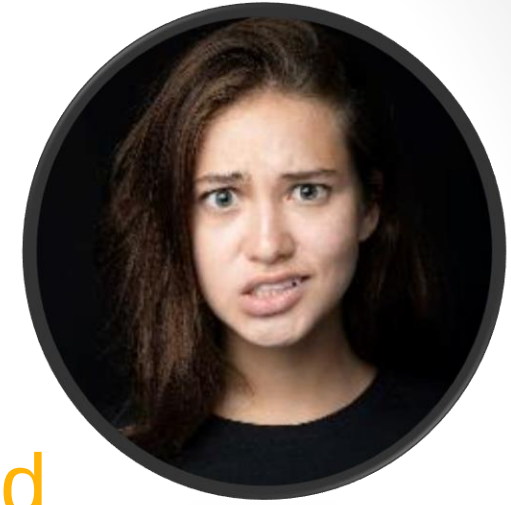
PUBLIC CONTRACTING INSTITUTE



What are Controlled Unclassified Information and Covered Defense Information, and Why Should we Care?

Jim Goepel
General Counsel
Continuous Compliance LLC
JGoepel@FutureFeed.co

FutureFeed

About Jim Goepel

- General Counsel and Director of Education at FutureFeed
- Author of 2 books on Controlled Unclassified Information (https://CUIInformed.com)
- Founding Director of the CMMC Accreditation Body (Cyber AB)
  - Created and taught the RP program
  - Board Treasurer
- Co-author of Certified CMMC Professional (CCP) curriculum
- Co-Founder of the CMMC Information Institute
- Adjunct Professor at RIT; former Adjunct at Drexel University
- Expert Witness
- BSECE – Drexel University
  - Designed satellite test equipment and processes
  - Systems Administrator and Developer for the US Congress (House of Representatives)
- JD and LLM – George Mason University
  - Advisor to many government contractors including Unisys and JHU/APL
- Certifications:
  - Certified CMMC Assessor (CCA), CMMC Provisional Instructor, Certified CMMC Professional

Bottom Line Up Front:

- CUI is:
  - 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 an agency to handle using safeguarding or dissemination controls.
- The information **must** be appropriately protected, or it is a violation of law.
- The CUI program helps agencies identify CUI and ensure it is properly protected.

It really is that simple.

Of course, the devil is in the details.

History

Government Information

- The government creates a LOT of information.
- Some is classified.
- Much is not.
- Some is publicly available.
- Much is not.
- This “middle ground” area (unclassified but non-public information) is where we will focus today

Government Information

Unclassified, non-public information

- Federal agencies have wrestled with how to identify and protect this information for decades
- Over 100 different information "categories" were created, such as:
  - For Official Use Only ("FOUO")
  - Sensitive but Unclassified ("SBU")
  - Law Enforcement Sensitive ("LES")
  - Sensitive Security Information ("SSI")
- Each agency had its own definitions for:
  - What constituted FOUO, SBU, etc.
  - How to safeguard FOUO, SBU, etc.
  - To whom FOUO, SBU, etc. could be disclosed

Inconsistency Led to Distrust

- Agency A said SBU can't be disclosed to contractors
- Agency B's SBU definition allowed SBU to be disclosed to contractors
- Agency A learns Agency B personnel shared information with contractors
- Agency A's employees now don't trust Agency B
- This distrust built up over decades, and led to information silos
- As a result, agencies failed to share information that would benefit another agency.

