Controlled Unclassified Information (CUI) Training Template

These training slides are a resource that DOD and Industry can use to provide to personnel required to complete CUI Training.

IMPORTANT!

The FIRST thing you should do BEFORE working with CUI is to WORK WITH THE INFORMATION OWNER (IO) (customer, prime, agency, GCA etc.) to validate CUI requirements.

Always obtain clear, written verification and guidance on how to receive, handle, store material under your contract/customer (i.e., CUI marking guide).

Work with the **Defense Counterintelligence Security Agency (DCSA)** to assist with guidance if you are unable to obtain from the IO.

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

Content

- Introduction
- Why?
- Previous Markings
- How and Who Decides?
  - 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 agency developed its own practices for sensitive unclassified information, resulting in a patchwork of systems.
- The Controlled Unclassified Information (CUI) program represents an unprecedented initiative to standardize practices.

Why CUI Training?

CUI training is conducted **ANNUALLY** and, at a minimum, must include the following items (per CUI Notice 2020-01 and 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;
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 training categories, but Industry may instead use this training to meet the requirement:
DOD CDSE course https://securityawareness.usalearning.gov/cui/index.html

Previous/Legacy Markings

1. **FOUO as a marking identification is no longer to be utilized**.
    - Engage with Information Owners 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 Information Owner (IO) 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 IO reviews the information** to determine if the data meets the CUI requirements and re-marks this data accordingly.

Legacy Distribution Statements

Legacy CUI technical documents and materials have used distribution statements in order to address the shared responsibility between the DOD and its contractor to safeguard this information. This was done for legacy CUI creation, transmission, receipt, storage, distribution, decontrol, and approved disposition authorities, including destruction.

How Do They Decide?

There is a registry for that!

There are **TWO** registries. Determining which registry to use depends on the owner of the information. The Information Owner (IO) of the CUI must consult the appropriate registry to find the indexes and categories used to identify the various types of CUI.

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

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

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

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

CATEGORIES OF CUI

For information to be considered CUI, it must fall within a category, such as:

- Critical Infrastructure
- Defense
- Export Control
- Financial and Tax
- Immigration
- Intelligence
- International Agreements
- Law Enforcement
- Legal
- Natural and Cultural Resources
- NATO
- Nuclear
- Patent
- Privacy
- Procurement and Acquisition
- Proprietary Business Information
- Provisional *(for DHS use only)*
- Statistical
- Transportation

Who Decides?

The **Information Owner (IO)** 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 IO is responsible for applying the appropriate CUI markings and dissemination controls accordingly.

Information Owners include:

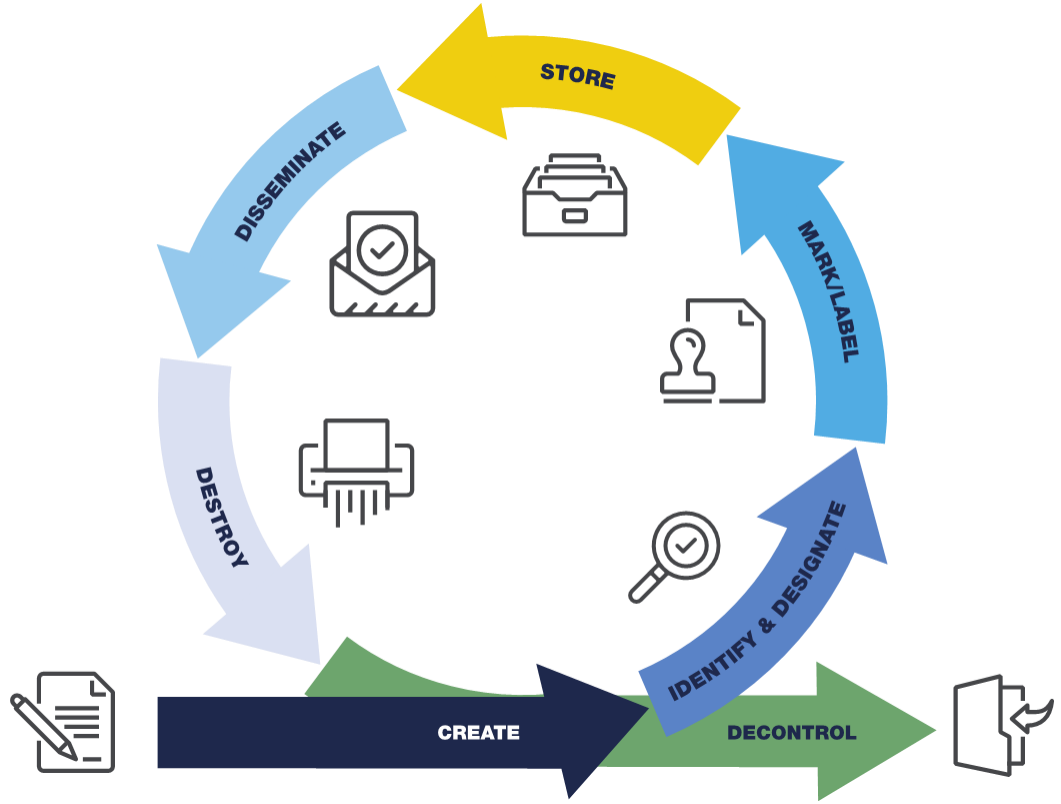
- DOD civilian and military personnel
- Agencies
- Contractors providing support to the DOD pursuant to contractual requirements

