CUI Deep(ish) Dive

James Goepel
CEO and General Counsel
Fathom Cyber LLC

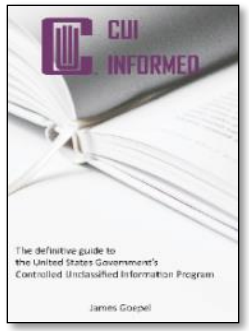
Fathom Cyber
Cybersecurity and Compliance Experts

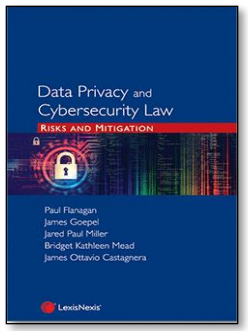
CUI-CON 2025

Disclaimers

- The views expressed in this presentation are those of the presenter(s) and do not necessarily constitute the views or legal positions of their employer(s), clients, the US Department of Defense, or the Cybersecurity Maturity Model Certification Accreditation Body (Cyber AB).
- The information is being provided for general informational purposes and does not constitute legal or business advice.
- You should **always** consult a competent advisor to discuss the specifics of your situation before taking any action.

About Me



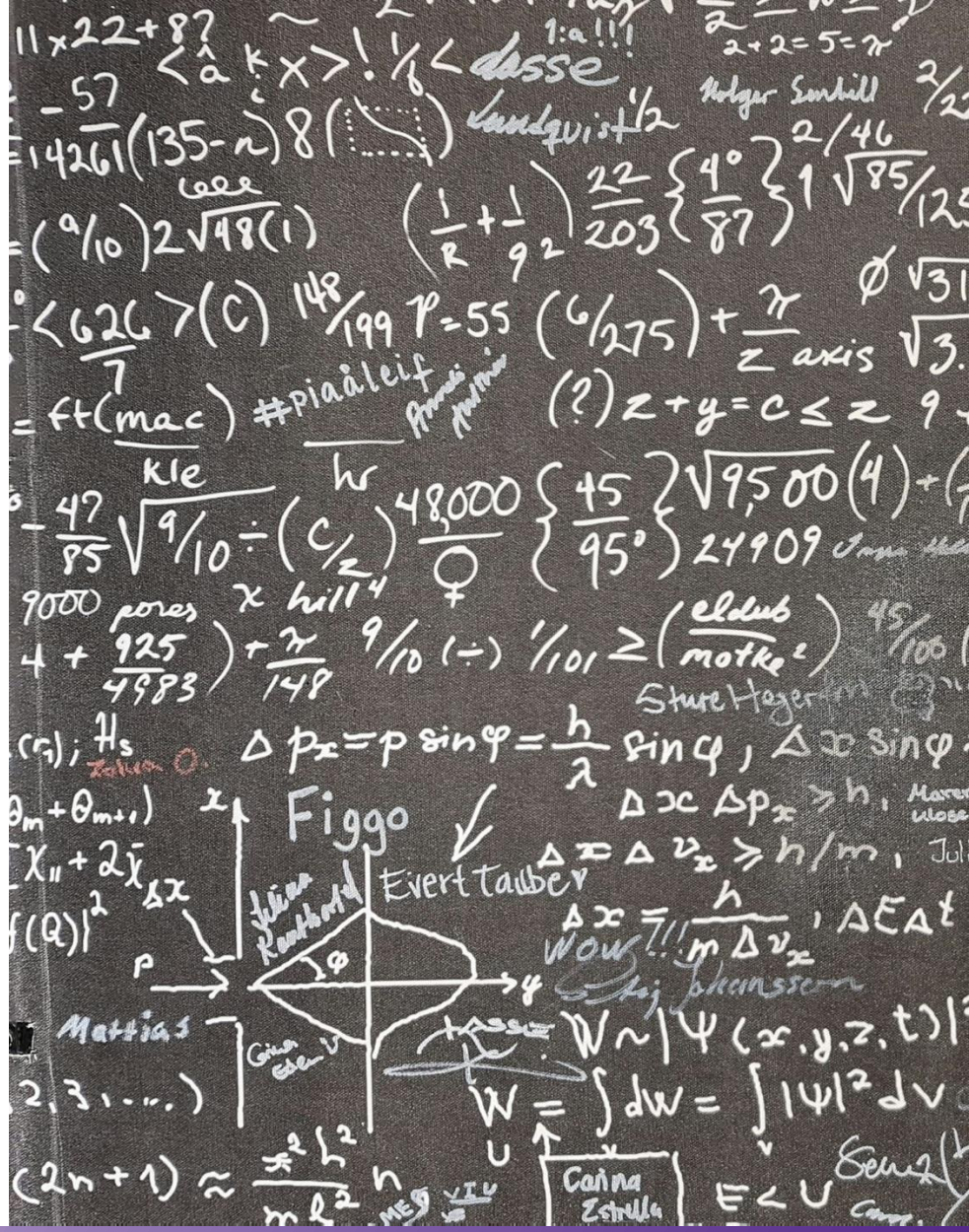


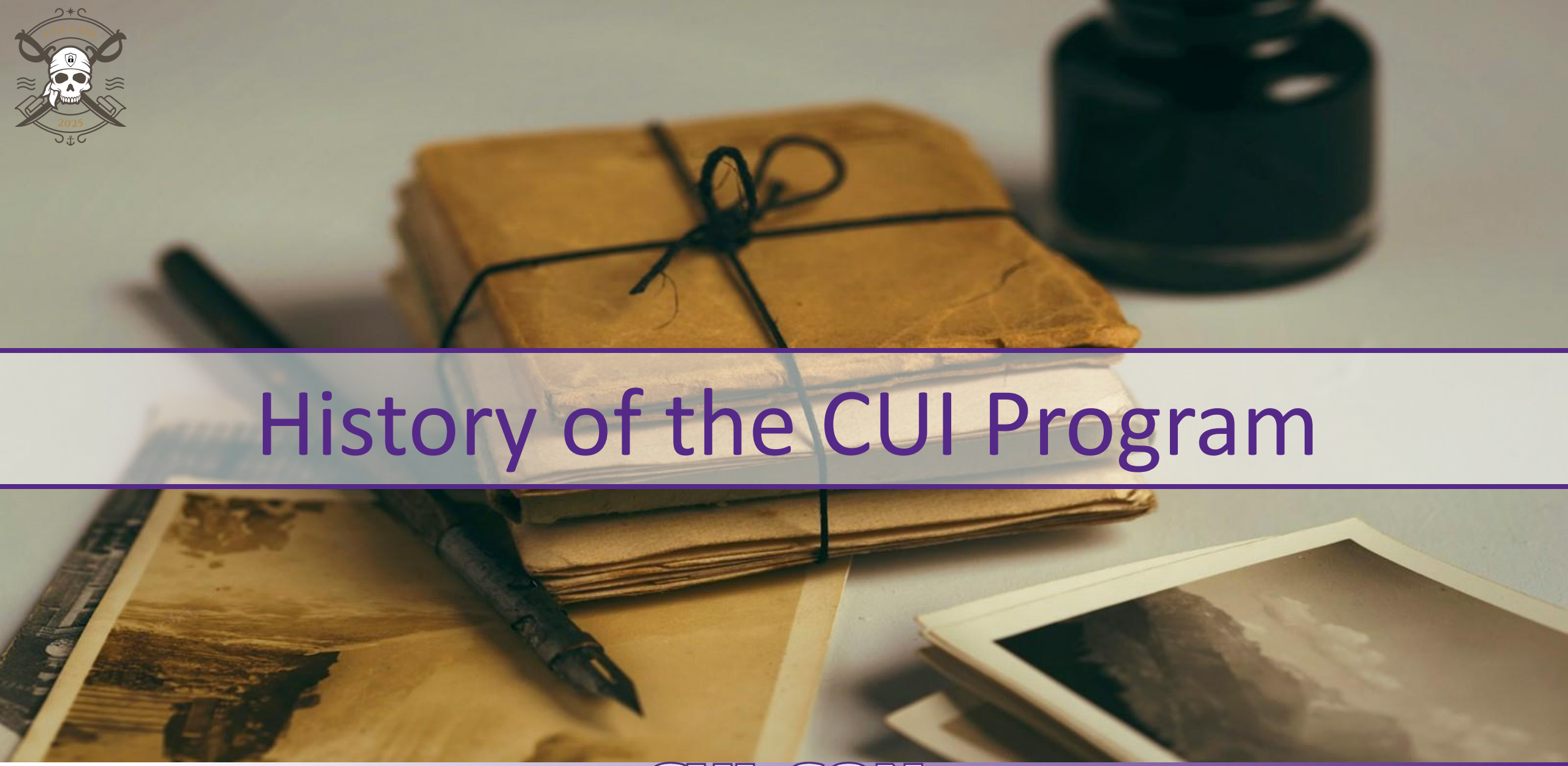
- CEO and General Counsel, Fathom Cyber LLC
- Provisional CMMC Instructor (PI), Certified CMMC Assessor (CCA), Certified CMMC Professional (CCP)
- Founding Director of the CMMC Accreditation Body (Cyber AB) (Prev.)
  - Created and taught the original RP training program
  - Board Treasurer
- Co-Founder of the CMMC Information Institute
- Author
  - 2 books on Controlled Unclassified Information (**https://CUIInformed.com**)
  - 2 books on enterprise risk management and international cybersecurity law (Co-author)
  - Certified CMMC Professional (CCP) curriculum (Co-author)
- Adjunct Faculty at RIT; former Adjunct Professor at Drexel University
- Expert Witness in Government Contract Cybersecurity Cases, Healthcare Cybersecurity
- JD and LLM – George Mason University
  - Advisor to many government contractors including Unisys, JHU/APL, Textron, United Space Alliance
- BSECE – Drexel University
  - Designed satellite test equipment and processes
  - Systems Administrator and Developer for the US Congress (House of Representatives)

CUI is not Complicated

Bottom Line Up Front:

- CUI is:
  - unclassified information
  - created or received for or on behalf of the government
  - to which a law, regulation, or government-wide policy (not just an Agency policy) requires or permits the application of:
    - safeguarding controls or
    - limited dissemination controls
- Non-federal information systems must safeguard CUI Basic in accordance with NIST SP 800-171





History of the CUI Program

Fathom Cyber

Cybersecurity and Compliance Experts

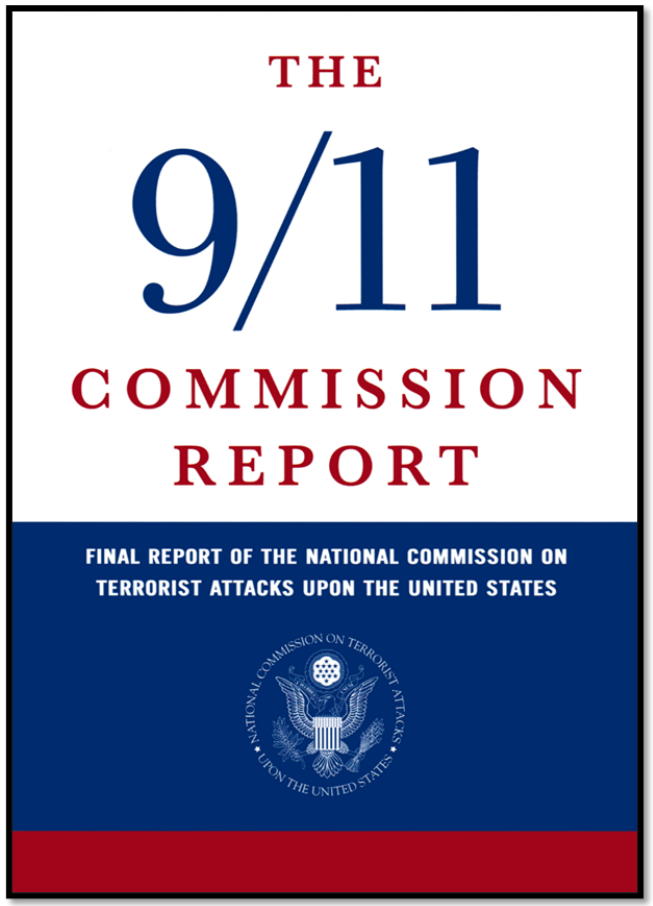
CUI-CON 2025

September 11, 2001

Terrorist attacks on New York and DC

Congress Appoints the 9/11 Commission

Distrust Among Agencies Led to Catastrophe



- Agencies had the information needed to identify and catch the 9/11 terrorists.