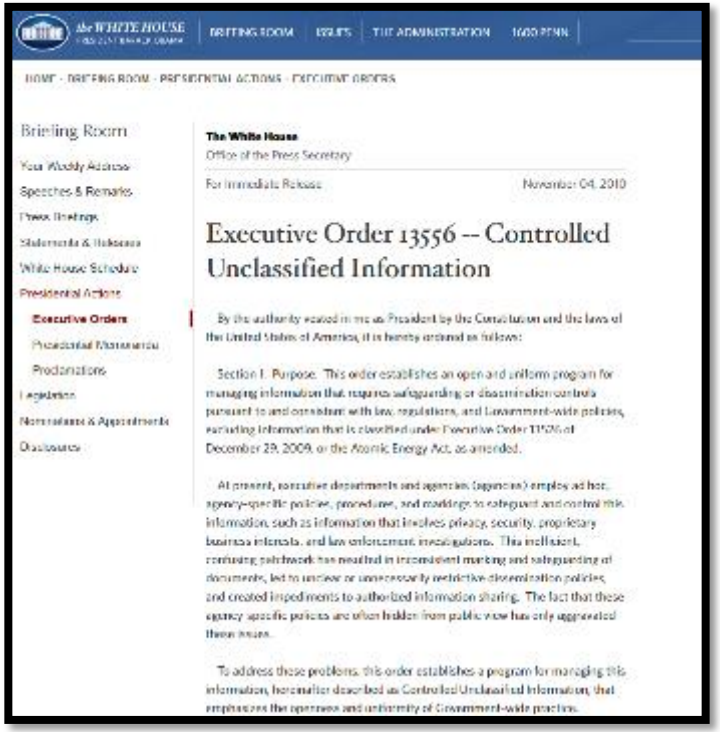
Catastrophic Effects

- The 9/11 Commission found that agencies had the information needed to identify and catch the 9/11 perpetrators before the attacks.
- Agencies failed to share critical information that would have allowed the right people to have connected the dots.
- Agencies focused too much on protecting "their" information, failing to appreciate that it was taxpayer-funded, and the entire government's.
- Agencies applied the "need-to-know" standard, which comes from classified information, to unclassified information.

FCI and CUI

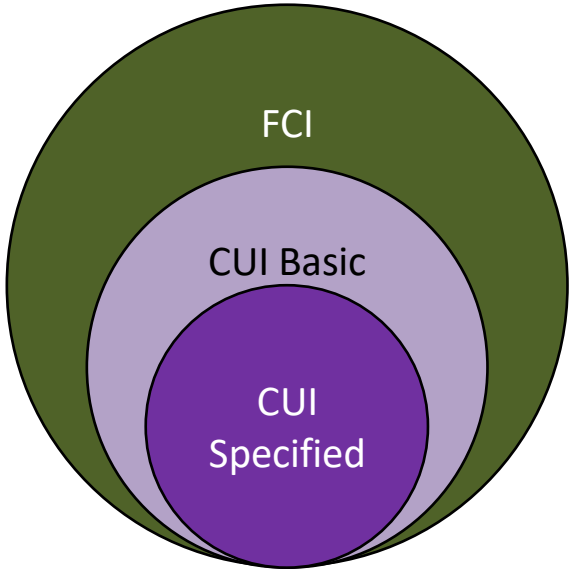
Controlled Unclassified Information ("CUI") Program

- President George W. Bush instituted a comprehensive review of the classified and unclassified information programs.
- In 2008, the White House issued an Executive Memo creating the initial CUI program.
- In 2010, President Obama used the lessons learned to formalize the CUI Program under Executive Order 13556.
- EO13556 authorizes the National Archives and Records Administration ("NARA") to create a government-wide CUI program.
- NARA's CUI Program (32 CFR 2002) establishes standardized approaches to:
  - identifying sensitive information;
  - determining when dissemination of sensitive information is to be limited; and,
  - defining minimum safeguarding requirement for sensitive information.
- Also resulted in the creation of a minimum safeguarding requirement for all non-public government information [outside the scope of the CUI program].



Federal Contract Information ("FCI") and CUI

- **Federal Contract Information** – information, not intended for public release, that 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.
- **Controlled Unclassified Information** - is 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 an agency to handle using safeguarding or dissemination controls.
- **CUI Basic** - the subset of CUI for which the authorizing law, regulation, or Government-wide policy does not set out specific handling or dissemination controls.
- **CUI Specified** - the subset of CUI in which the authorizing law, regulation, or Government-wide policy contains specific handling controls that it requires or permits agencies to use that differ from those for CUI Basic.