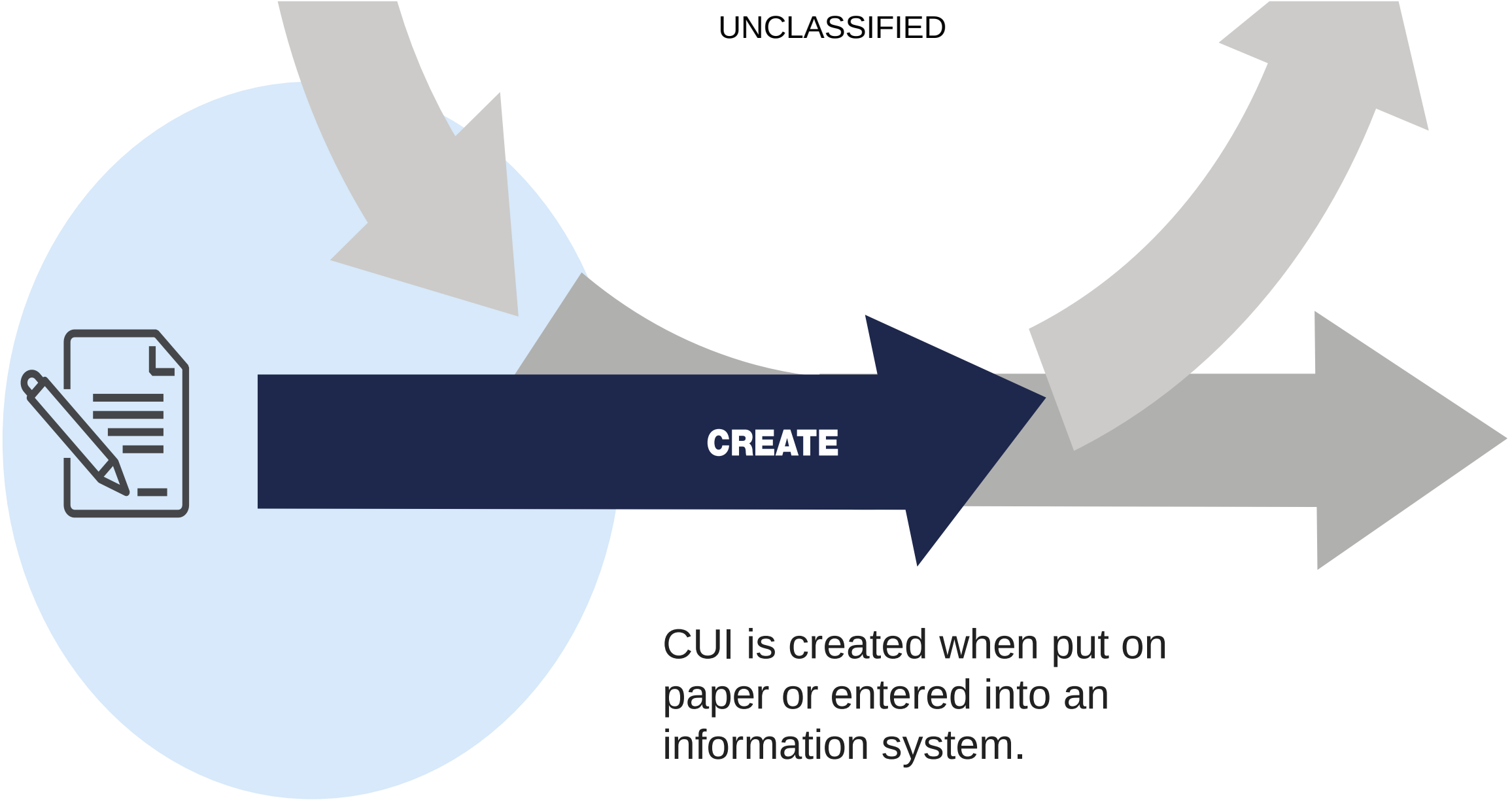
CUI Lifecycle

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

Whenever CUI is distributed, the **Information Owner** shall ensure who they are distributing to has the proper controls for receiving and protecting CUI.

However, it is everyone's responsibility to identify if they receive CUI and handle accordingly.





CUI is created when put on paper or entered into an information system.

What is CUI?

- **CUI is generally government-created or owned information** that requires safeguarding or dissemination controls consistent with applicable laws, regulations and government wide policies.
- **Anyone can be an Information Owner** and create CUI as long as it is generated for, or on behalf of, an Executive Branch agency under a contract and it falls into one of the over one hundred DOD CUI categories. However, in most situations, Industry will be guided by its customer (the Information Owner) on what is CUI and what isn't.
- **CUI is not a classification** and should not be referred to as "classified as CUI." A better way to phrase it is "designated as CUI."
- **CUI is not corporate intellectual property**, unless created for or included in requirements related to a Government contract. Contractors should consult with their Government Contracting Activity (GCA) to make this determination.
- **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 ***cannot 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.

Receiving CUI

Creating 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 52.204-21defines 15 specific safeguarding controls to protect FCI.
- 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-D041Interim DFARS rule imposed new requirements.
- Contractors working with CUI must now conduct an internal self-assessment based on NIST SP 800-171.
- Contractors must upload their assessment scores into the Supplier Performance Risk System (SPRS). Before making an award, contracting officers now have to verify 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 within Plan of Action and Milestones (POAM).
- Cybersecurity Maturity Model Certification (CMMC) Info:
  - https://www.acq.osd.mil/cmmc/faq.html
  - Cybersecurity Maturity Model Certification (dodcui.mil)

The **Information Owner (IO)** of the CUI material is responsible for marking the material before distributing so that anyone receiving the CUI can properly identify it.

