- Page numbers

Other Notes

- There is no requirement to add the “U”, signifying unclassified, to the banner and footer as was required with the old FOUO marking (i.e., U//FOUO).
- Do NOT use “UNCLASSIFIED “U” before “CUI” in banner line or portion markings.
- Supplemental markings commonly used to inform recipients of the non-final status of a document (*e.g., DRAFT, Pre-decisional, Working Paper*) **do not** go in the banner line as they are not authorized CUI categories used to control information. Supplemental markings can be placed outside the banner line if approved by the **Authorized Holder.**
- Please see the DoD Desktop Marking Guide found on the DoD CUI Web Page here: DOD CUI Markings


Header
Portion Marking
CUI Designation Indicator
Footer

CUI

FOR: See Distribution

FROM: USD(I&S)

SUBJECT: (U) Information Security Considerations during Novel Coronavirus Disease (COVID-19) Mitigation Telework

(U) The President of the United States declared a National Emergency concerning the Novel Coronavirus Disease (COVID-19) outbreak on March 13, 2020. One aspect of the Federal Executive Branch's response is encouraging maximum telework flexibility. The Department of Defense is maximizing social-distancing COVID-19 mitigation efforts for all telework-ready employees.

(CUI) While the Department strongly encourages every reasonable effort to keep the DoD population and its family members and loved ones safe through social-distancing telework, we must also ensure that non-public, protected information—including Controlled Unclassified Information (CUI) and Classified National Security Information (CNSI) is safeguarded from unauthorized disclosure. Safeguarding includes a combination of physical, cyber, and other security measures.

(U) While performing COVID-19-related telework, DoD employees and contractors must make every reasonable effort to protect CUI information from unauthorized disclosure. In accordance with references (a), (c), and (d), CUI requires safeguarding measures identified in Part 2002.14 of Title 32, CFR and, as necessary, in the law, regulation, or government-wide policy with which it is associated.

1. (CUI) No individual may have access to CUI information unless it is determined he or she has an authorized, lawful government purpose.
2. (CUI) CUI information may only be shared to conduct official DoD business and must be secured from unauthorized access or exposure.
3. (U) Unauthorized disclosures of CUI information may result in administrative, civil, or criminal penalties, depending on the category.

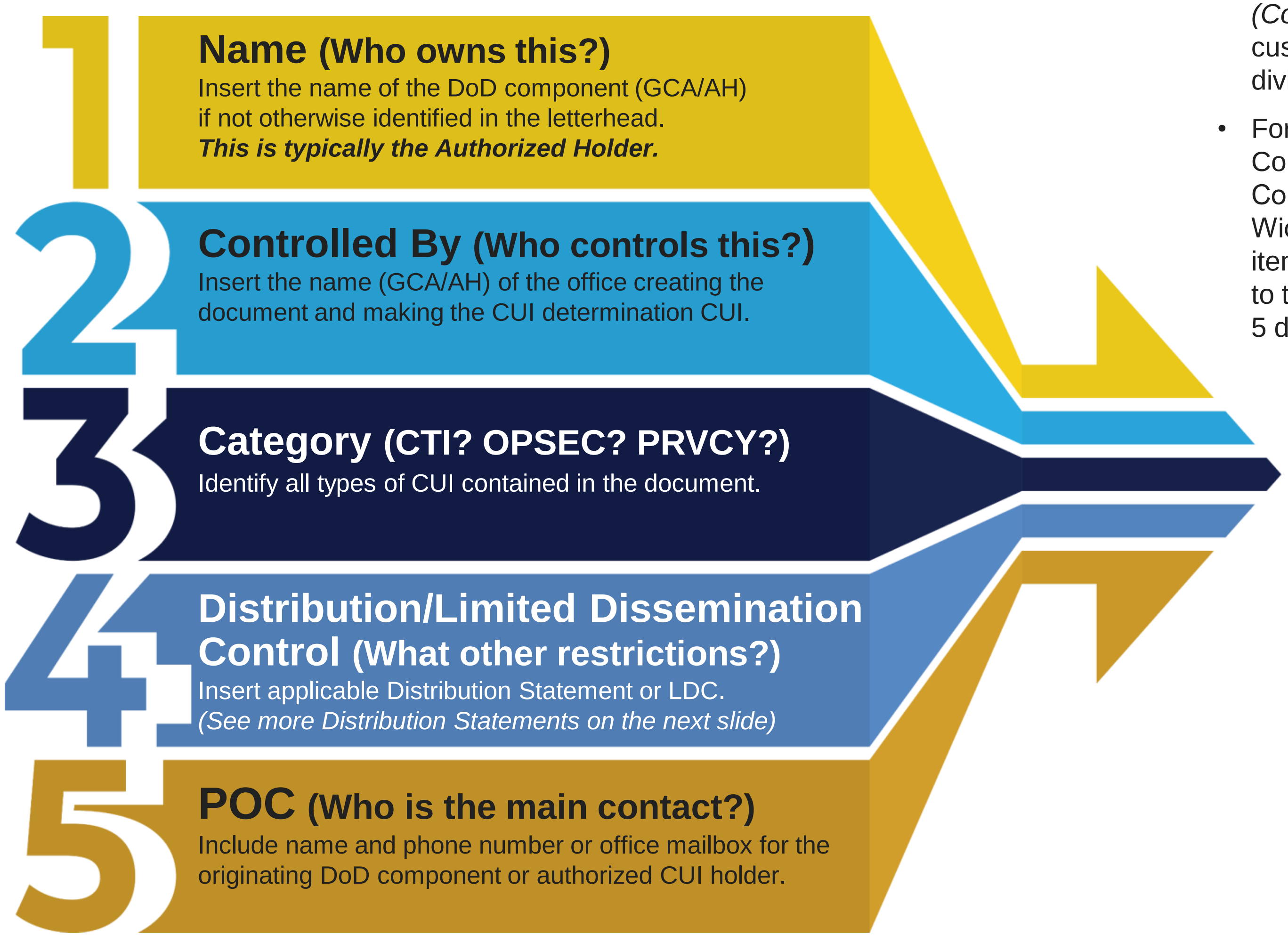
Controlled by: OUSD(I&S)
Controlled by: CL&S INFOSEC
CUI Category(ies): PRVCY
Limited Dissemination Control: FEDCON
POC: John Brown, 703-555-0123

CUI

MARK/LABEL

Designation Indicator

The designation indicator ***MUST INCLUDE*** these five items.



1 **Name** **(Who owns this?)**
Insert the name of the DoD component (GCA/AH) if not otherwise identified in the letterhead.
This is typically the Authorized Holder.

2 **Controlled By** **(Who controls this?)**
Insert the name (GCA/AH) of the office creating the document and making the CUI determination CUI.

3 **Category** **(CTI? OPSEC? PRVCY?)**
Identify all types of CUI contained in the document.

4 **Distribution/Limited Dissemination Control** **(What other restrictions?)**
Insert applicable Distribution Statement or LDC.
(See more Distribution Statements on the next slide)

5 **POC** **(Who is the main contact?)**
Include name and phone number or office mailbox for the originating DoD component or authorized CUI holder.