- Agency reluctance to share information with other agencies allowed the terrorists to complete their acts.
- The Federal Government needs a new approach to identifying and protecting sensitive information.
- That approach must:
  - be consistent across the entire federal government;
  - recognize that unclassified information is unclassified and treat it as such (get away from “need to know” mindset); and,
  - encourage information sharing to authorized persons.

The Result: Sensitive Information Overhaul

- **Executive Order 13292** – 2003
  (Overhauls how Classified Info is Identified and Handled)
- **Intelligence Reform and Terrorism Prevention Act** – 2004
  (Requires the creation of an "information sharing environment")
- **CUI Executive Memo** – 2008
  (Lays a Foundation for the CUI Program, Convenes an Interagency Task Force on Controlled Unclassified Information)
- **Executive Order 13526** – 2010
  (Further Refines the Classified Info Program)
- **Executive Order 13556** – 2010
  (Formally Establishes a CUI Program)

> "To address these problems, this order establishes a program for managing this information, hereinafter described as Controlled Unclassified Information, that **emphasizes the openness and uniformity of Government-wide practice.**"
>
> – Executive Order 13556

CUI Concepts

Fathom Cyber

Cybersecurity and Compliance Experts

CUI-CON 2025

Legacy Information

SBU

Sensitive but Unclassified

SSI

Sensitive Security Information

CII

Critical Infra
Informa

LES

Law Enforcement Sensitive

CUI

FOUO

For Official Use Only

97+

Additional

NATIONAL ARCHIVES

Legacy information is not automatically CUI

- Agencies and authorized holders must…Discontinue all use of legacy or other markings not permitted by the CUI Program or included in the CUI Registry.
- If legacy markings remain on information, the legacy markings are void and no longer indicate that the information is protected or that it is or qualifies as CUI.
- **Agencies** must review documents created prior to November 14, 2016 and re-mark any that contain information that qualifies as CUI in accordance with Executive Order 13556, 32 CFR 2002, and the CUI Registry.

FOUO
For Official Use Only

LES
Law Enforcement Sensitive

SBU
Sensitive but Unclassified

CUI
Controlled Unclassified Information

Controlled Unclassified Information

"…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. However, CUI does not include classified information … or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency." *– 32 CFR 2002.4(h)*

Oversimplification: Unclassified information created or received for or on behalf of the US government that a law, regulation, or government-wide policy ("**LRGWP**") says can or must be safeguarded or is subject to limited dissemination controls.