Examples of FCI

- E-mails between a contractor and the government or a prime contractor
- Internal E-mails about the contractor's performance under a contract
- Notes taken about the contractor's performance under a contract
- Drafts of reports (even reports that will eventually become public)

Safeguarding FCI

- FAR 52.204-21 specifies the minimum safeguarding requirements that must be in place when handling FCI
- 15 basic safeguarding requirements
- A 2020 study by Sera Brynn found that 70+% of contractors failed to meet at least one of the 15 requirements

Examples of CUI Basic

- Certain kinds of nuclear information
- Geospatial data collected by (or on behalf of) the Department of Agriculture
- Patent applications
- Most general privacy information
- SBIR/STTR information
- Pesticide producer information
- Federal building threat assessments, security system plans, contingency plans, etc.
- Federal building, grounds, or property security information
- DoD critical infrastructure security information
- Public drinking water system vulnerability analyses
- General critical infrastructure information
- Information systems vulnerability information

Safeguarding CUI Basic

- 32 CFR 2002 establishes the consistent set of security controls that must be in place when handling CUI Basic
- For non-federal (i.e., contractor) information systems, NARA selected the requirements defined in NIST Special Publication ("SP") 800-171.
- Federal agencies must use NIST SP 800-171, and its companion assessment guide (NIST SP 800-171A) as the standard when evaluating whether non-federal systems can be used to store, process, or transmit CUI.

Examples of CUI Specified

- Export Controlled Information
- Health Information
- Genetic Information
- Federal Budget Information
- Financial records obtained for intelligence or counterintelligence purposes
- Consumer Complaint Information
- Accident Investigation Information
- Campaign Fund Information
- Controlled Technical Information
- Covered Defense Information

Safeguarding CUI Specified

- CUI Specified is to be protected in accordance with NIST SP 800-171 **plus** the additional safeguarding or dissemination controls defined in the corresponding law, regulation, or government-wide policy.

Don't Worry…

- You don't have to read an analyze every law, regulation, and government-wide policy ("LRGWP") to try to guess whether it makes information CUI.
- NARA has published a CUI Registry which lists all LRGWPSs agencies can use as the basis for designating information as CUI. (see https://Archives.gov/CUI/registry/category-list)
- There are currently 400+ LRGWPs in the NARA CUI Registry
- Agencies can create their own CUI Registries, but the NARA CUI Registry is the definitive Registry
  - Agency CUI registries can help narrow the number of LRGWPs that must be analyzed by agency personnel when designating information as CUI
  - Agency CUI registries can also provide agency guidance on how the agency applies and interprets certain LRGWPs
  - See, e.g., DoD's CUI registry: https://www.dodcui.mil/CUI-Registry-New/

REMEMBER

- From a contractor's perspective, information is only CUI if:
  - it is:
    - created by the contractor during the performance of a contract; or
    - received by the contractor from the government or a higher-tier contractor during the performance of a contract;
  - AND
    - a law, regulation, or government-wide policy exists which requires or permits the information to be subject to safeguarding or dissemination controls
- This means, for example, that your company's proprietary information is not CUI while in your environment (including coming back into your environment), including:
  - Employee social security numbers or healthcare information
  - Business plans and proprietary designs
  - System security plans or vulnerability scan results
  - Floorplans
- Always be sure to mark your information as PROPRIETARY before giving it to the government
  - DO NOT mark it as CUI, even though it may become CUI once received by the government

IMPORTANT POINT

- Only federal agencies can **designate** information as CUI (i.e. determine that information is CUI)
- All “authorized holders” of the CUI are authorized to **mark** information as CUI

Digging Deeper: Covered Defense Information

- One of the more commonly-encountered forms of CUI for DoD contractors
- Defined in DFARS 252.204-7012(a) as:
  - Unclassified **controlled technical information** or other information, as described in the Controlled Unclassified Information (CUI) Registry, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is
    - (1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or
    - (2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.
- Covered Defense Information definition creates a circularity issue and makes all CUI into CUI Specified
- Controlled Technical Information is defined as:
  - technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.
- DFARS 252.204-7012 also includes additional safeguarding requirements, including FedRAMP moderate authorization (or equivalent) for cloud providers handling CUI and strict incident reporting and system access requirements