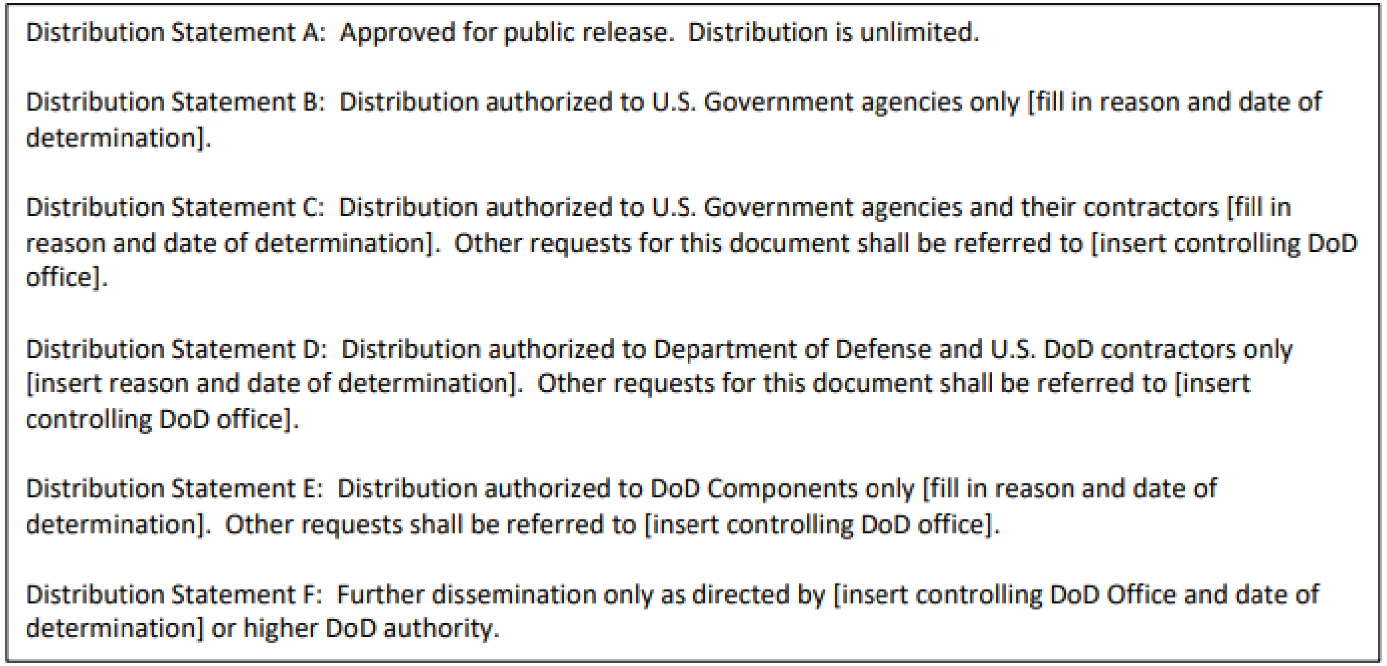
- You can see a difference between #1 *(Name)* and #2 *(Controlled by)* by reading the definitions. #1 will be the customer, but #2 *might* be a different customer or a division.
- For example, maybe we have a contract with a DoD Component building Widgets. #1 would be GCA (DoD Component), but the #2 might be “Secret Division of Widgets”. If you obtain CUI and you don’t see these 5 items on the first page or coversheet, you should go back to the owner/customer and ask them to please include the 5 designation indicators.

**DoDM 5200.01, Volume 2.*

Name: OUSD(I&S)
Controlled by: CL&S INFOSEC
CUI Category(ies): PRVCY
Limited Dissemination Control: FEDCON
POC: John Brown, 703-555-0123

MARK/LABEL

Distribution Statements (Part of Designation Indicator)



Distribution Statement A: Approved for public release. Distribution is unlimited.

Distribution Statement B: Distribution authorized to U.S. Government agencies only [fill in reason and date of determination].

Distribution Statement C: Distribution authorized to U.S. Government agencies and their contractors [fill in reason and date of determination]. Other requests for this document shall be referred to [insert controlling DoD office].

Distribution Statement D: Distribution authorized to Department of Defense and U.S. DoD contractors only [insert reason and date of determination]. Other requests for this document shall be referred to [insert controlling DoD office].

Distribution Statement E: Distribution authorized to DoD Components only [fill in reason and date of determination]. Other requests shall be referred to [insert controlling DoD office].

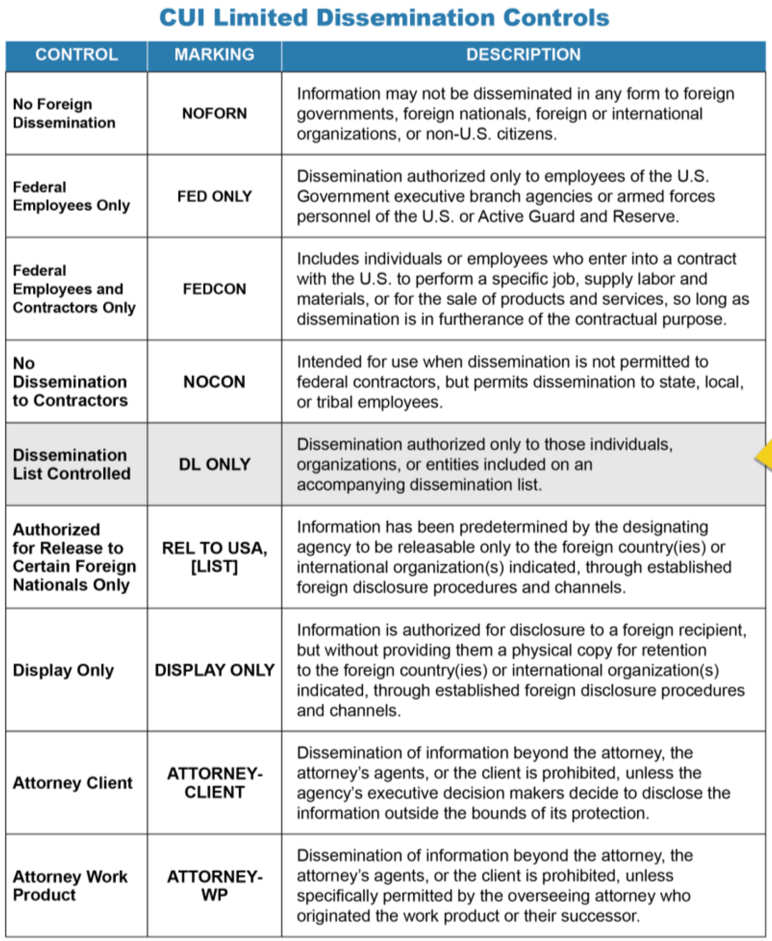
Distribution Statement F: Further dissemination only as directed by [insert controlling DoD Office and date of determination] or higher DoD authority.