CUI Basic vs CUI Specified

- **CUI Specified** – The LRGWP specifies how the information is to be safeguarded.
- **CUI Basic** – The LRGWP says that the information must be safeguarded, but it doesn't specify how.
- NIST SP 800-171 is the minimum set of requirements for safeguarding all CUI, including CUI Basic.
- If the information is CUI Specified, the information must **<u>also</u>** be safeguarded in accordance with the LRGWP's requirements.

By Definition, For Government Contractors:

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
- **AND**
  - a **federal agency** has designated the information as CUI.

Designation vs Marking

- **Marking:** applying appropriate notices (banner, footer, designation indicator) to information containing CUI so others are aware of its status as CUI
- **Designation:** determining that a law, regulation, or government-wide policy applies to information such that it qualifies as CUI
  - Only laws, regulations, and government-wide policies ("LRGWPs") approved by NARA can be the basis for a CUI designation
  - NARA publishes the list of approved LRGWPs on the CUI Registry (https://archives.gov/CUI)
  - CUI designation impedes the free flow of information.
  - This makes it an **inherently governmental act.**
  - Designation authority must be properly delegated.
  - Improper CUI designation is subject to sanctions.
  - "The designating **agency** determines that the information qualifies for CUI status and applies the appropriate CUI marking when **it** designates that information as CUI." – 32 CFR 2002.20(a)(4)

§ 128 TITLE 10—ARMED FORCES Page 152

oversight of policies and programs authorized by this section.

(j) OPERATIONAL PREPARATION OF THE ENVIRONMENT DEFINED.—In this section, the term "operational preparation of the environment" means the conduct of activities in likely or potential operational areas to set conditions for mission execution.

(Added Pub. L. 116–283, div. A, title X, §1052(a), Jan. 1, 2021, 134 Stat. 3849; amended Pub. L. 117–81, div. A, title X, §1093(b), Dec. 27, 2021, 135 Stat. 1935; Pub. L. 117–263, div. A, title XVI, §1621, Dec. 23, 2022, 136 Stat. 2933; Pub. L. 118–31, div. A, title XII, §1221(a), Dec. 22, 2023, 137 Stat. 451.)

Editorial Notes

AMENDMENTS

2023—Pub. L. 118–31, §1221(a)(1), inserted "and non-conventional assisted recovery capabilities" after "environment" in section catchline.

Subsec. (a). Pub. L. 118–31, §1221(a)(2), substituted par. (1) for "Subject to subsections (b) through (d), the Secretary of Defense may expend up to $15,000,000 in any fiscal year for clandestine activities for any purpose the Secretary determines to be proper for preparation of the environment for operations of a confidential nature." and designated remainder of subsec. (a) as par. (2).

Subsec. (b). Pub. L. 118–31, §1221(a)(3), added subsec. (b) and struck out former subsec. (b). Prior to amendment, text read as follows: "Funds for expenditures under this section in a fiscal year shall be derived from amounts authorized to be appropriated for that fiscal year for operation and maintenance, Defense-wide."

Subsec. (c). Pub. L. 118–31, §1221(a)(5), added subsec. (c). Former subsec. (c) redesignated (d).

Subsec. (d). Pub. L. 118–31, §1221(a)(6), substituted "Limitations" for "Limitation on Delegation" in heading and "The Secretary of Defense—", par. (1), and "(2) may not delegate" for "The Secretary of Defense may not delegate" in text.

Pub. L. 118–31, §1221(a)(4), redesignated subsec. (c) as (d).

Subsecs. (e) to (g). Pub. L. 118–31, §1221(a)(4), redesignated subsecs. (d) to (f) as (e) to (g), respectively. Former subsec. (g) redesignated (h).

Subsec. (g)(1) to (5). Pub. L. 118–31, §1221(a)(7), added pars. (1) to (4), redesignated former par. (4) as (5), and struck out former pars. (1) to (3) which read as follows:

"(1) the amount and date of such expenditure;

"(2) a detailed description of the purpose for which such expenditure was made;

"(3) an explanation why other authorities available to the Department of Defense could not be used for such expenditure; and".

Subsec. (h). Pub. L. 118–31, §1221(a)(4), redesignated subsec. (g) as (h).

Subsecs. (i), (j). Pub. L. 118–31, §1221(a)(8), added subsecs. (i) and (j).

2022—Subsecs. (e) to (g). Pub. L. 117–263 added subsec. (e) and redesignated former subsecs. (e) and (f) as (f) and (g), respectively.

2021—Subsec. (f). Pub. L. 117–81 added subsec. (f).

§ 128. Control and physical protection of special nuclear material: limitation on dissemination of unclassified information

(a)(1) In addition to any other authority or requirement regarding protection from dissemination of information, and subject to section 552(b)(3) of title 5, the Secretary of Defense, with respect to special nuclear materials, shall prescribe such regulations, after notice and opportunity for public comment thereon, or issue such orders as may be necessary to prohibit the unauthorized dissemination of unclassified information pertaining to security measures, including security plans, procedures, and equipment for the physical protection of special nuclear material.

(2) The Secretary may prescribe regulations or issue orders under paragraph (1) to prohibit the dissemination of any information described in such paragraph only if and to the extent that the Secretary determines that the unauthorized dissemination of such information could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of—

(A) illegal production of nuclear weapons, or

(B) theft, diversion, or sabotage of special nuclear materials, equipment, or facilities.

(3) In making a determination under paragraph (2), the Secretary may consider what the likelihood of an illegal production, theft, diversion, or sabotage referred to in such paragraph would be if the information proposed to be prohibited from dissemination under this section were at no time available for dissemination.

(4) The Secretary shall exercise his authority under this subsection to prohibit the dissemination of any information described in paragraph (1)—

(A) so as to apply the minimum restrictions needed to protect the health and safety of the public or the common defense and security; and

(B) upon a determination that the unauthorized dissemination of such information could reasonably be expected to result in a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of—