Identifying Controlled Technical Information

- Controlled Technical Information is defined as:
  - technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.
- If you receive information marked with a DoD Distribution Statement (except Distribution Statement A, public release), that information has been designated as CUI even if it does not have other CUI markings.
- It should be treated as though it is CUI and handled in accordance with DFARS 252.204-7012

Designation vs Marking in the Real World

Designating CUI

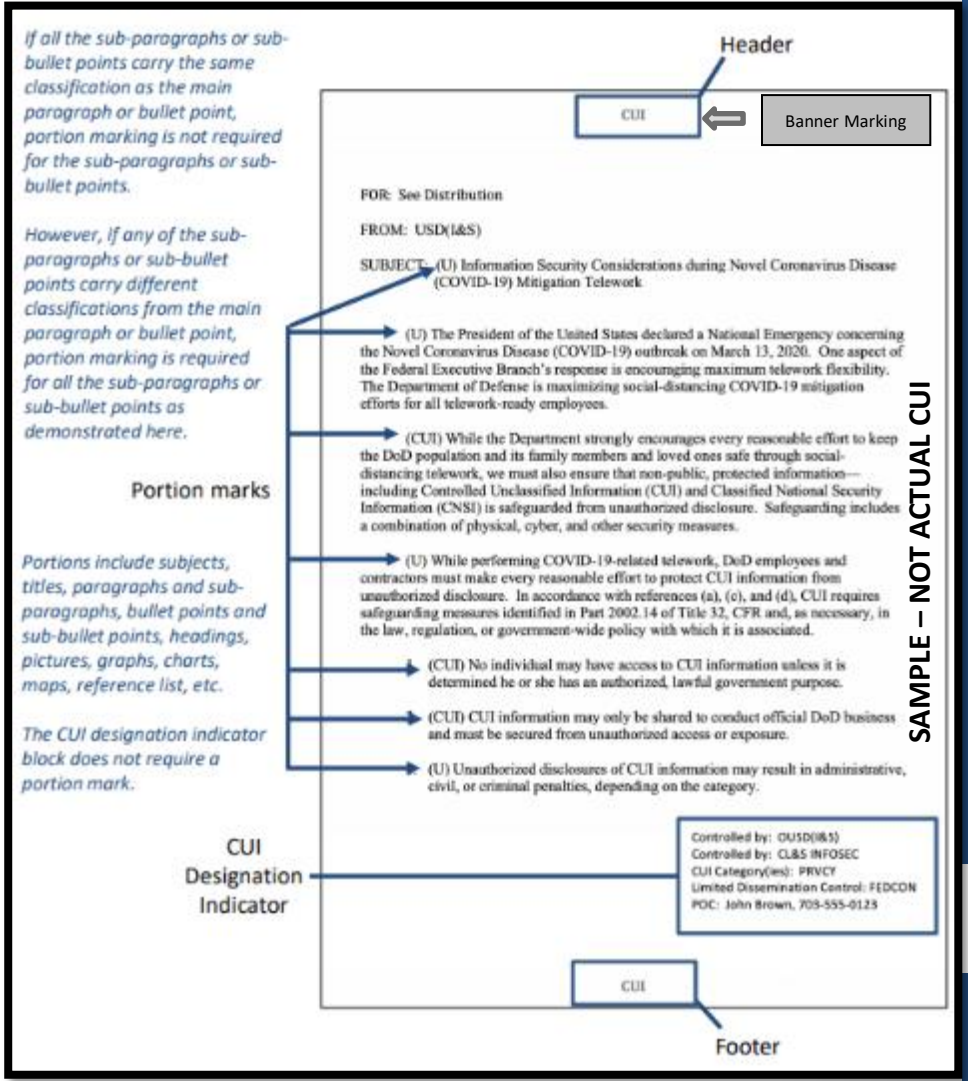
- Designating information as CUI restricts the free flow of that information
- This is an inherently governmental act and can **only** be performed by persons to whom appropriate authority has been expressly delegated
- Agencies designate information internally through memos or through analysis by an authorized representative of the agency
- Government contractors are **not** inherently delegated authority to designate information as CUI
- Entering into a contract with the government is not, on its own, implied delegation of authority
- Agencies may delegate authority to contractors, but it is exceedingly rare
- Instead, agencies communicate the fact that information has been designated as CUI by:
  - Marking the information as CUI prior to disseminating it; or
  - Through contracts or other agreements with the recipient.