Distribution statements, in accordance with DoDI 5230.24, are authorized for use with:

- CUI export controlled technical information
- Other scientific, technical, and engineering information
- Controlled technical information

MARK/LABEL

Limited Dissemination Control Markings (Part of Designation Indicator)



CUI Limited Dissemination Controls

CONTROL	MARKING	DESCRIPTION
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.
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.
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.
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.
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.

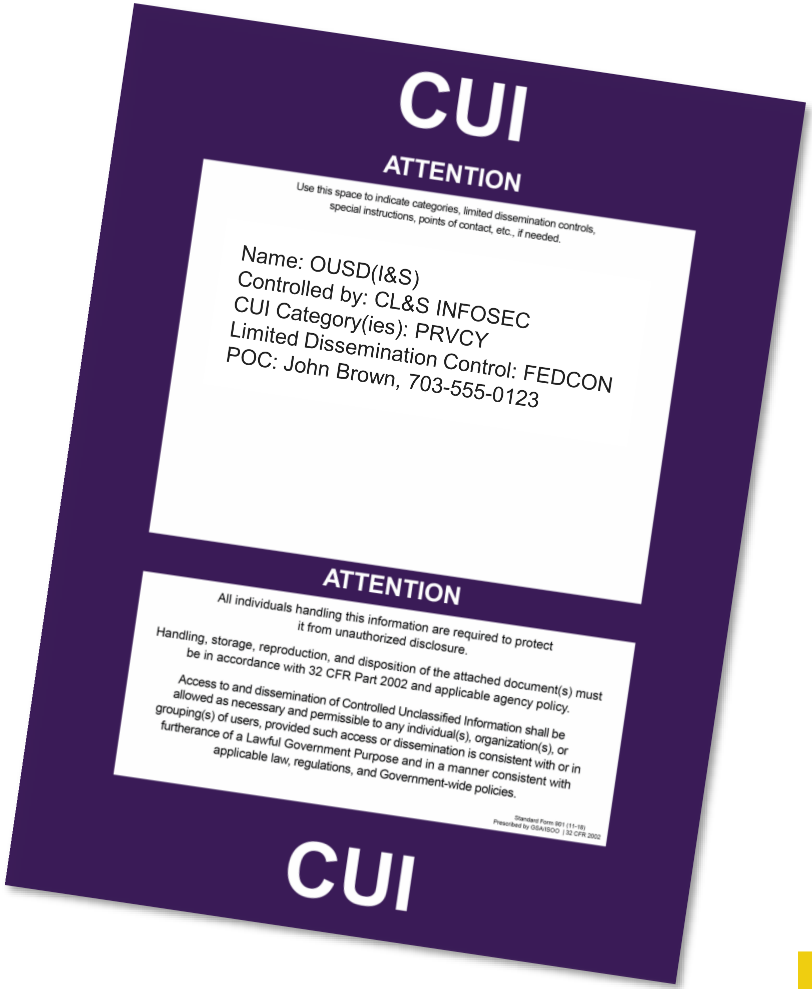
"DL ONLY" is used when you have a specific organization or list of individuals authorized to receive the document and none of the other LDCs apply. The list must be on or attached to the document, or a link to the list annotated on the document.

- 32 CFR Part 2002.4 defines LDC as any CUI EA-approved control that agencies may use to limit or specify CUI dissemination.
- LDCs are to be placed on unclassified documents and other materials when the CUI requires access restrictions, including those required by law, regulation, or government-wide policy.
- LDC markings cannot unnecessarily restrict CUI access, e.g., do not mark a document as "No Dissemination to Contractors" or "NOCON" unless there is a law, regulation, or policy that prohibits dissemination to a contractor.
- LDCs identify the audience deemed to have an authorized lawful government purpose to use the CUI.
- The absence of an LDC on a document means anyone with an authorized lawful government purpose is permitted access to the document. This does not imply it can be publicly released. All CUI documents must go through a public release review in accordance with DoDI 5230.09 and 5230.29.
- For a complete list LDC markings visit www.dodcui.mil.
- **LDC markings are NEW TO CUI and was not required on FOUO or other legacy materials.**

MARK/LABEL

CUI Coversheets (Optional)

- First blank area of coversheet CAN be filled out with Designator indicator.
- You can download a copy of the CUI coversheet (SF901) at either of these sites:
  - https://www.gsa.gov/forms-library/controlled-unclassified-information-cui-coversheet-0
  - https://www.archives.gov/cui/additional-tools



CUI

ATTENTION

Use this space to indicate categories, limited dissemination controls, special instructions, points of contact, etc., if needed.

Name: OUSD(I&S)
Controlled by: CL&S INFOSEC
CUI Category(ies): PRVCY
Limited Dissemination Control: FEDCON
POC: John Brown, 703-555-0123

ATTENTION

All individuals handling this information are required to protect it from unauthorized disclosure.

Handling, storage, reproduction, and disposition of the attached document(s) must be in accordance with 32 CFR Part 2002 and applicable agency policy.

Access to and dissemination of Controlled Unclassified Information shall be allowed as necessary and permissible to any individual(s), organization(s), or grouping(s) of users, provided such access or dissemination is consistent with or in furtherance of a Lawful Government Purpose and in a manner consistent with applicable law, regulations, and Government-wide policies.

Standard Form 901 (11-18)
Prescribed by GSA/ISOO | 32 CFR 2002

CUI

MARK/LABEL

Marking CUI and Classified

- "CUI" markings do not go in banner.
- Classified documents will be marked IAW DoDM 5200.01 Volume 2.
- Portion markings are required.
- CUI markings will appear in portions known to contain only CUI.
- Document will have both the CUI Designation Indicator and Classification Authority.