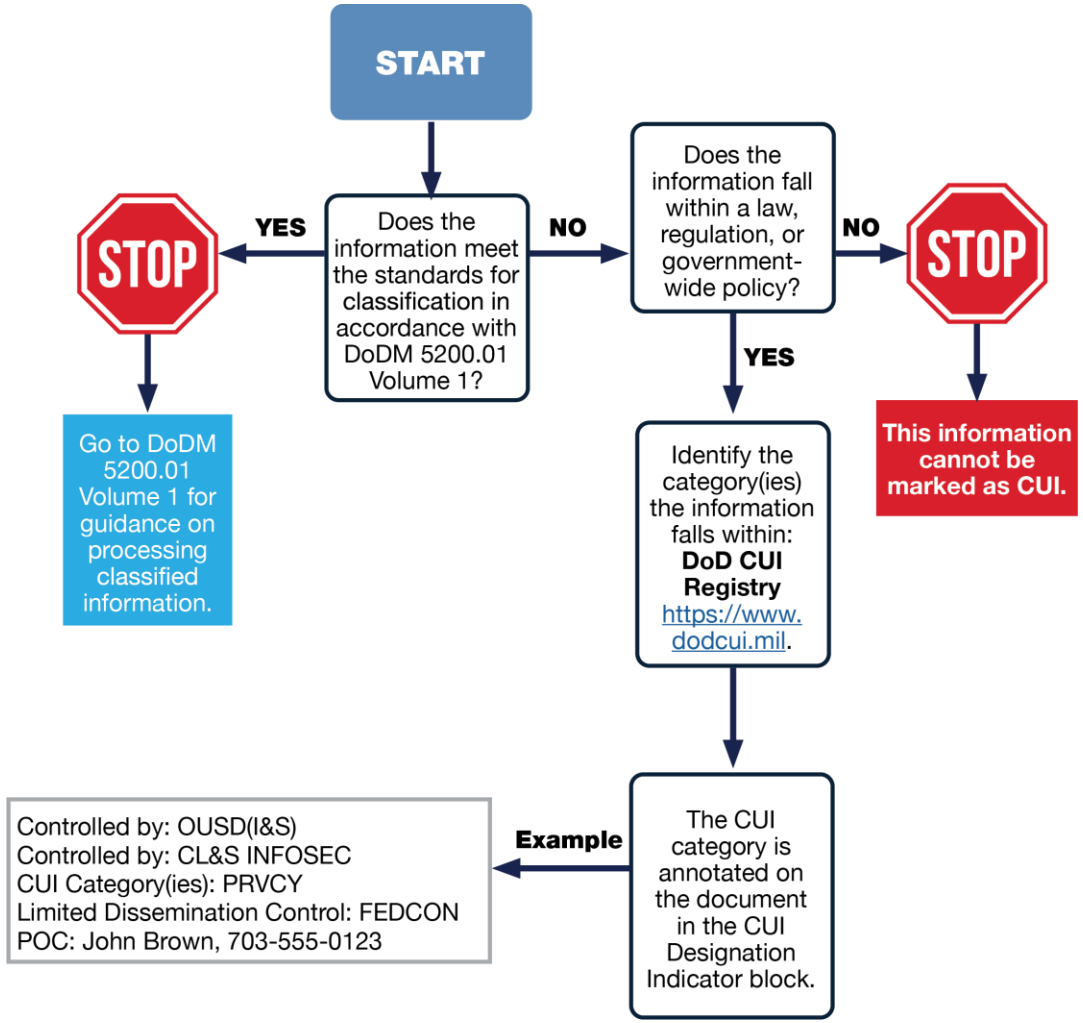
Identify & Designate

Identification

- The identification of CUI is critical in determining what sensitive information needs to be protected.
- CUI is generated for or on behalf of an agency within the Executive Branch under a contract and determines if the information falls into one of the more than one hundred categories of CUI in the National CUI Registry.

WHAT IS *NOT* CUI?

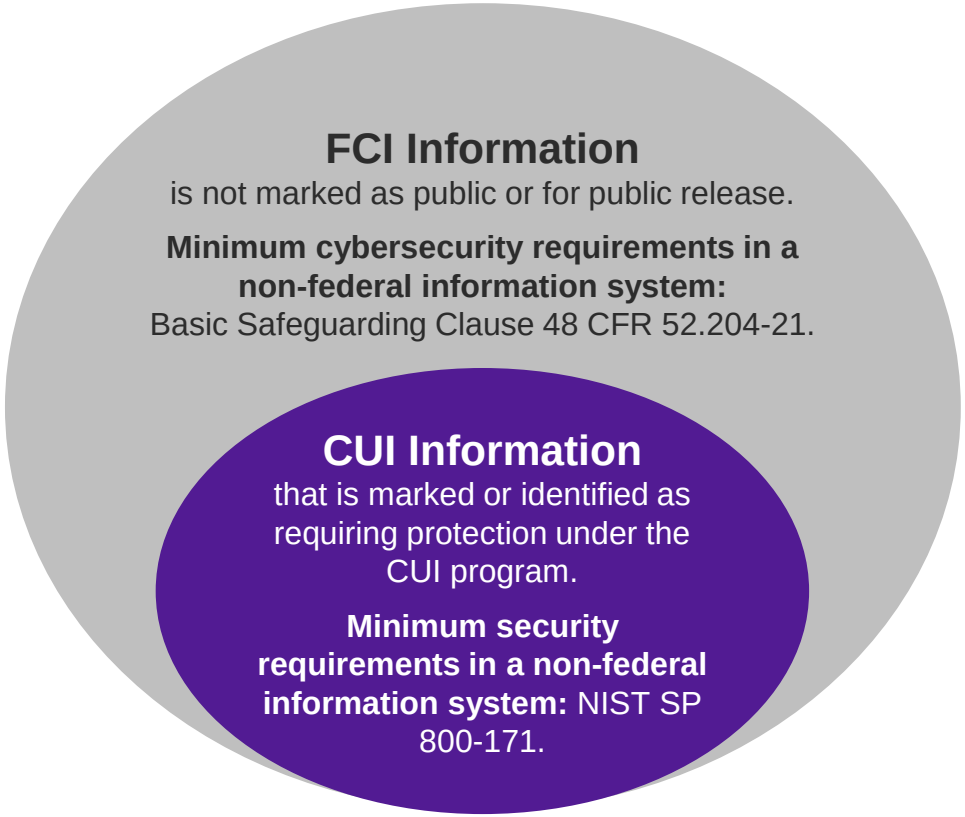
- Classified information or a classification
- Corporate intellectual property (unless created for or included in requirements related to a government contract)
- Publicly available information



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.



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” or “CONTROLLED” in the banner of the document.