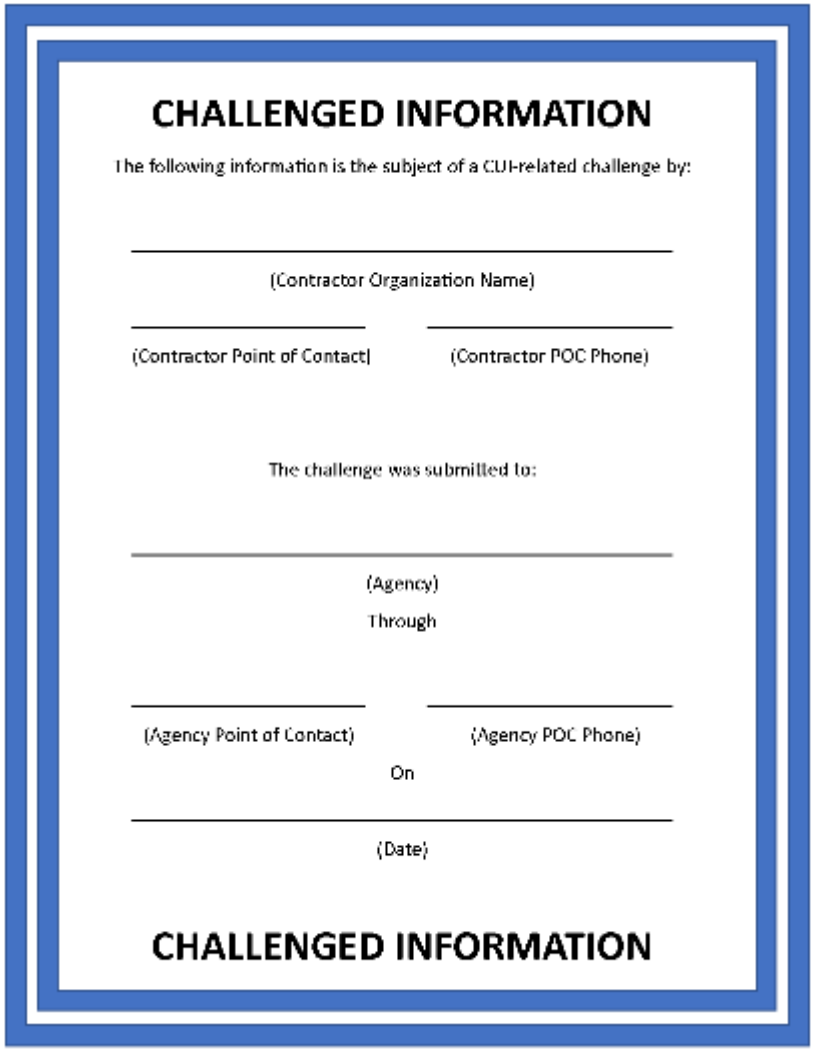
Example

- Department of Good Works wants ABC Co. to perform a vulnerability assessment of a DGW facility
- In the contract with ABC Co., DGW indicates that the vulnerability assessment and all related reports are CUI and should be appropriately marked by ABC Co. when created
  - DGW must specify:
    - CUI Marking(s) to be used
    - Designator block to be included
  - ABC Co. should also ask:
    - for the LRGWP that is the basis for the CUI designation
    - whether the information is CUI Basic or CUI Specified
  - In ABC Co's assumptions, ABC Co should discuss with counsel adding something along the lines of the following:
    - Contractor recognizes that any contract resulting from this proposal is likely to involve the creation or handling of CUI by contractor and/or a subcontractor. Consistent with the agency's obligations under 32 CFR 2002, contractor assumes that the agency will properly mark as CUI all information which the agency has designated as CUI prior to its dissemination to contractor.
    - In addition, contractor assumes that, consistent with the agency's obligations under 32 CFR 2002, the agency has previously communicated, and will continue to communicate, to contractor regarding any information that contractor may create under this contract which the agency has designated as CUI.
    - Contractor further assumes that the agency recognizes that the agency's failure to properly designate information as CUI, mark information as CUI, and/or communicate appropriate designation and marking information to contractor in a timely manner may result in schedule delays, may increase contractor's costs of performance, and may have other impacts on the overall performance of the contract which will be addressed by the agency in the form of one or more contract modifications.

Marking CUI

- "CUI" or "Controlled" **must** be in the Banner
  - CUI or Controlled may also be in the footer
  - If the CUI is CUI Specified, banner (and footer, if used) must also include the CUI category
- All CUI **must** include a designation indicator (or designation block)
  - Identifies the agency that designated the information as CUI
  - Provides point(s) of contact in the event there are questions
- All CUI **must** be marked before it is disseminated





CHALLENGED INFORMATION

The following information is the subject of a CUI-related challenge by:

_____

(Contractor Organization Name)

_____ _____

(Contractor Point of Contact) (Contractor POC Phone)

The challenge was submitted to:

_____

(Agency)

Through

_____ _____

(Agency Point of Contact) (Agency POC Phone)

On

_____

(Date)