(i) illegal production of nuclear weapons, or

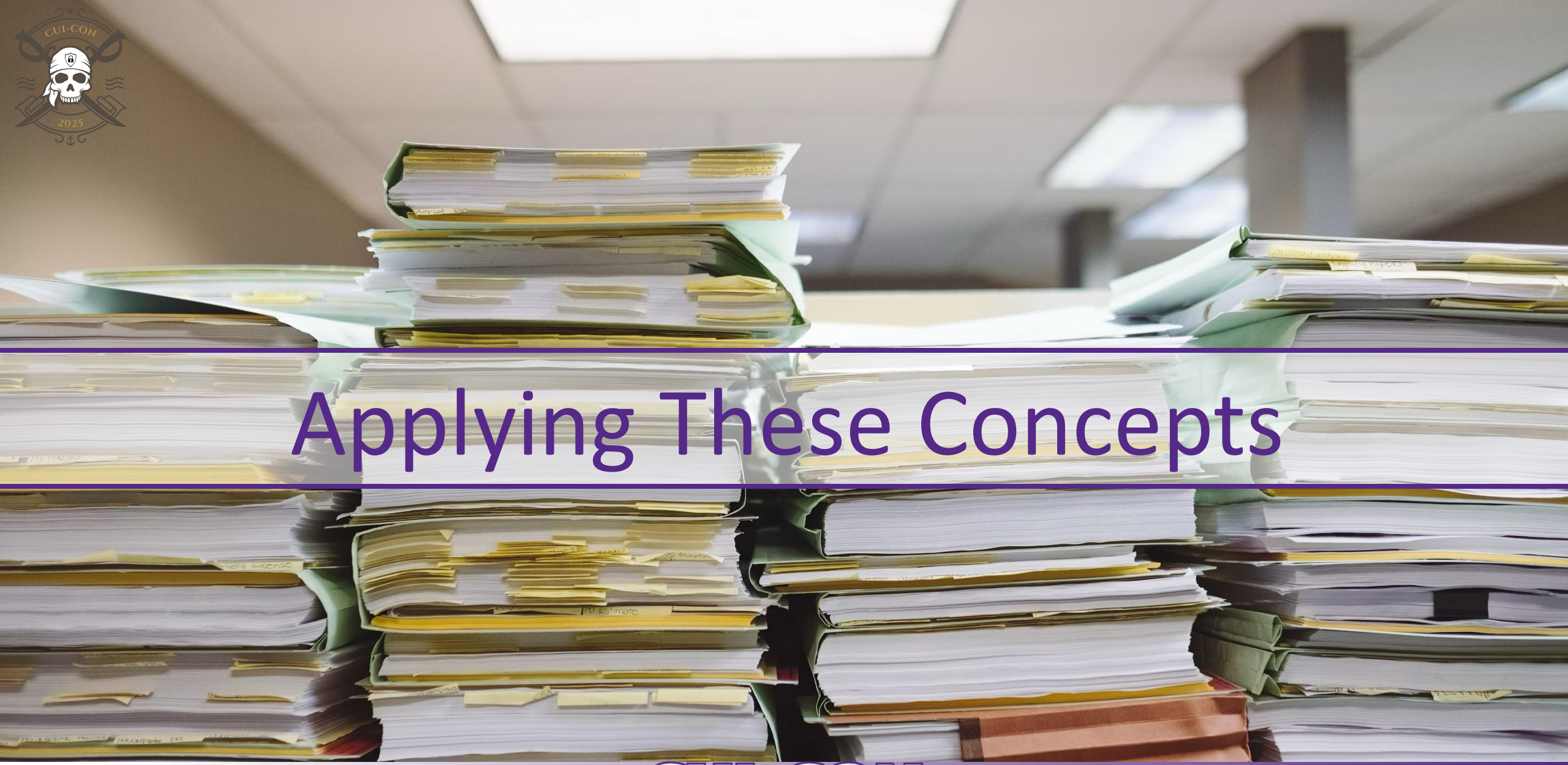
(ii) theft, diversion, or sabotage of nuclear materials, equipment, or facilities.

(b) Nothing in this section shall be construed to authorize the Secretary to withhold, or to authorize the withholding of, information from the appropriate committees of the Congress.

(c) Any determination by the Secretary concerning the applicability of this section shall be subject to judicial review pursuant to section 552(a)(4)(B) of title 5.

(d) Information that the Secretary prohibits to be disseminated pursuant to subsection (a) that is provided to a State or local government shall remain under the control of the Department of Defense, and a State or local law authorizing or requiring a State or local government to disclose such information shall not apply to such information.

(Added Pub. L. 100–180, div. A, title XI, §1123(a), Dec. 4, 1987, 101 Stat. 1149; amended Pub. L. 101–510, div. A, title XIII, §1311(1), Nov. 5, 1990, 104 Stat. 1669; Pub. L. 108–136, div. A, title X, §1031(a)(4), Nov. 24, 2003, 117 Stat. 1596; Pub. L. 114–328, div. A, title XVI, §1662(a)(1), (2), Dec. 23, 2016, 130 Stat. 2614.)



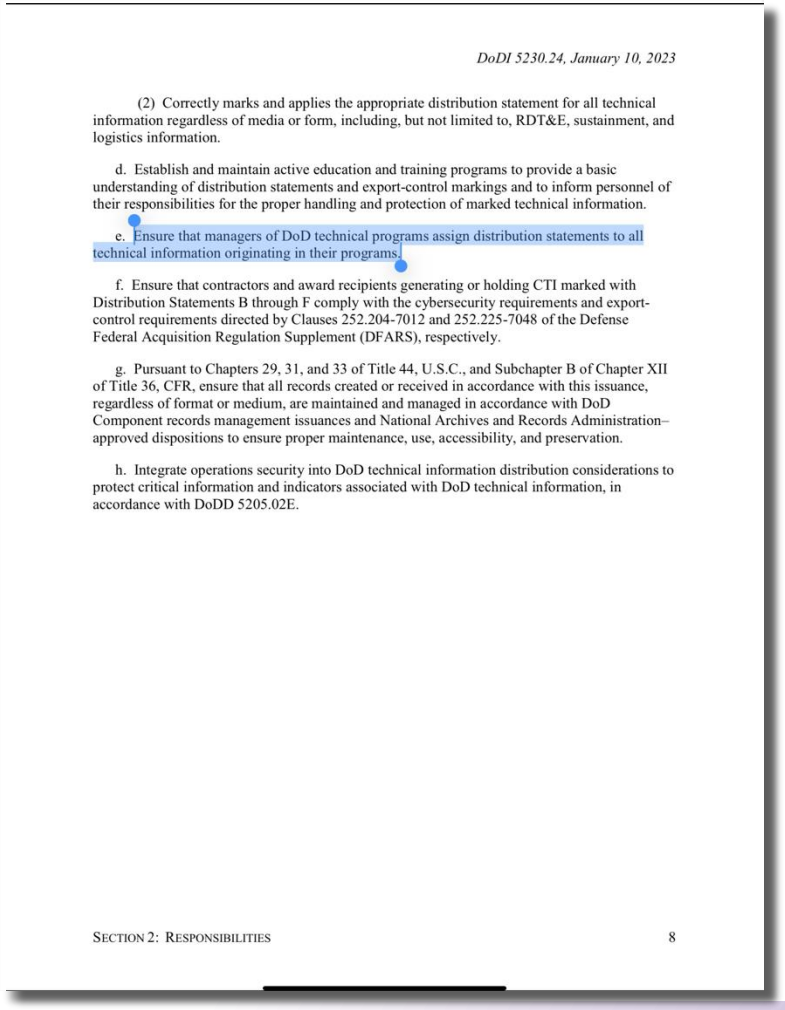
Applying These Concepts

Fathom Cyber

Cybersecurity and Compliance Experts

CUI-CON 2025

Who in DoD has Designation Authority?



DoDI 5230.24, January 10, 2023

(2) Correctly marks and applies the appropriate distribution statement for all technical information regardless of media or form, including, but not limited to, RDT&E, sustainment, and logistics information.

d. Establish and maintain active education and training programs to provide a basic understanding of distribution statements and export-control markings and to inform personnel of their responsibilities for the proper handling and protection of marked technical information.

e. Ensure that managers of DoD technical programs assign distribution statements to all technical information originating in their programs.

f. Ensure that contractors and award recipients generating or holding CTI marked with Distribution Statements B through F comply with the cybersecurity requirements and export-control requirements directed by Clauses 252.204-7012 and 252.225-7048 of the Defense Federal Acquisition Regulation Supplement (DFARS), respectively.

g. Pursuant to Chapters 29, 31, and 33 of Title 44, U.S.C., and Subchapter B of Chapter XII of Title 36, CFR, ensure that all records created or received in accordance with this issuance, regardless of format or medium, are maintained and managed in accordance with DoD Component records management issuances and National Archives and Records Administration–approved dispositions to ensure proper maintenance, use, accessibility, and preservation.

h. Integrate operations security into DoD technical information distribution considerations to protect critical information and indicators associated with DoD technical information, in accordance with DoDD 5205.02E.