MARK/LABEL

Emails with CUI

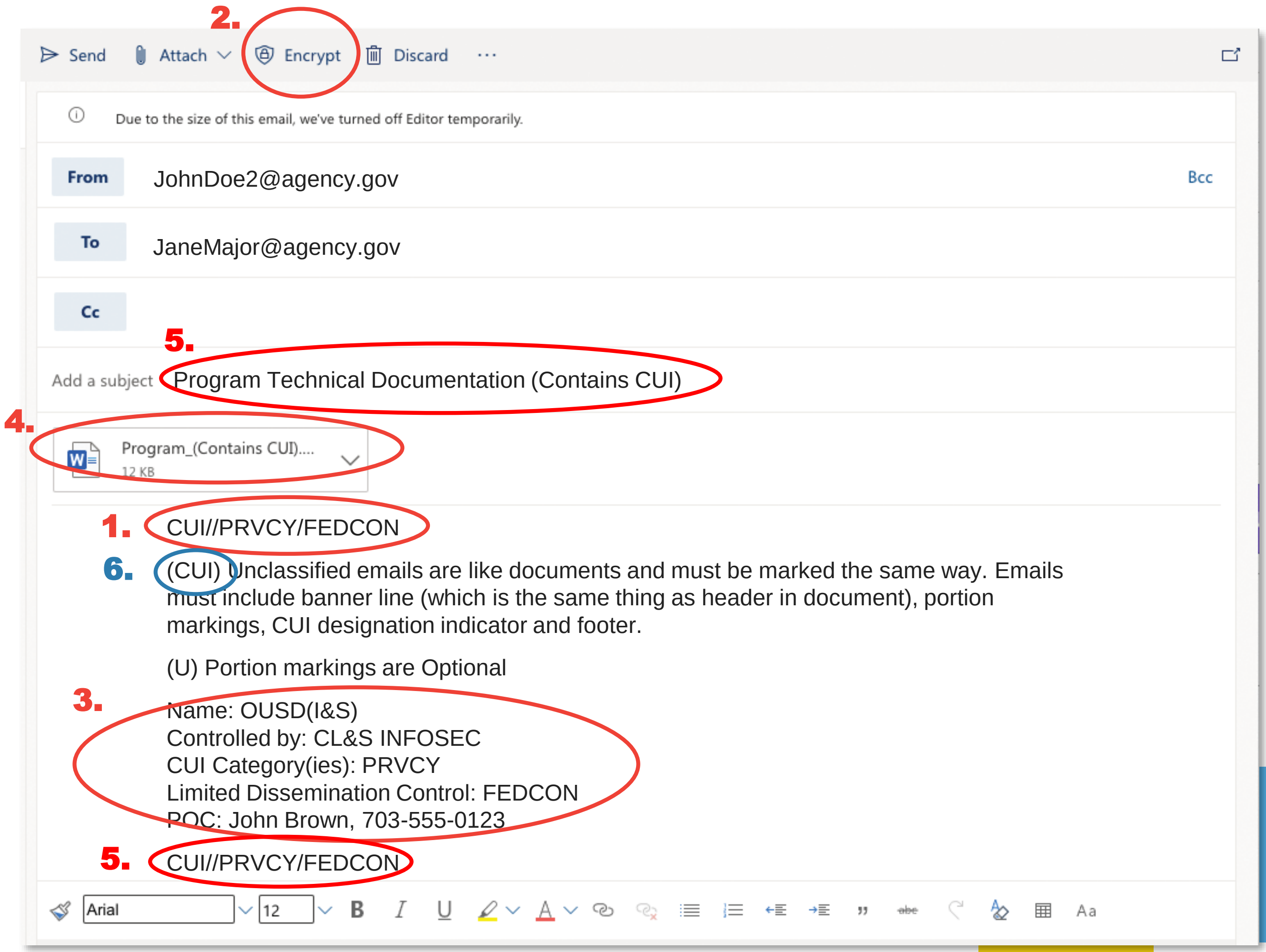
Required

1. Must apply “CUI” to top/banner.
2. **Must be encrypted.**
3. Must contain a CUI *Designation Indicator* block.
4. If including attachments containing CUI, the file name must indicate it includes CUI.
5. Apply “CUI” to the footer and subject line.

Optional but best practice

6. All paragraphs known to contain CUI may be portion marked.

DO NOT USE PERSONAL EMAIL ACCOUNTS to send CUI. This is necessary to ensure proper accountability for Federal records and to facilitate data spill remediation in accordance with Public Law 113-187 and the January 16, 2018 Deputy Secretary of Defense memorandum.



Due to the size of this email, we've turned off Editor temporarily.

From JohnDoe2@agency.gov

To JaneMajor@agency.gov

Cc

Add a subject Program Technical Documentation (Contains CUI)

Program_(Contains CUI)....
12 KB

CUI//PRVCY/FEDCON

(CUI) Unclassified emails are like documents and must be marked the same way. Emails must include banner line (which is the same thing as header in document), portion markings, CUI designation indicator and footer.

(U) Portion markings are Optional

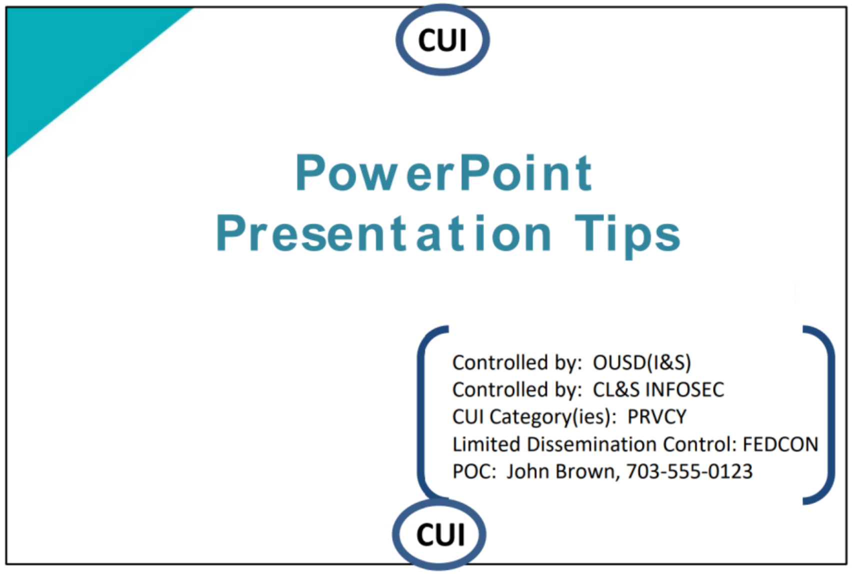
Name: OUSD(I&S)
Controlled by: CL&S INFOSEC
CUI Category(ies): PRVCY
Limited Dissemination Control: FEDCON
POC: John Brown, 703-555-0123

CUI//PRVCY/FEDCON

MARK/LABEL

Marking Presentations

- Mark all slides top and bottom as you would any other document containing CUI except when the presentation is comingled with classified.
- Front cover must have the CUI Designation Indicator block.
- Classified briefings that contain CUI must have both the classification block, and CUI Designation Indicator block.
- Any warning boxes or distribution statements required by a Law, Regulation, or Government-wide policy (LRGWP).
- Alternate acceptable placement of “CUI” in top and bottom corners.

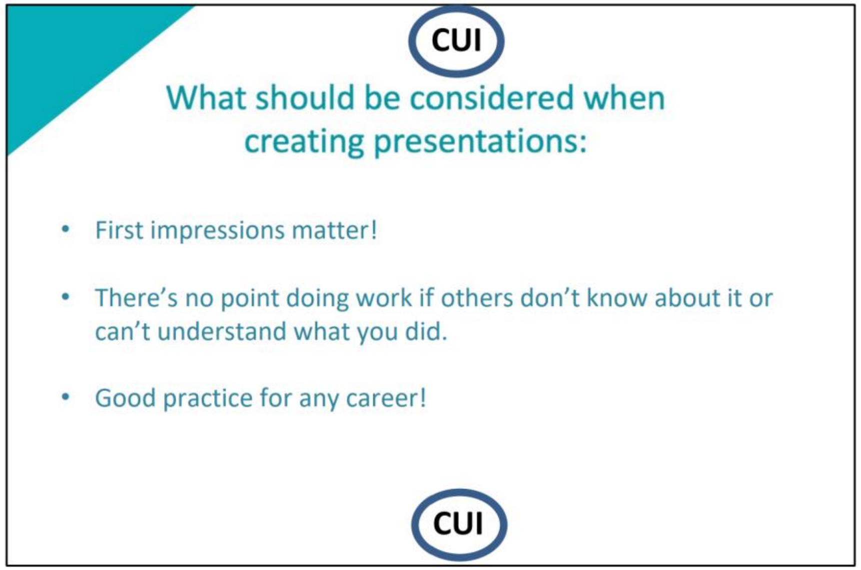


CUI

PowerPoint Presentation Tips

Controlled by: OUSD(I&S)
Controlled by: CL&S INFOSEC
CUI Category(ies): PRVCY
Limited Dissemination Control: FEDCON
POC: John Brown, 703-555-0123

CUI



CUI

What should be considered when creating presentations:

- First impressions matter!
- There’s no point doing work if others don’t know about it or can’t understand what you did.
- Good practice for any career!