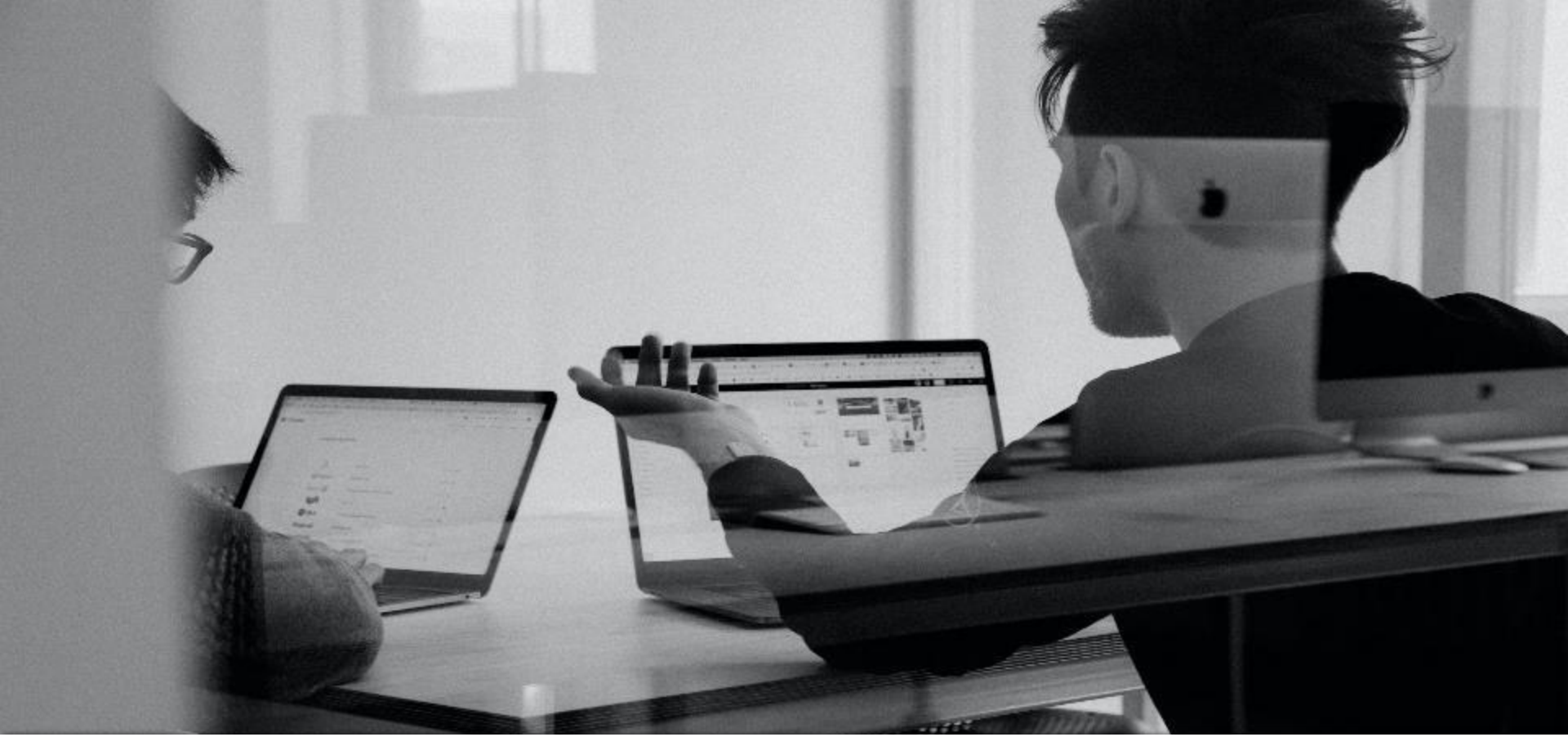
CHALLENGED INFORMATION

Unmarked CUI

- CUI **must** be marked before dissemination
  - This includes to others inside the same agency or within the contractor's organization
- **However**, we are all human, and mistakes will be made
- If you think you have received information that should be CUI:
  - Do NOT mark it as CUI – you do not have the authority to designate information as CUI
  - Ask the organization that gave the information to you (e.g., your prime contractor or the government) whether it is CUI (this is referred to as a "challenge")
  - In the interim, treat (i.e., safeguard, disseminate) it as though it is CUI
  - Consider adding a Challenged Information coversheet

Misdesignated CUI

- Designating information as CUI when that information is not CUI is punishable by sanctions and disciplinary action within the agency.
- If a contractor receives information that is marked as CUI but which the contractor does not believe is CUI:
  - If DoD is the disseminating agency, ask for the Security Classification Guide (required under DoD Instruction 5200.48) for the information
  - Ask for the LRGWP that is the basis for the CUI designation; if it is CUI Specified, the contractor needs to know what other safeguarding requirements exist
  - Continue to handle the information as though it is CUI until the "challenge" is adjudicated
  - Challenges should always be submitted to your prime contractor, the Program Manager, or the Contracting Officer
    - If that route does not result in an answer, or if further clarification is necessary, contact the agency's CUI Senior Agency Official.
      - NARA has a list of agency CUI Senior Agency Official contact information (see https://www.archives.gov/cui/about/contact.html#contact-an-agency



Dissemination

Authorized Holders

- Authorized holders are those who are permitted to handle CUI
- To be an authorized holder, a person must have a lawful government purpose for handling that (CUI) information
- Lawful government purpose is "…any activity, mission, function, operation, or endeavor that the U.S. Government authorizes or recognizes within the scope of its legal authorities or the legal authorities of non-executive branch entities (such as state and local law enforcement)."