Mark/Label

Marking Documents

Required

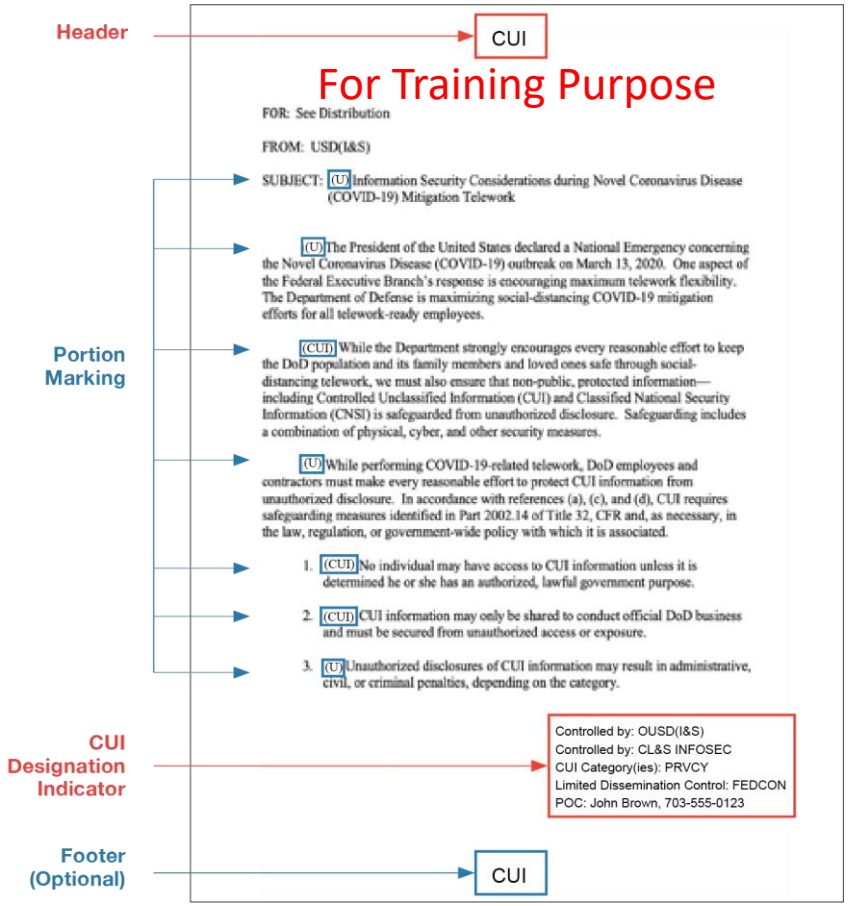
- Header/top/banner of document has “CUI” or “CONTROLLED” in bold letters
- ***Designation Indicator (5 items)***

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
- Bottom/footer marking (but highly recommended!)
- 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** to go in the banner line as they are not an authorized CUI category used to control information. Supplemental markings can be placed outside the banner line if approved by the **Information Owner (IO)**.



CUI Banner Marking

These are preceded by a double forward slash (//) to separate them from the rest of the CUI banner marking. When a document contains multiple Limited Dissemination control markings, those Limited Dissemination control markings must be alphabetized and separated from each other with a single forward slash (/).

Example of CUI banner marking

CUI CONTROL MARKING	CUI CATEGORY MARKING (If required)	Limited Dissemination

CUI OR CONTROLLED//CATEGORIES//SUBCATEGORIES//DISSEM

Example of CUI banner marking includes all Specified and Dissemination markings from throughout document

CUI	CUI CATEGORY MARKING (If required)	LIMITED DISSEM

CUI//SP-SPECFIED-A/SP-SPECIFIED-B//DISSEM

Designation Indicator

Mark/Label

- 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 the Navy building Flying Squirrels. #1 would be NAVY but the #2 might be "Secret Division of Flying Squirrels." 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.

**GCA: Government Contracting Authority* **IO: Information Owner*

The designation indicator ***must include*** these five items.

1. **Name (Who owns this?)**
   Insert the name of the DoD component (GCA/IO) if not otherwise identified in the letterhead.
   This is typically the Information Owner.
2. **Controlled By (Who controls this?)**
   Insert the name (GCA/IO) of the office creating the document and making the CUI determination CUI.
3. **Category (Is this 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.

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

Limited Dissemination Control Markings
(Part of Designation Indictors)

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

Limited Dissemination Control Markings
(Part of Designation Indictors)

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 LDCM 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.
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.

Updated December 28, 2021

"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 5203.09 and DODI 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

Mark/Label

CUI with 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.