SECTION 2: RESPONSIBILITIES 8

- DoDI 5200.48 delegates to Original Classification Authorities (“**OCAs**”) the authority to designate information as CUI.
- DoDI 5230.24 impliedly delegates to technical Program Managers the authority to apply limited designation controls on information, making it CUI.
- That’s it.

Can a contractor designate information as CUI?

- NO. (not usually, especially subcontractors)
- CUI designation is an inherently governmental act.
- Authority must be delegated to you to designate.
  - A contract, on its own, does not delegate that authority to you.
- MAYBE if you are an OCA in a staff-augmentation or other, similar role.

What about 32 CFR 2004.04(d)?

- 32 CFR 2002.04(d) is a definition
  - ***Authorized holder*** is an individual, agency, organization, or group of users that is permitted to designate or handle CUI, in accordance with this part.
  - i.e., "whenever we say 'authorized holder' we mean both someone who is authorized to designate CUI **as well as** someone who is authorized to handle CUI."
- Definitions define, they are not sources of authority.
- The remainder of 32 CFR 2002 specifically focuses on CUI being designated by an **agency**.

§ 2002.4 Definitions.

As used in this part:

(a) ***Agency*** (also Federal agency, executive agency, executive branch agency) is any "executive agency," as defined in 5 U.S.C. 105; the United States Postal Service; and any other independent entity within the executive branch that designates or handles CUI.

(b) ***Agency CUI policies*** are the policies the agency enacts to implement the CUI Program within the agency. They must be in accordance with the Order, this part, and the CUI Registry and approved by the CUI EA.

(c) ***Agreements and arrangements*** are any vehicle that sets out specific CUI handling requirements for contractors and other information-sharing partners when the arrangement with the other party involves CUI. Agreements and arrangements include, but are not limited to, contracts, grants, licenses, certificates, memoranda of agreement/arrangement or understanding, and information-sharing agreements or arrangements. When disseminating or sharing CUI with non-executive branch entities, agencies should enter into written agreements or arrangements that include CUI provisions whenever feasible (see § 2002.16(a)(5) and (6) for details). When sharing information with foreign entities, agencies should enter agreements or arrangements when feasible (see § 2002.16(a)(5)(iii) and (a)(6) for details).

(d) ***Authorized holder*** is an individual, agency, organization, or group of users that is permitted to designate or handle CUI, in accordance with this part.

(e) ***Classified information*** is information that Executive Order 13526, "Classified National Security Information," December 29, 2009 (3 CFR, 2010 Comp., p. 298), or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended, requires agencies to mark with classified markings and protect against unauthorized disclosure.

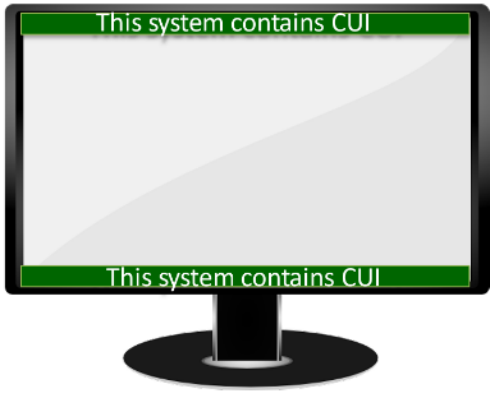
(f) ***Controlled environment*** is any area or space an authorized holder deems to have adequate physical or procedural controls (*e.g.,* barriers or managed access controls) to protect CUI from unauthorized access or disclosure.

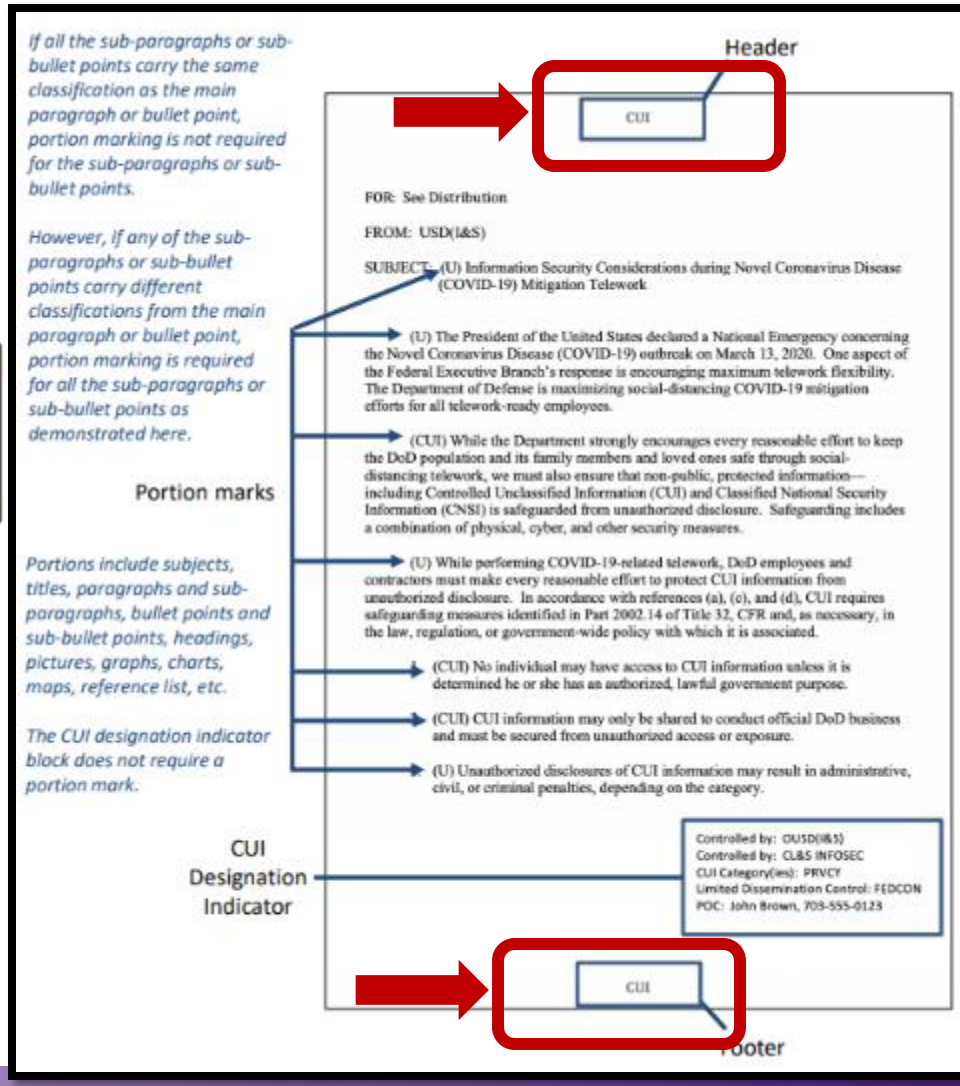
If you give the government your proprietary information…

- Always be sure to mark your information as PROPRIETARY before giving it to the government.
- You can/should include a cover letter that tells them that it is proprietary information and cite a specific LRGWP as the basis for why you believe it should be designated as CUI by them.
- **DO NOT** mark it as CUI, even though it may/should become CUI once received by the government.
  - You are not an **agency**, therefore you have not been delegated the authority to make the CUI designation on behalf of the government.
- Also, be careful about the term “Confidential”. It is one of the categories of “classified” information (Top Secret, Secret, Confidential).