CUI

MARK/LABEL

Marking Media

- Removable media and storage devices containing CUI must be marked.
- Standard Form 902 (stickers) are available through GSA for purchase but only the Government can order them. Find out more here.
- You can also create your own stickers. Find out more here.
- It is recommended you always engage with your **GCA** for additional guidance on what is required to be marked for your program (systems, materials etc.).
- **References:**
  - DOD CUI Web Page: Home (dodcui.mil)
  - DOD CUI Marking Guides:
    - OUSD(I&S)/DDI(CL&S) Controlled Unclassified Information Marking Aid
    - CUI Awareness and Marking

This system contains CUI
This Medium is
CUI
U.S. Government Property
Protect it from unauthorized disclosure in compliance with applicable executive orders, statutes, and regulations.

MARK/LABEL

Other Marking Considerations

- Once you start marking a document, the entire document must be marked with the banner markings.
- CUI Category Marking is mandatory for CUI Specified.
- The below warning statement will be placed at the bottom of the first page of multi-page documents alerting readers to the presence of CUI in a classified DoD document.

> *"This content is classified at the [insert highest classification level of the source data] and may contain elements of controlled unclassified information (CUI), unclassified or information classified at a lower level than the overall classification displayed. This content shall not be used as a source of derivative classification; refer instead to the [cite specific reference, where possible, or state the applicable classification guide(s)]. It must be reviewed for both Classified National Security Information (CNSI) and CUI in accordance with DoD 5230.09 prior to public release."* [Add a point of contact when needed.]

DO NOT

- **Insert CUI in the banner line for classified documents.**
- **Spell out CUI categories.**

CUI may be stored in NIST 800-171 compliant Non-Federal information systems or controlled physical environments.

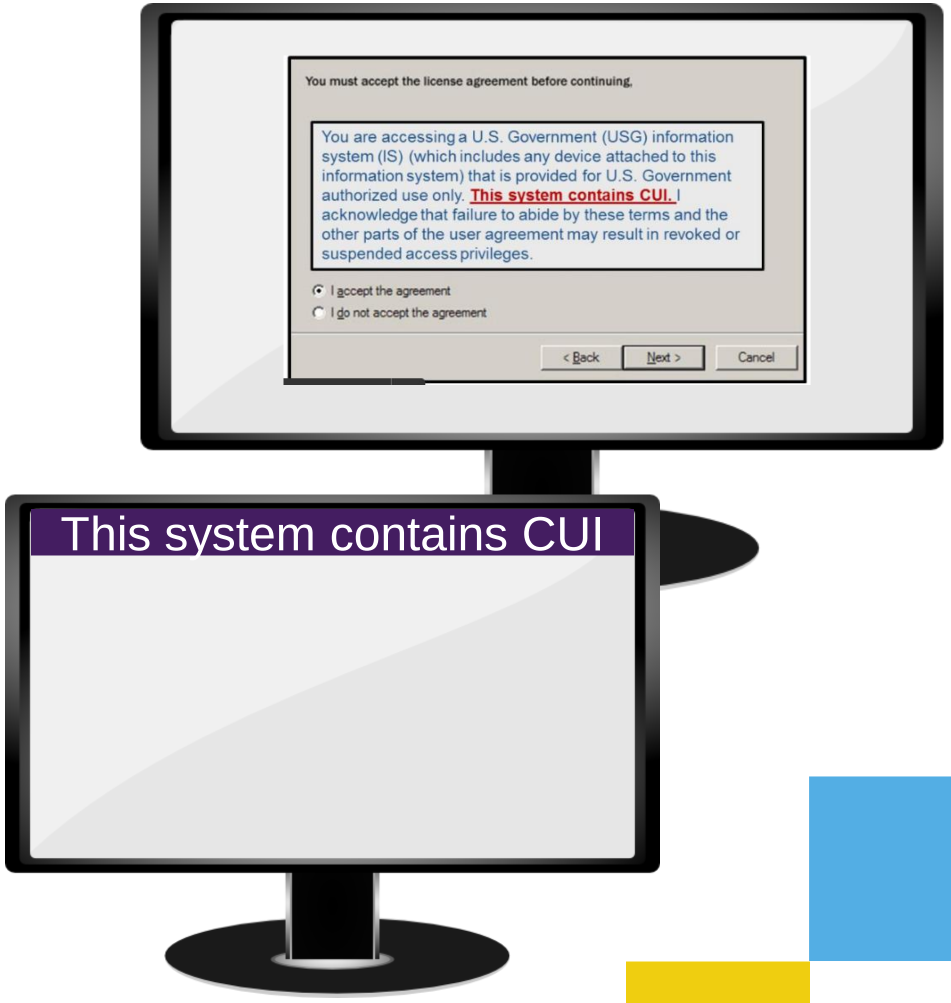
STORE

System Storage

Per the DoDI 8500.01:

> *“Systems processing CUI will be categorized at no less than the moderate confidentiality impact level in accordance with Part 2002*
> *of Title 32, Code of Federal Regulations (Reference (z)).”*

- Always engage with your **GCA** for CMMC implementation level and additional safeguarding requirements.
- It is recommended at the minimum to include a “splash screen” users must agree to before logging into system or using stickers/banners.
- The NIST SP 800-171 governs and protects CUI on non-Federal Information Systems.
- Here is a CUI POAM template and a CUI SSP template.



You must accept the license agreement before continuing.

You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government authorized use only. **This system contains CUI.** I acknowledge that failure to abide by these terms and the other parts of the user agreement may result in revoked or suspended access privileges.