Emails with CUI

Mark/Label

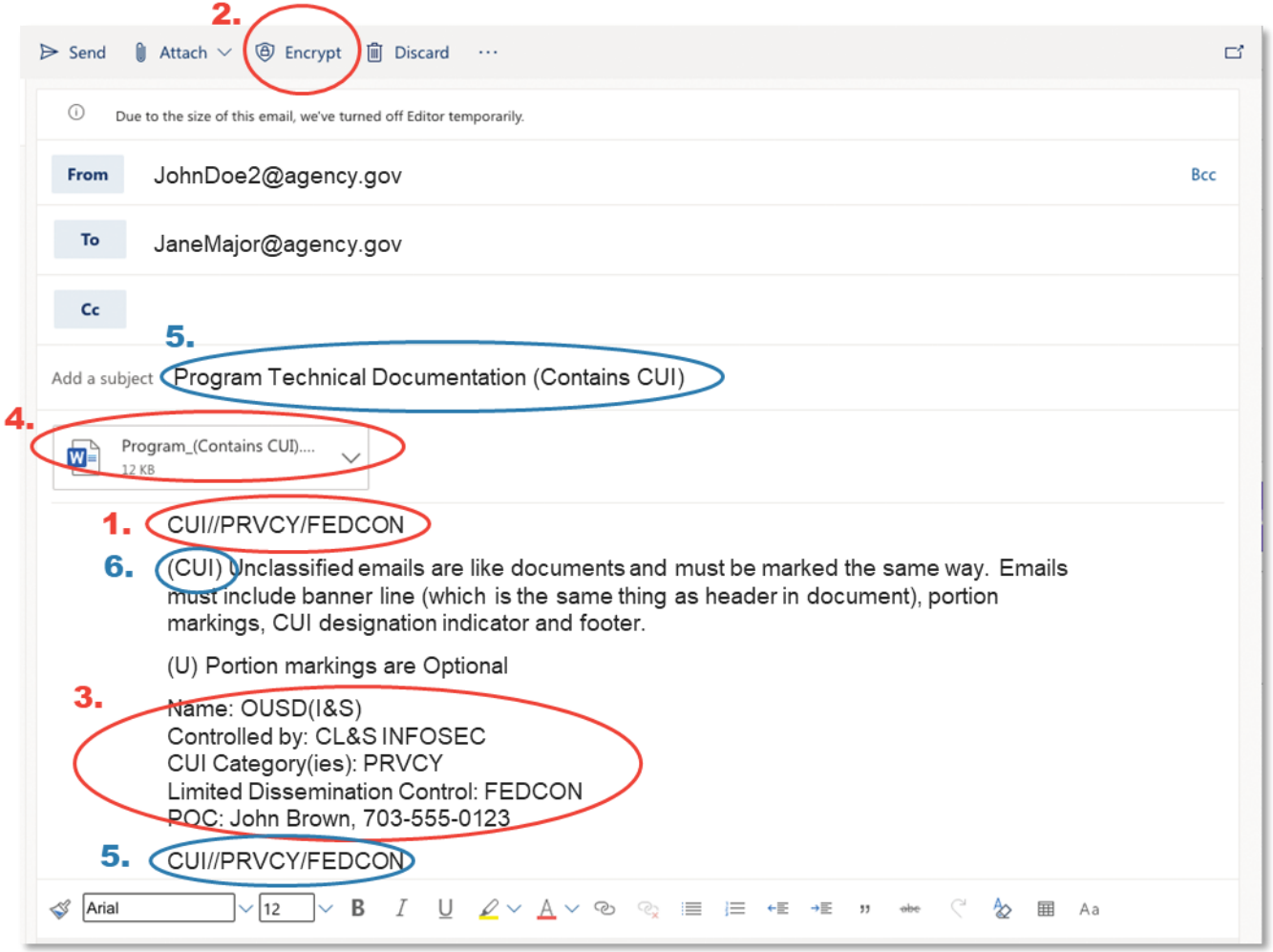
Required

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, file name must indicate it includes CUI.

Optional but best practice

5. Apply “CUI” to footer and subject line.
6. All paragraphs known to contain CUI may be portion marked.

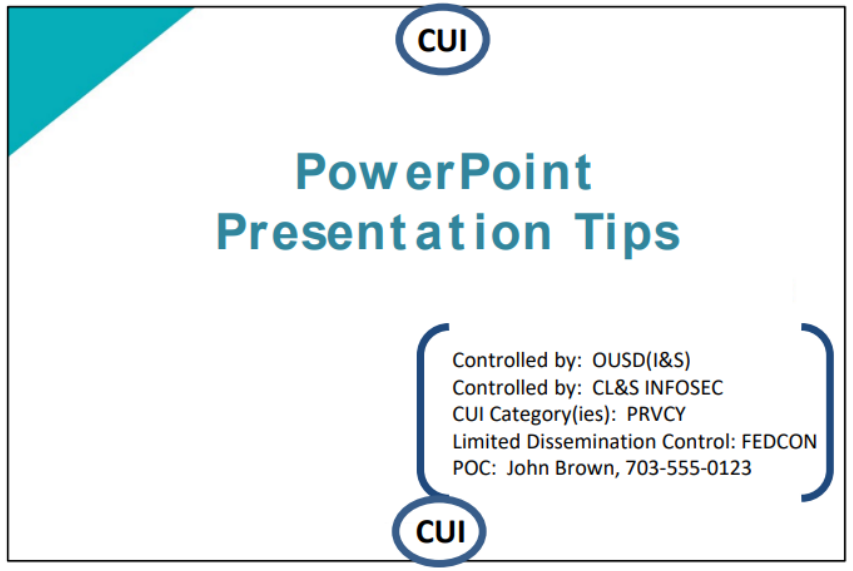
DO NOT USE PERSONAL EMAIL ACCOUNTS to send CUI. This is necessary to ensure proper accountability for Federal records and to facilitate data spill remediation.



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,
- Alternate acceptable placement of “CUI” in top and bottom corners.



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.
- It is recommended you always engage with your **Information Owner** for additional guidance on what is required to be marked for your program (systems, materials etc.).

References:

- ISOO marking guidebook for more information https://www.archives.gov/files/cui/20161206-cui-marking-handbook-v1-1.pdf
- 32 CFR 2002 https://www.federalregister.gov/documents/2016/09/14/2016-21665/controlled-unclassified-information