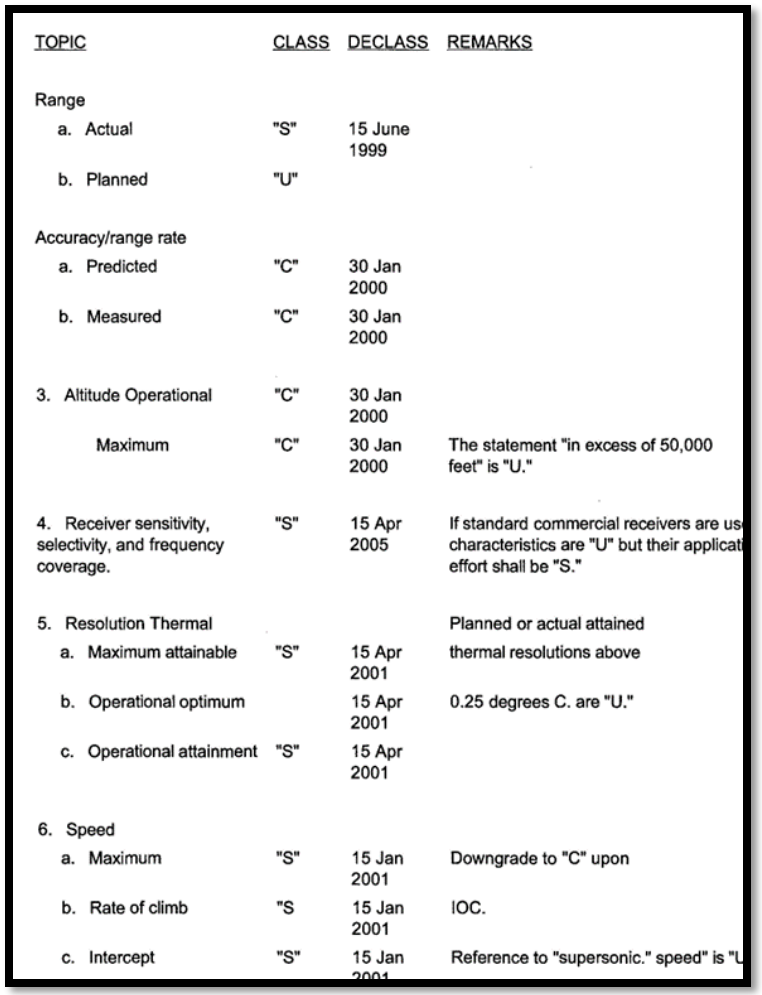
How do I know if information I receive is CUI?

- CUI must be marked before it is disseminated (shared) to **anyone**, therefore:
  - it will be overtly marked as CUI or
  - its container will be marked as CUI or
  - your contract will specify that it is CUI





What about Information I create?

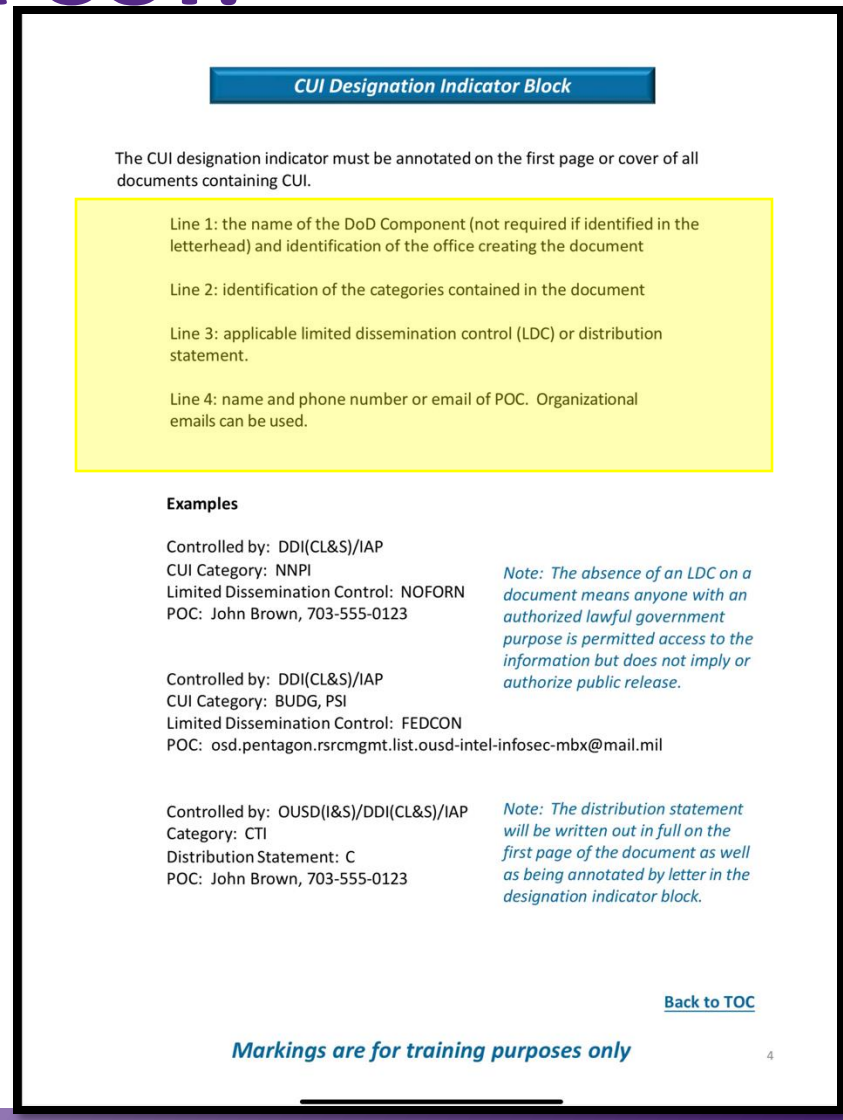


TOPIC	CLASS	DECLASS	REMARKS
Range			
a. Actual	"S"	15 June 1999	
b. Planned	"U"		
Accuracy/range rate			
a. Predicted	"C"	30 Jan 2000	
b. Measured	"C"	30 Jan 2000	
3. Altitude Operational	"C"	30 Jan 2000	
Maximum	"C"	30 Jan 2000	The statement "in excess of 50,000 feet" is "U."
4. Receiver sensitivity, selectivity, and frequency coverage.	"S"	15 Apr 2005	If standard commercial receivers are us characteristics are "U" but their applicat effort shall be "S."
5. Resolution Thermal			Planned or actual attained
a. Maximum attainable	"S"	15 Apr 2001	thermal resolutions above
b. Operational optimum		15 Apr 2001	0.25 degrees C. are "U."
c. Operational attainment	"S"	15 Apr 2001	
6. Speed			
a. Maximum	"S"	15 Jan 2001	Downgrade to "C" upon
b. Rate of climb	"S	15 Jan 2001	IOC.
c. Intercept	"S"	15 Jan 2001	Reference to "supersonic." speed" is "U

- Only the agency that "owns" the information can designate it as CUI.
- If the agency hires you to create/collect information, the agency <u>should</u> communicate any CUI designations as part of your contract.
- DoD has instructed its personnel that the designation information is to be communicated in a Security Classification Guide ("**SCG**").
  [**see DoDI 5200.48 §3.7.e.**]
  - FAR CUI Rule says that a new Standard Form is coming that will be used by agencies.
- The SCG is supposed to help you understand the attributes of the information that make it CUI.
- In contracts to create information, you should also use the SCG to determine when to mark information as CUI.
- If you receive information that is marked as CUI, or are told information has been designated as CUI, and you don't think it should be, ask for the SCG and LRGWP.
  - This is a good practice for **<u>all</u>** CUI
- Once information has been designated as CUI, it **<u>must</u>** be properly marked before it is disseminated to **<u>anyone</u>**.