● I accept the agreement
○ I do not accept the agreement

STORE

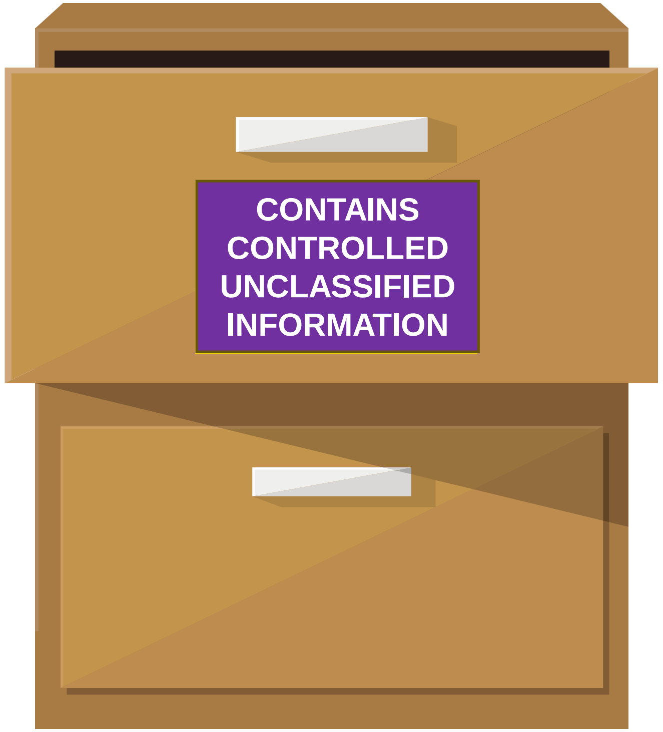
Physical Storage

During Working Hours

- **Personnel must take care not to expose CUI to unauthorized users** or others who do not have a lawful government purpose to see the information.
- **CUI cover sheets (optional) may be placed on top of documents** to conceal the contents from casual viewing.
- **Always control or protect CUI with at least one physical barrier** and take reasonable care to ensure that the information is protected from unauthorized access and observation.

After Working Hours

- **Store in unlocked containers, desks, or cabinets only if facility provides continuous monitoring.** If not, CUI must be in a locked desk, file cabinet, locked room or where security measures are in place to prevent or detect unauthorized access.
- **Locked container should indicate it contains CUI**.
- **Do Not store CUI in public areas** (car, home office etc.) or view while on public transportation.



CUI is limited to those with a lawful Government purpose.

A lawful Government purpose is any activity, mission, function, operation, or endeavor that the U.S. Government authorizes or recognizes as within the scope of its legal authorities or the legal authorities of non-executive branch entities (such as state and local law enforcement).

DISSEMINATE

Sharing CUI

IN PERSON

- Ensure you are in a controlled area where you cannot be overheard, recorded etc.

ELECTRONIC TRANSMISSION

- Must apply "CUI" to top/banner and bottom/footer.
- **Must be encrypted.**
- Must contain a CUI *Designation Indicator* block.
- If including attachments containing CUI, file name must indicate it includes CUI.
- DO NOT USE PERSONAL EMAIL to transmit CUI.
- There are available Secure File Transfer Protocol (SFTP) sites (i.e. SAFE site). Always check with your customer on which sites you are able to use.

FAX

- Sender is responsible for determining appropriate protections are in place at the receiver end and Fax machine is located in a controlled government facility. Sender should contact receiver to inform them CUI is being transmitted.

MAIL

- May be transmitted via first class mail, parcel post, or bulk shipments. Do not place CUI markings on the outer envelopes or packaging when mailing.
- Address packages that contain CUI for delivery only to a specific recipient.
- DO NOT put CUI markings on the outside of an envelope or package for mailing/shipping.
- Remember to track the package.

When to share CUI?
When access promotes a common project or operation between agencies or under a contract or agreement with the designating agency, then share!

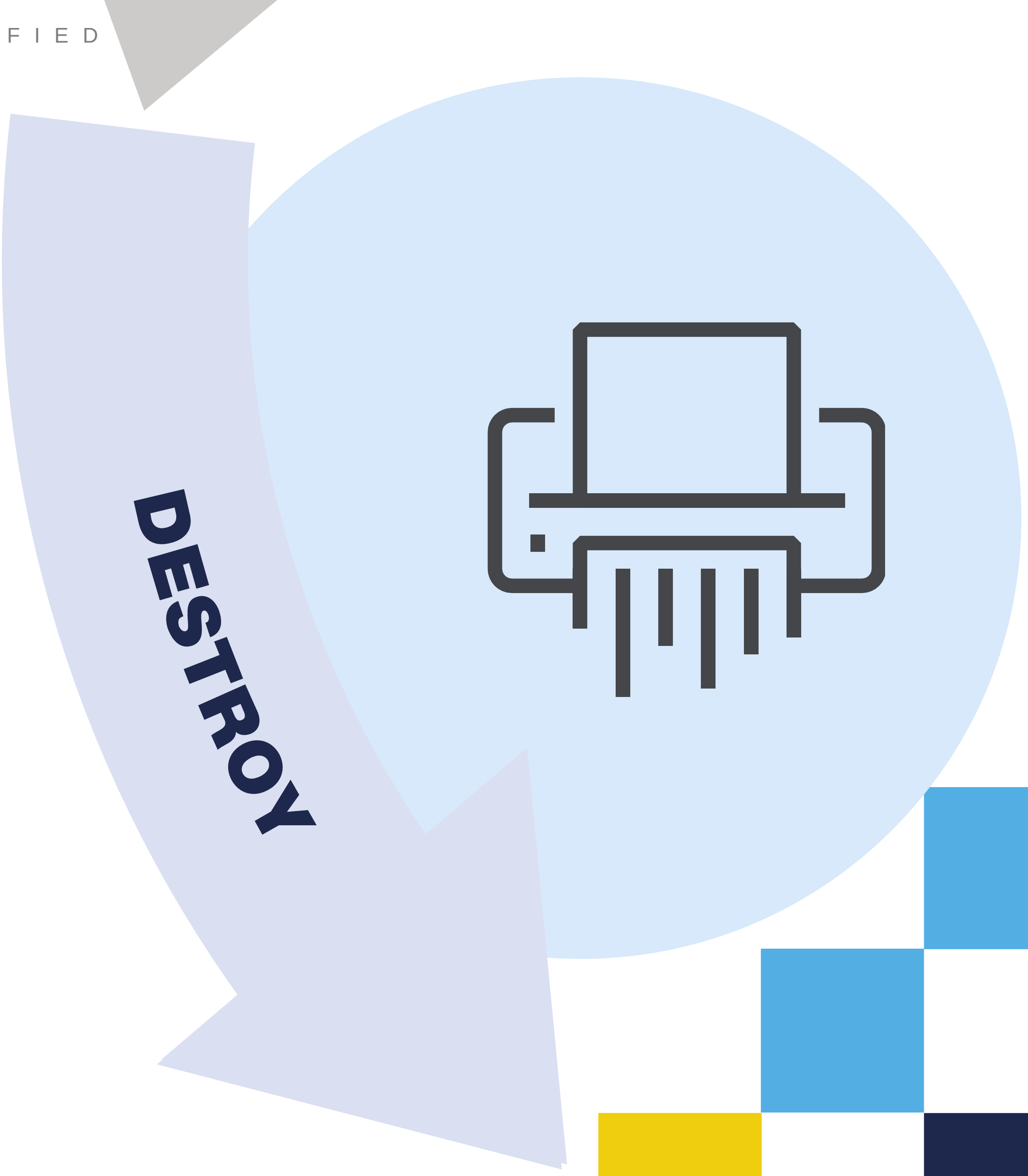
When NOT to share CUI?
If access harms or inhibits a common project or operation between agencies or under a contract or agreement with the designating agency, then do not share.