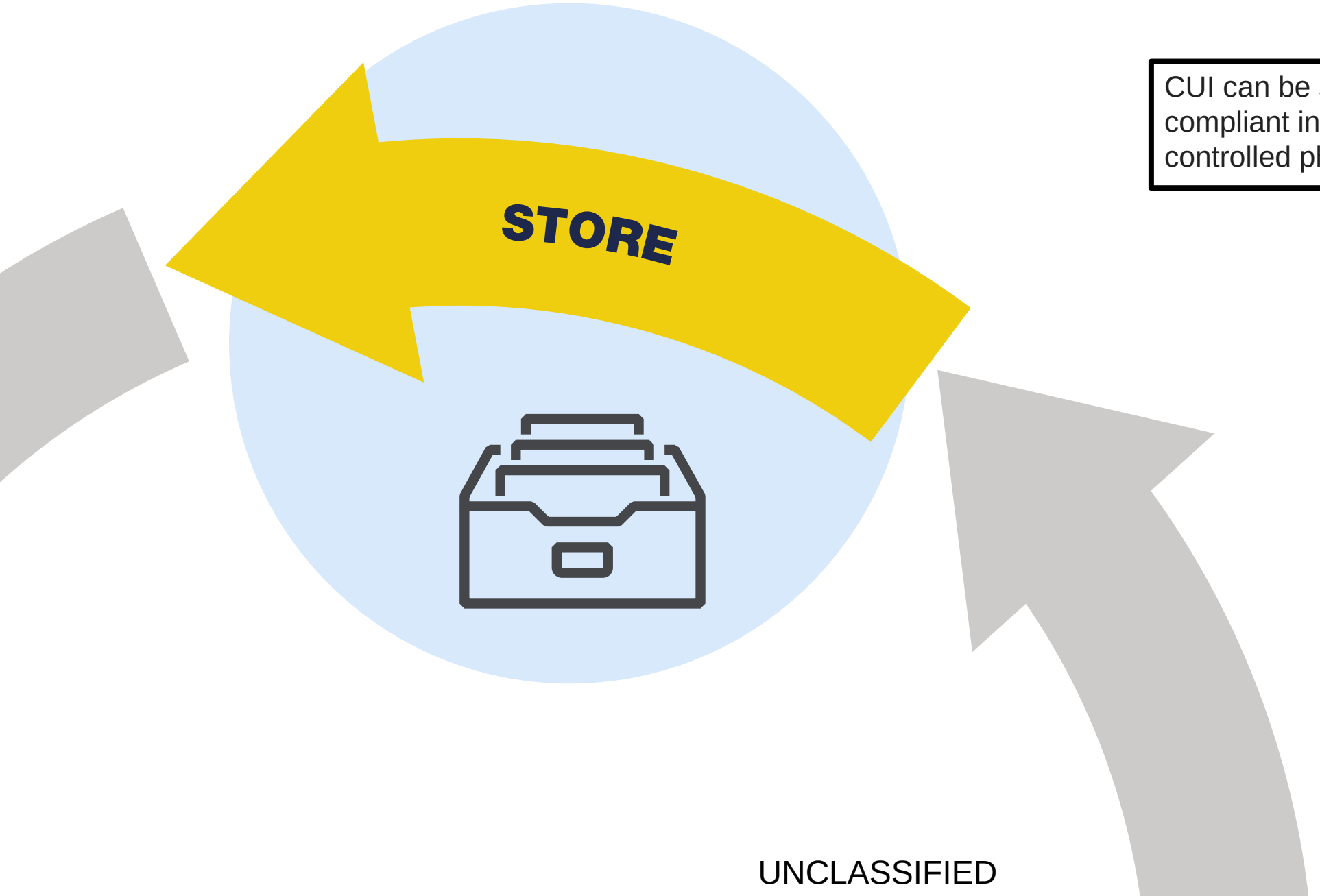
Other Marking Considerations

- 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. Use only DOD-approved abbreviations for the CUI categories.**



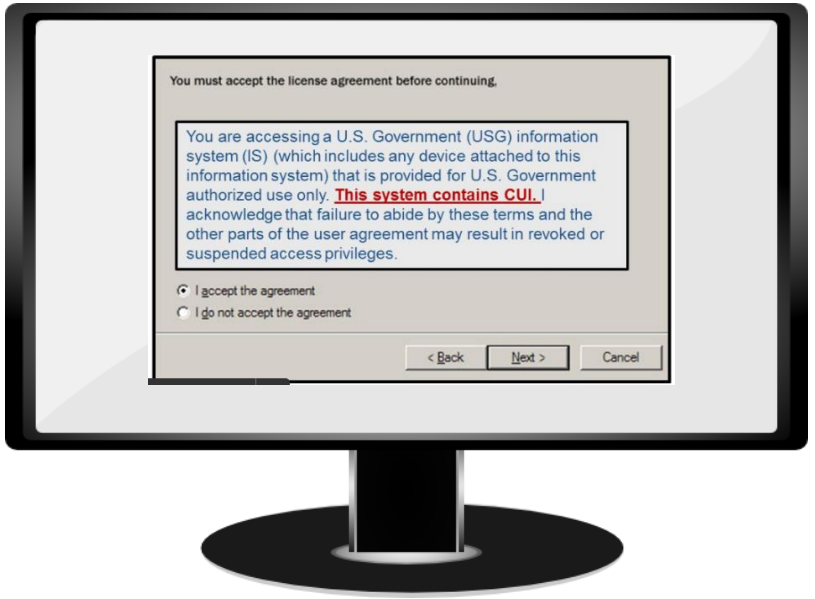
CUI can be stored in NIST SP 800-171 compliant information systems or controlled physical environments.

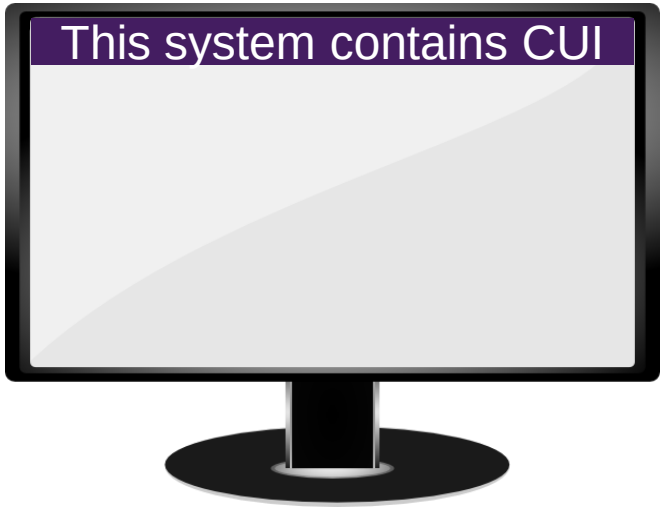
System Storage

Per DODI 8500.01 (Cybersecurity:

"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 **Information Owner** for additional requirements.
- It is recommended at the minimum to include a "splash screen" users must agree to before logging into system or using stickers/banners.
- NIST SP 800-171 governs and protects CUI on non-Federal Information Systems.