How Should I Mark CUI?

- NARA CUI Marking Guide
  - https://archives.gov/CUI
- DoD CUI Marking Aid
  - https://www.dodcui.mil/Training/DoD-Training/
  - Portion marking is optional but recommended
  - CUI in the header and footer
  - Designation indicator on the first page
    - Can a contractor be a POC in a designation indicator?



CUI Designation Indicator Block

The CUI designation indicator must be annotated on the first page or cover of all documents containing CUI.

Line 1: the name of the DoD Component (not required if identified in the letterhead) and identification of the office creating the document

Line 2: identification of the categories contained in the document

Line 3: applicable limited dissemination control (LDC) or distribution statement.

Line 4: name and phone number or email of POC. Organizational emails can be used.

Examples

Controlled by: DDI(CL&S)/IAP
CUI Category: NNPI
Limited Dissemination Control: NOFORN
POC: John Brown, 703-555-0123

Note: The absence of an LDC on a document means anyone with an authorized lawful government purpose is permitted access to the information but does not imply or authorize public release.

Controlled by: DDI(CL&S)/IAP
CUI Category: BUDG, PSI
Limited Dissemination Control: FEDCON
POC: osd.pentagon.rsrcmgmt.list.ousd-intel-infosec-mbx@mail.mil

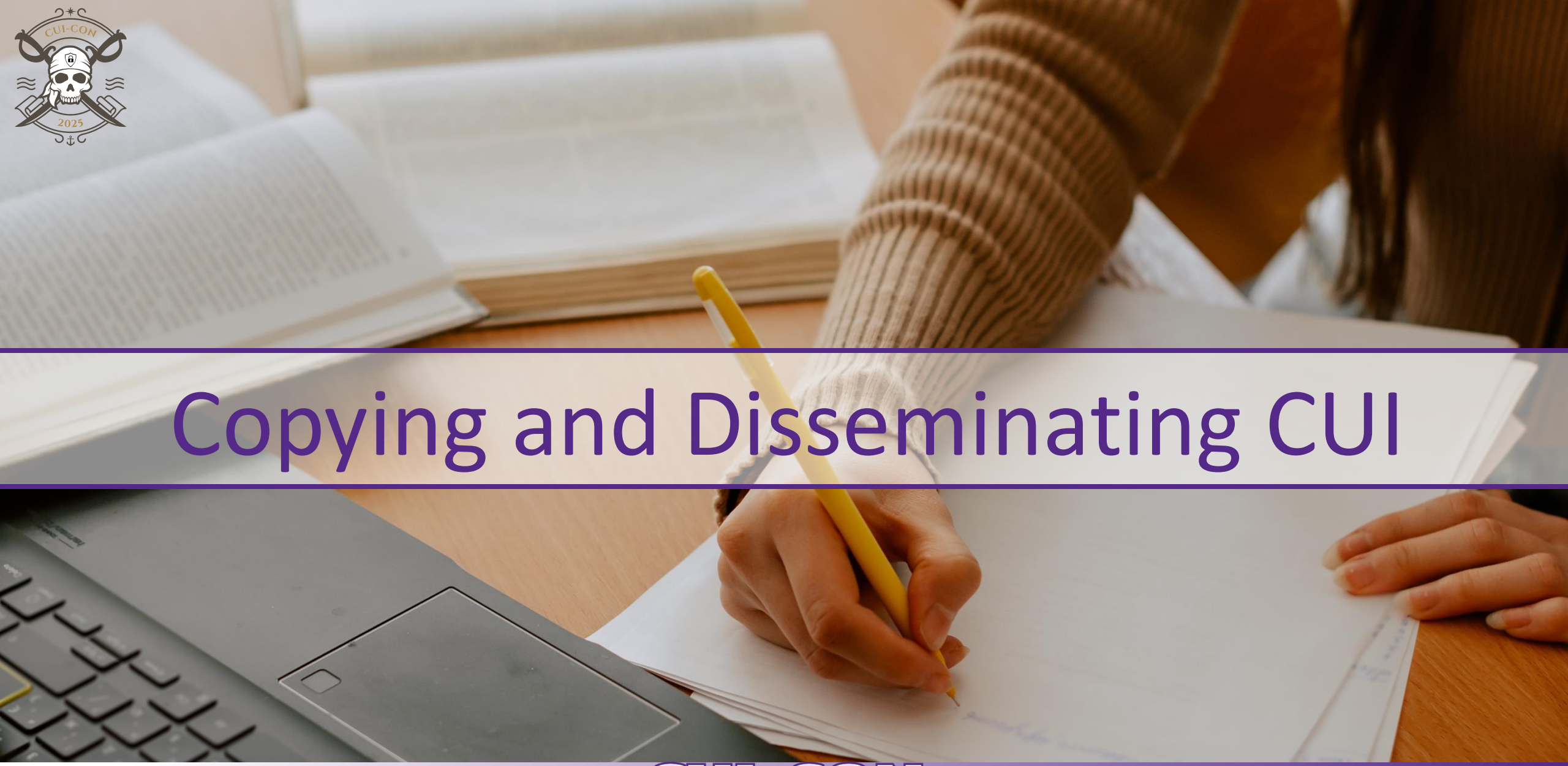
Controlled by: OUSD(I&S)/DDI(CL&S)/IAP
Category: CTI
Distribution Statement: C
POC: John Brown, 703-555-0123

Note: The distribution statement will be written out in full on the first page of the document as well as being annotated by letter in the designation indicator block.

Back to TOC

Markings are for training purposes only

4



Copying and Disseminating CUI

Fathom Cyber
Cybersecurity and Compliance Experts

CUI-CON 2025

Copies and Derivative Works

- CUI is about the protection of information.
- Copies are copies of…the information…and therefore still CUI.
- Derivative works are likely to still be CUI as long as the derivative work includes the attributes or information that made the original work CUI in the first place.
  - This is why the SCG and LRGWP are so important.
  - If you are unsure, safest to assume that information derived from CUI is CUI and to mark it accordingly.
  - Use the same markings as the original CUI.

What About Unmarked CUI?

- If a contractor believes they have received information that is CUI but it is not marked as CUI:
  - They are not authorized to designate information as CUI and therefore must ***NOT*** mark it as CUI.
  - HOWEVER, it must still be **treated** as though it is CUI until told otherwise.
  - Ask your prime contractor or the government if it is CUI.
  - If the government doesn't know, then 32 CFR 2002 says it is not CUI.
    - But THEY (government) need to make that designation determination, **not** the contractor.

A Note About Distribution Statements

- Under DoDI 5230.24, DoD technical Program Managers are authorized to assign Distribution Statements to technical information (Controlled Technical Information) created or disseminated as part of their program.
- If you see Distribution Statement B-F on a document that isn't marked as CUI…it should be treated as CUI.
- Ask the Program Manager for appropriate CUI markings.