CUI should be destroyed or decontrolled whenever possible to reduce risk of exposure to unauthorized individuals.

Employees and contractors should contact the **Authorized Holder** to discuss decontrolling (downgrading) the CUI material when the need arises.

Triggers to request decontrol may include:

- Request to release the CUI material to the public
- End of contract
- Contract Renewal



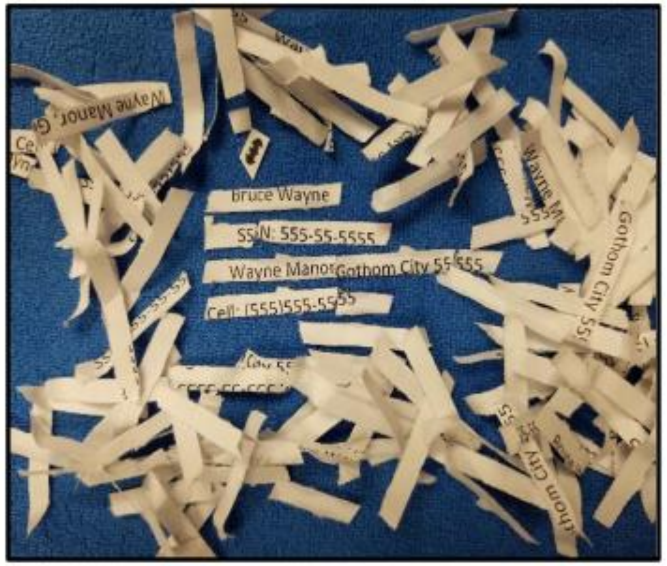
DESTROY

DESTROY

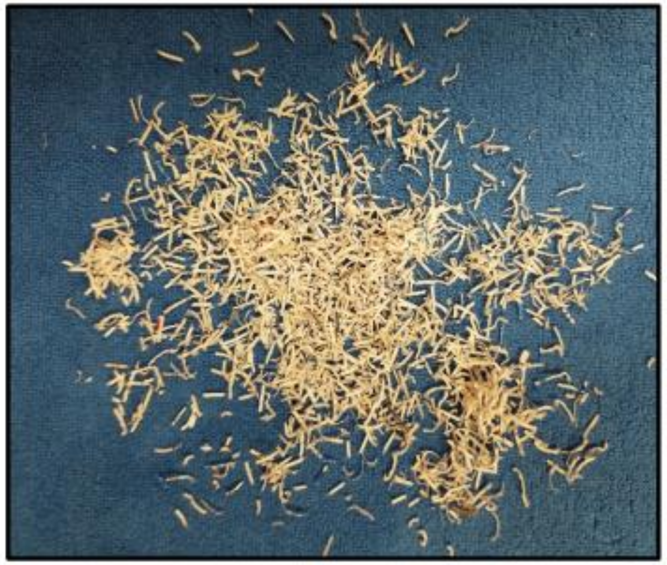
Shredding

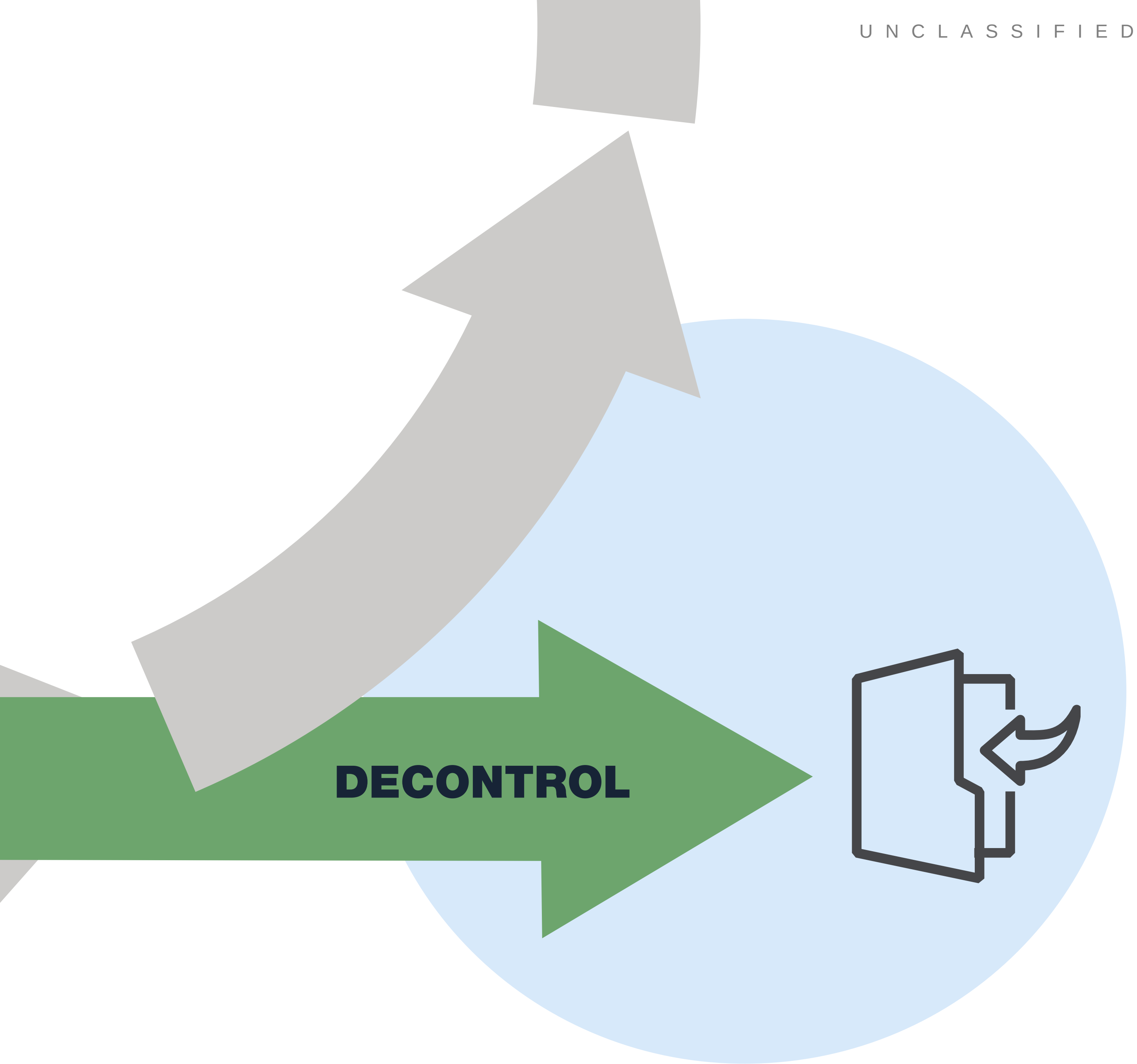
- When you are finished with paper CUI, per the ISOO Notice, CUI must be destroyed using a cross-cut shredder that produces particles less than 1mm by 5mm. For companies that have classified, shred machines used to shred classified meet this requirement.
- If you are utilizing a third-party shred company (i.e., ShredIT®), as long as you can prove the company is recycling the material to make it unreadable after it shreds (no matter the size of the shred), this also meets the requirement.