Physical Storage

During Working Hours

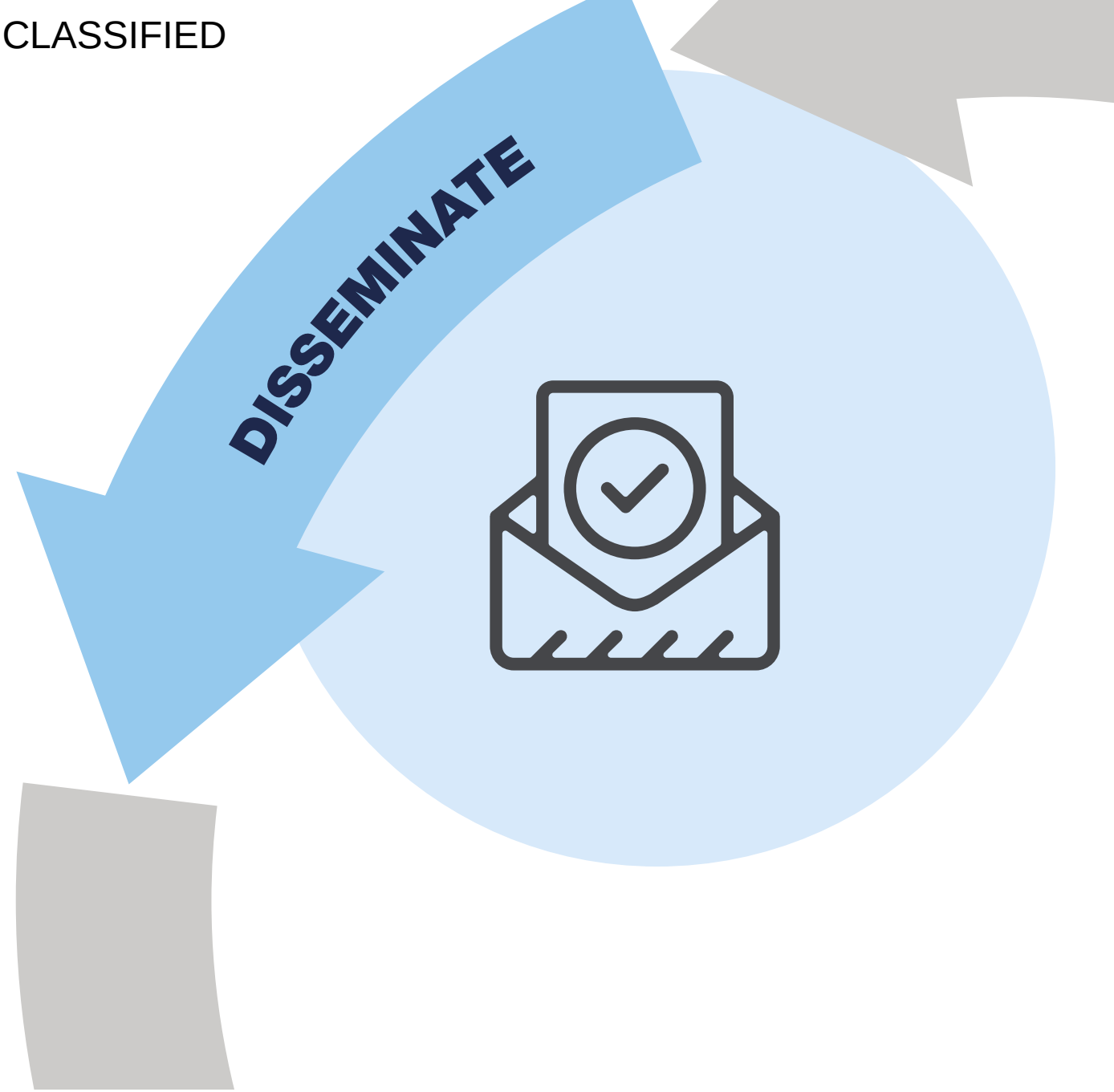
- **Personnel must take care not to expose CUI to unauthorized users** or others who do not have a lawful government purpose to see the information.
- **CUI cover sheets (not required) may be placed on top of documents** to conceal the contents from casual viewing.
- **Always control or protect CUI with 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).



Sharing CUI

Disseminate

IN PERSON

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

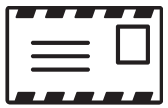
ELECTRONIC TRANSMISSION

- Must apply “CUI” to top/banner.
- **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?

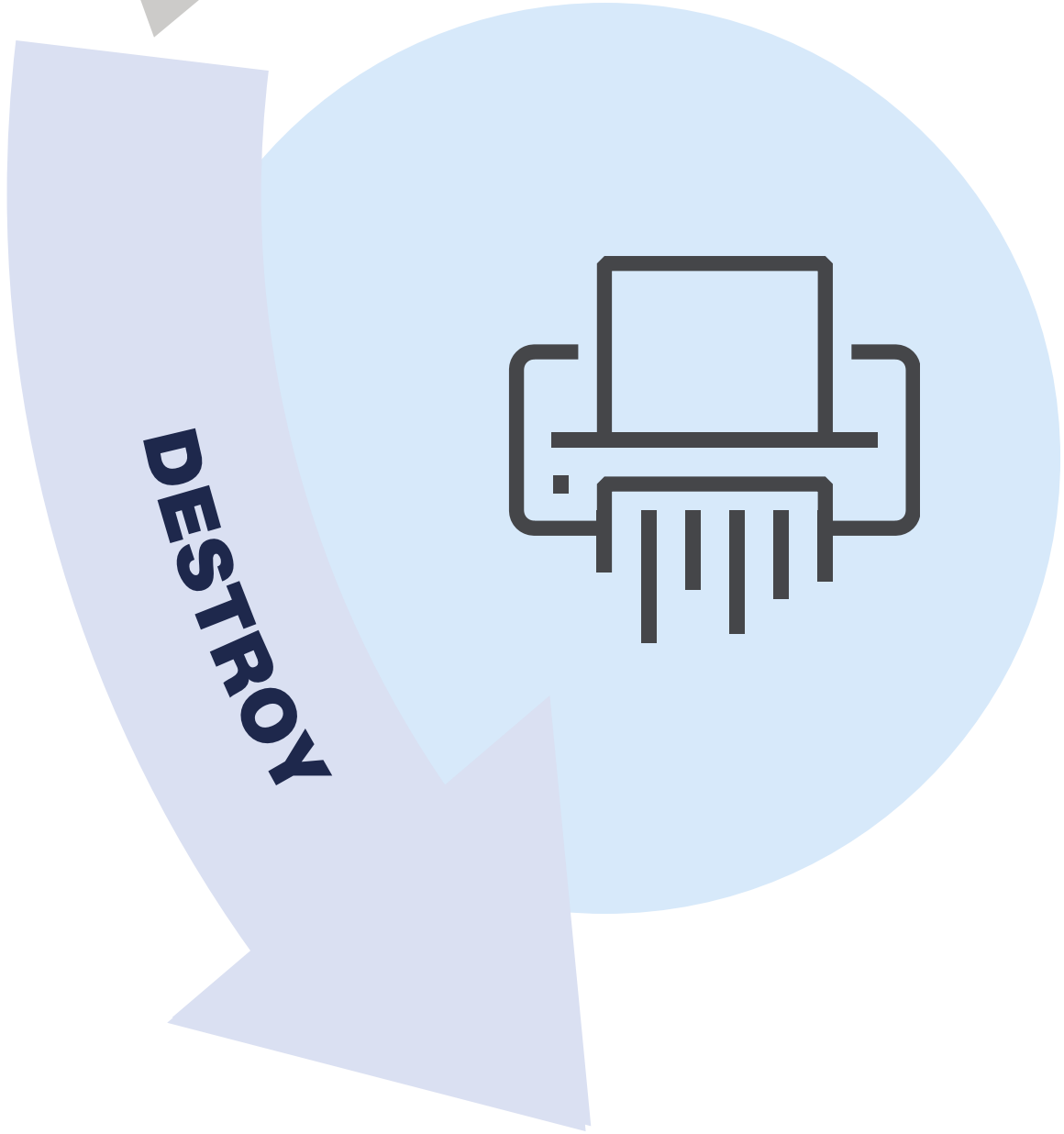
If access harms or inhibits a common project or operation between agencies or under a contract or agreement with the designating agency, then do not share.