1. Authorized Audience or Who Can Access
2. Reason for Control or Why/Reason
3. Date of Determination
4. Controlling Office or Releasing Authority

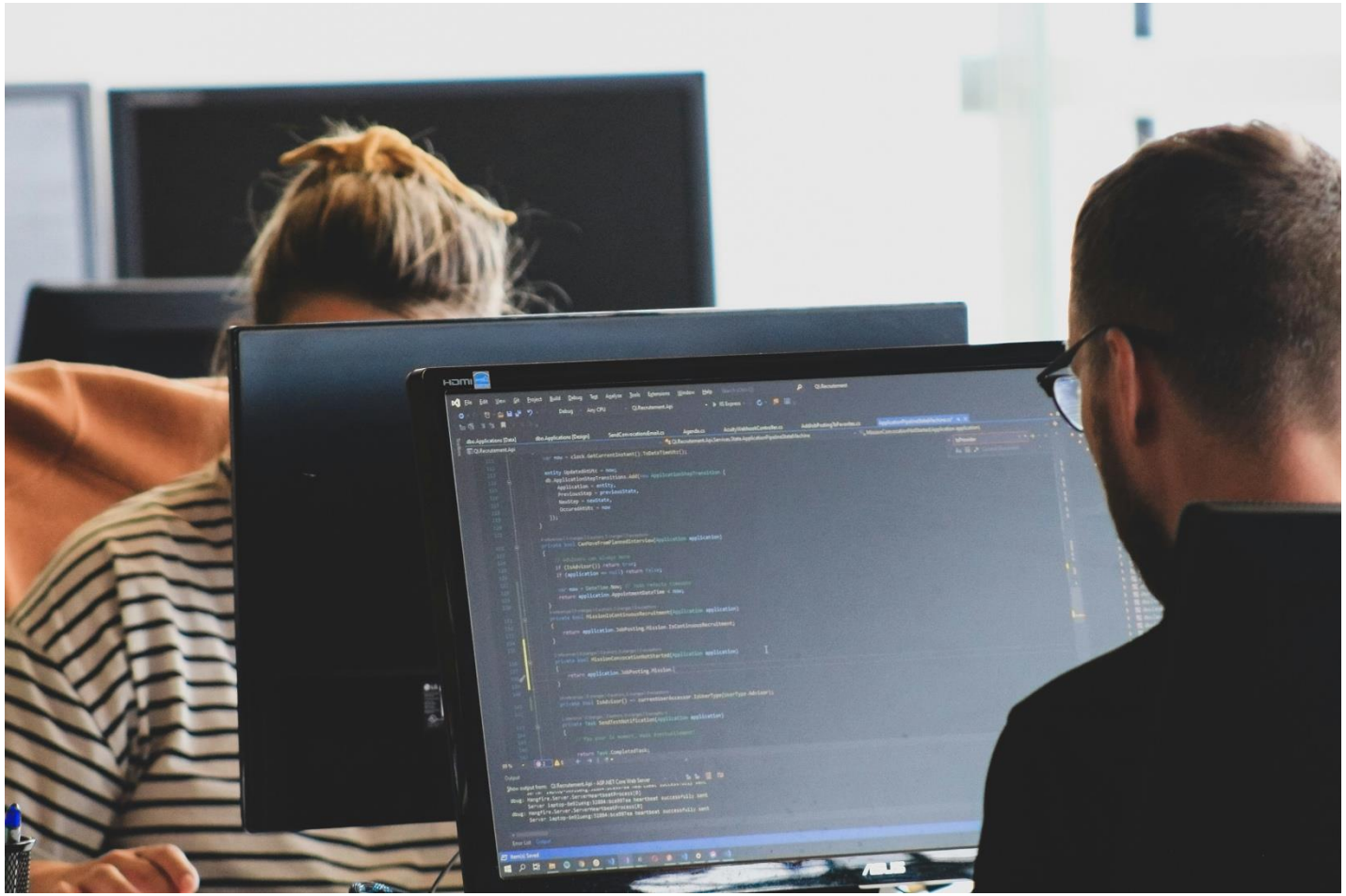
More About Distribution Statements

- DoD's CUI Marking Aid states: "A distribution statement on a document does not automatically mean the document contains CUI. Distribution statements may be used on documents that do not contain CUI."
- While this may be DoD's perspective, it is not correct under 32 CFR 2002.
  - CUI is information against which a LRGWP permits the application of…limited dissemination controls.
  - Once a limited dissemination control is applied, the information is CUI.
  - Only the limited dissemination controls specified in the NARA CUI Registry or those in a LRGWP may be applied to information.
- So…either DoD's use of Distribution Statements as defined in DoDI 5230.24 is contrary to the CUI Program and the IRTPA requirement to create a standardized information sharing environment, or information with distribution statements is subject to a limited dissemination control…making it CUI.
  - Except for Distribution Statement A.
- **If DoD gives you information marked with a distribution statement, other than Distribution Statement A, and says it is not CUI, get that in writing.**

Authorized Holders

- Only Authorized Holders are permitted to handle CUI.
  - This includes being permitted to access systems which handle CUI or locations where CUI is handled.
- To be an Authorized Holder, a person must have a Lawful Government Purpose to access that information.
- Lawful Government Purpose is defined as:
  - "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)." [32 CFR 2002.4]
- Contractors: As a practical matter, if someone needs access to the information to help further the purposes of your contract with the government, then they probably have a Lawful Government Purpose to do so.

Cleaning Crews and Systems Administrators



Disseminating CUI

- Under 32 CFR 2002, an Authorized Holder can disseminate CUI to someone else provided the intended recipient:
  - is an Authorized Holder; and,
  - the disseminator has a reasonable belief that the intended recipient can properly handle CUI.
- How do you prove reasonable belief?
  - Ask LOTS of questions; or
  - Ask for SPRS score and some questions to validate it; or
  - You learn from DoD

CMMC and CUI

- **2019 NDIA Survey:**
  - Nearly half of all contractors had not implemented NIST SP 800-171
  - Over 40% had not even read DFARS 252.204-7012
- **2019 Sera Brynn Study:**
  - Not one company out of the 50 it assessed had properly implemented all 110 controls in NIST SP 800-171
  - Most companies implemented less than thirty-nine percent (39%) of the requirements
- **2022 DIBCAC Assessment Results:**
  - With the introduction of 5-day audits, the average contractor self-assessment score in SPRS dropped by 100 points
- **CMMC:** Third-party validation of a contractor's compliance with NIST SP 800-171 requirements
  - In other words…DoD is building a reasonable belief that it can disseminate CUI to contractors, as required under the CUI program.

Questions?

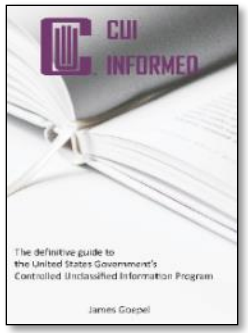
Jim Goepel

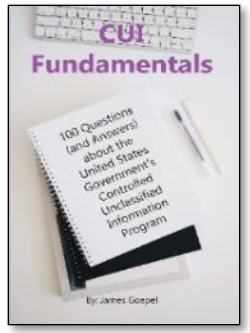
CEO and General Counsel

Fathom Cyber LLC

Jim@FathomCyber.com

Schedule a Meeting:
https://FathomCyber.com/Jim






Thank You