NOT APPROVED



APPROVED





The originator or other competent authority will terminate the CUI status of specific information when the information no longer requires protection from public disclosure.

- Decontrolling occurs when the originator of the CUI material removes safeguarding or dissemination controls from CUI that no longer requires such controls.
- CUI documents and materials must be formally reviewed in accordance with DoDI 5230.09 *before* being decontrolled or released to the public.

UNAUTHORIZED DISCLOSURE (UD)/ FAILURE TO PROTECT

- The 32 CFR 2002 states “Unauthorized disclosure occurs when an authorized holder of CUI intentionally or unintentionally discloses CUI without a lawful Government purpose, in violation of restrictions imposed by safeguarding or dissemination controls, or contrary to limited dissemination controls.”
- Failure to properly mark, control, and protect CUI falls underthe personnel security adjudicative guideline of “Handling Protected Information.”
- The misuse, mishandling, or unauthorized disclosure of CUI is to be reported to the designated official at the worksite and the Security Manager or company Facility Security Officer (FSO).
- These rules apply to both cleared and uncleared personnel that access CUI as part of their job performance.
- 5200.48 – 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 will be informed of any UD.”

WRAP UP

1. National Security is affected by the loss of CUI and we must protect it.
2. **The FIRST thing you should do is work with the originator (customer, prime, agency, GCA, etc.)** to validate contractual CUI requirements.
3. Understanding of the DoD registry and CUI safeguarding requirements, applicable laws, regulations and government wide policies are paramount. Get familiar with them!
4. Stay in the know! Continue to look for updates to the CUI program.
5. Failure to comply with CUI requirements may result in administrative or criminal sanctions, fines, and penalties.

REFERENCES

Registries and Source Documents

- NARA CUI Registry https://www.archives.gov/cui
- DoD CUI Registry https://www.dodcui.mil
- Executive Order 13556 – Controlled Unclassified Information
- DoDI 5200.48 (Controlled Unclassified Information)
- DFARS 252.204-7012 clause
- Coversheets, stickers and more!
- 32 CFR 2002 CUI Final Rule NARA

IT/Systems

- DODI 8500.01 (Cybersecurity)
- NIST 800-171 (CUI on nonfederal systems)
- NIST 800-172 - Enhanced Security Requirements for CUI

CMMC

- OUSD A&S CMMC Site
- CMMC Accreditation Body (CMMC-AB) https://www.cmmcab.org
- CMMC Home Page https://www.acq.osd.mil/cmmc/draft.html

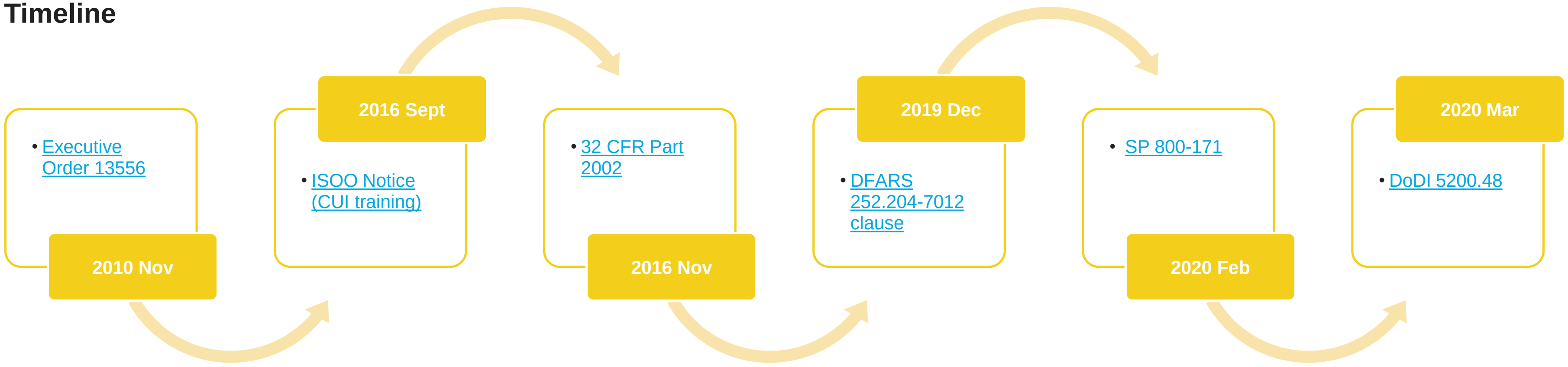
Training Materials

- https://www.dcsa.mil/mc/ctp/cui/
- https://www.archives.gov/cui/training.html
- https://www.dodcui.mil/Home/Training/
- CUI quick reference guide

Coversheets

- https://www.gsa.gov/forms-library/controlled-unclassified-information-cui-coversheet-0
- https://www.archives.gov/cui/additional-tools

Timeline



2010 Nov
- Executive Order 13556

2016 Sept
- ISOO Notice (CUI training)

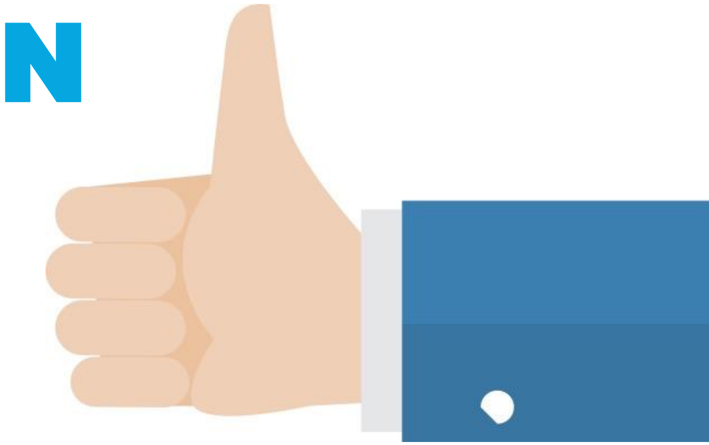
2016 Nov
- 32 CFR Part 2002

2019 Dec
- DFARS 252.204-7012 clause

2020 Feb
- SP 800-171

2020 Mar
- DoDI 5200.48

CERTIFICATE OF COMPLETION



If you have any questions, concerns, or require assistance, please contact:

[ENTER ORGANIZATION/COMPANY NAME]Security Manager/Facility Security Officer.

We are here to help you and ensure that [**ENTER ORGANIZATIONCOMPANY NAME]** remains compliant with CUI requirements.

Organization/Company Name: [ENTER NAME]

Security Manager/FSO Name: [ENTER NAME]

Security Manager/FSO Email Address: [ENTER EMAIL]

Security Manager/FSO Phone Number: [ENTER PHONE]

Your name: ______________________________

Signature: _______________________________

Date: ___________________________________