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

Employees and contractors should contact the **Information Owner** 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

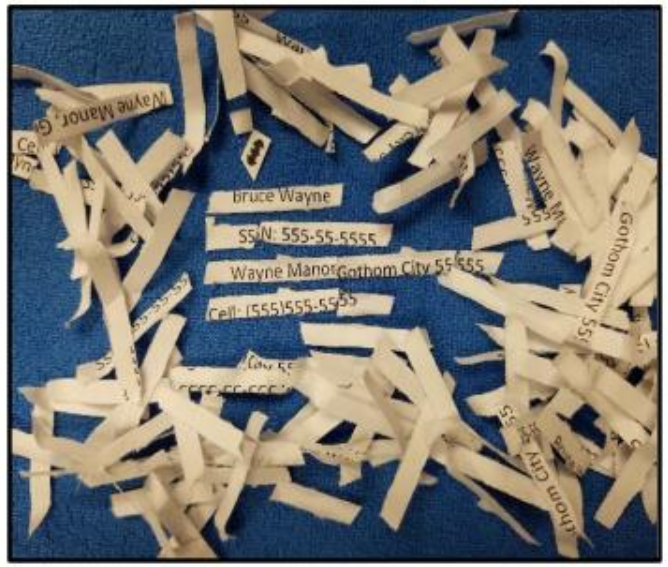


Destroy

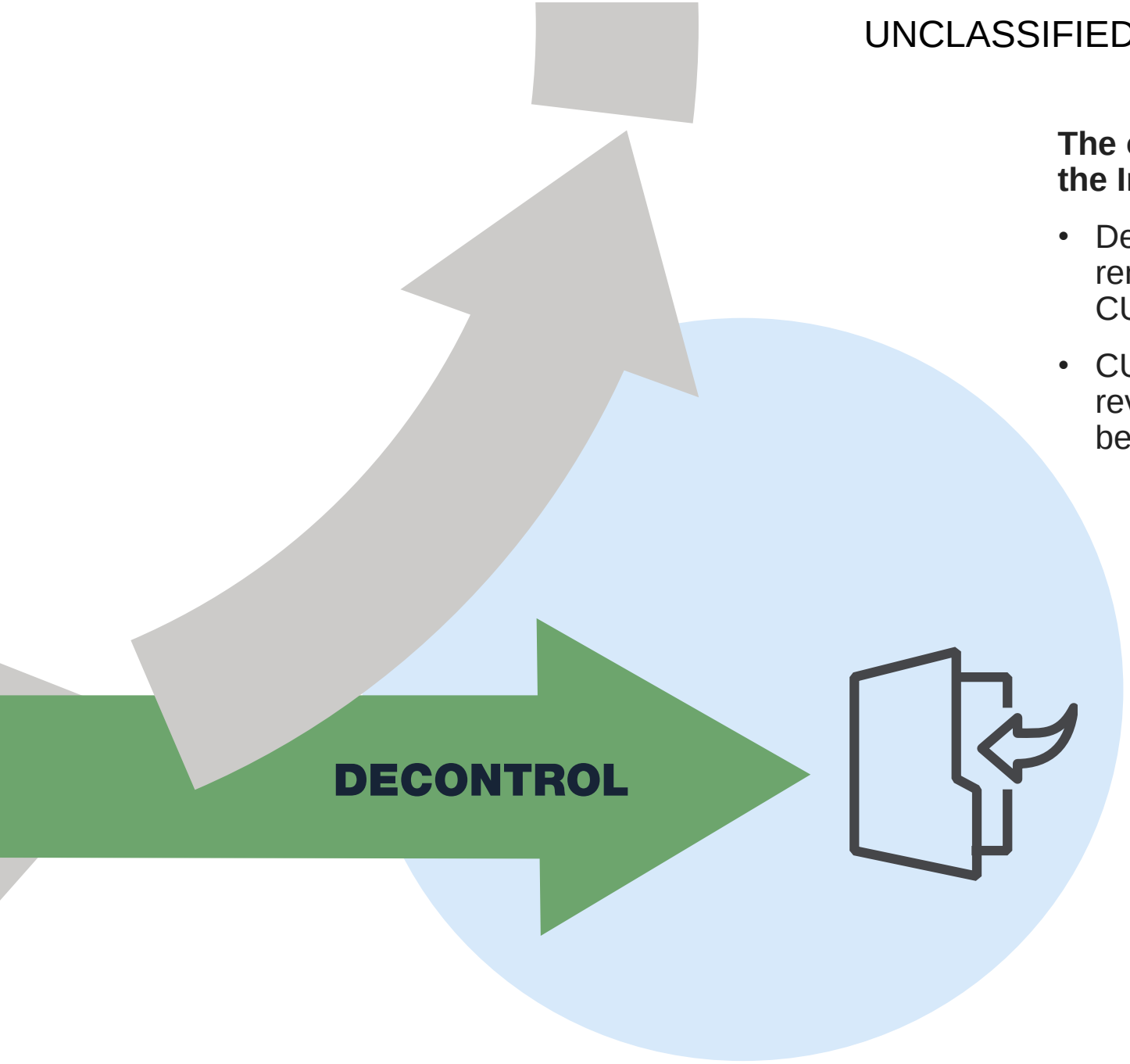
Shredding

- When you are finished with paper CUI, per ISOO CUI Notice 2019-03, CUI is destroyed using a cross-cut shredder producing 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 only entity that is authorized to decontrol CUI is the Information Owner (IO).

- Decontrolling occurs when the **IO** of the CUI material removes safeguarding or dissemination controls from CUI no longer requiring 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

- 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.
- DODI 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 Information Owner (customer, prime, agency, GCA etc.)** to validate CUI requirements.
3. Understandings of the ISOO and DOD Registries 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

- ISOO 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 and Stickers
- 32 CFR CUI Final Rule

IT/Systems

- DODI 8500.01 (Cybersecurity)
- NIST SP 800-171 (CUI on Non-Federal Systems
- NIST SP 800-172 (Enhanced Security Requirements for CUI)

References

Comparison of old vs. new CUI