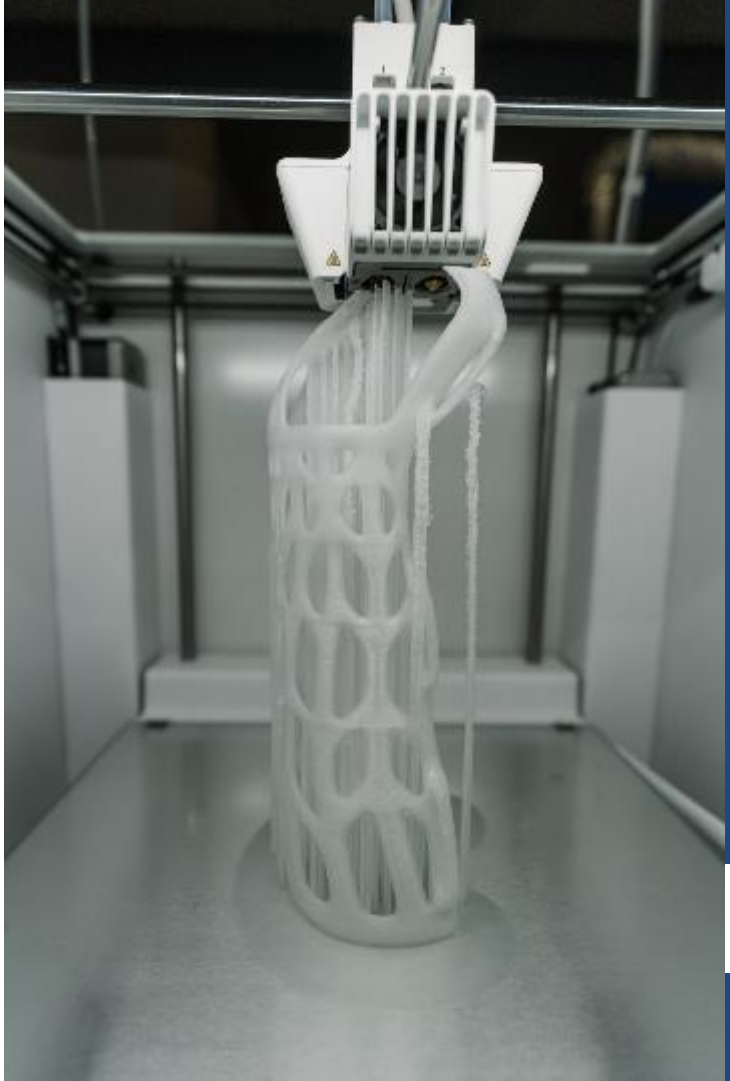
Dissemination

- Dissemination occurs when authorized holders **provide access**, transmit, or transfer CUI to other authorized holders through **any** means, whether internal or external to the agency. (emphasis added)
- Access can be provided intentionally or unintentionally, such as by leaving information out in plain sight
- Dissemination of CUI to anyone who is not an authorized holder is illegal
- Authorized holders are expected to take reasonable steps to ensure that recipients can properly handle CUI

Derivative Works

Derivative Works

- A work (e.g., document) based on or derived from one or more existing works.
  - Examples: translations, arrangements, new version of existing software, revision of a website, sculpture based on a drawing
- If the original work is CUI, the derivative work is likely to be CUI as well
- Example:
  - DoD hires ABC Co. to design a new type of cast that can be 3D printed in the field
  - DoD creates a requirements specification
  - DoD designates the requirements specification as Covered Defense Information ("CDI")
  - ABC Co. creates a design specification based on the design specification – this is likely to be CUI because the original work was CUI
    - ABC Co. should review the contract to confirm, but should assume it is CUI for internal purposes
  - ABC Co. creates a 3D model of the cast – this is likely to be CUI
  - ABC Co. 3D prints a sample cast – this is also likely to be CUI



Summary

- The government expects contractors to properly safeguard its information.
- FCI must be protected using minimum requirements defined in FAR 52.204-7012
- All CUI is subject to **at least** the enhanced safeguarding requirements defined in NIST SP 800-171
- CUI Specified is also subject to additional requirements defined in the corresponding LRGWP
- The most common DoD CUI encountered by contractors is Controlled Technical Information, a form of Covered Defense Information
  - CDI and CTI are not only subject to NIST SP 800-171, but also the additional requirements in DFARS 252.204-7012(c)-(g).
- CUI must only be disseminated to Authorized Holders
- To be an Authorized Holder, you must have a Lawful Government Purpose to handle that specific CUI
- CUI retains its nature as CUI even when translated or transformed (e.g., through derivative works)
- Only federal agencies are authorized to **designate** information as CUI; all authorized holders are authorized to **mark** information as CUI (e.g., information a contractor creates under a contract that has designated the information as CUI)

Thank You!

Please provide session feedback

https://CUIInformed.com

15 Minutes with FutureFeed:
https://FutureFeed.co/15

Q&A