ENTERPRISE SECURITY OPERATIONS (ESO)

FREQUENTLY ASKED QUESTIONS (FAQ's)

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

CUI Branch

27 May 2025, Version 3

CONTENTS

Opening Statement

The Defense Counterintelligence and Security Agency (DCSA) Controlled Unclassified Information (CUI) Frequently Asked Questions (FAQ) has been developed by the CUI Branch, Enterprise Security Operations (ESO) Division that functions as the CUI Program Office for Industry Support (CPOIS). The purpose of the CPOIS is to assist cleared industry in their understanding of CUI contractual and safeguarding requirements. The requirements are associated with classified contracts within the National Industrial Security Program (NISP) as part of the larger Department of Defense's CUI Program Implementation strategy.

The DCSA CUI FAQs was developed through multiple engagements with US Government and Industry stakeholders from 2023 to May 2025. The goal is to assist mission partners to better understand the contractual requirements levied upon industry in support of safeguarding CUI, the government's ability to communicate these requirements, ultimately strengthening DOD oversight of CUI at NISP contractor facilities.

General

Q 1. What are the hours of the CUI Branch Hotline?

A 1. The CUI Branch Hotline (571) 305-4878 is available M-F, 0800-1500. Additionally, the CUI Branch Support Mailbox is available 24/7 at dcsa.quantico.ctp.mbx.eso-cui@mail.mil, answered in the order which it was received.

Q 2. What is controlled unclassified information (CUI)? Is it a new classification level?

A 2. Controlled Unclassified Information (CUI) is not a CLASSIFICATION. CUI is defined as 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 safeguarding or dissemination controls. However, CUI does not include classified information or information a nonexecutive 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.

Q 3. What policies govern CUI?

A 3. Four primary documents govern Controlled Unclassified Information (CUI). Industry and Government partners should familiarize themselves with all such policies.

1. Executive Order 13556 “Controlled Unclassified Information” The Order establishes a uniform program for managing information that requires safeguarding or dissemination controls across the Executive Branch.
2. 32 CFR Part 2002 “Controlled Unclassified Information” Part 2002 establishes the CUI Program throughout the Federal Government and describes the roles, responsibilities, and key elements of the program.
3. DoDI Instruction 5200.48 “Controlled Unclassified Information” This Instruction establishes policy, assigns responsibilities and prescribes procedures for CUI throughout the DOD and establishes an open and uniform program for managing unclassified information that requires safeguarding, or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies.
4. NIST Special Publication 800-171 “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations” This publication identifies the baseline CUI system security requirements for Industry established by Part 2002 of Title 32, CFR.

Q 4. What tools and templates are available for Industry?

A 4. The DOD and other Federal agencies provide several resources and tools for industry and are working on more. The following websites provide helpful resources, Controlled Unclassified Information (CUI) governing policies, and available training:

- **DOD CUI Program Webpage (https://www.dodcui.mil/)**
- **DOD/OCIO CMMC Webpage (https://dodcio.defense.gov/CMMC/)**
- **DCSA CUI Webpage (https://www.dcsa.mil/)**
- **CDSE CUI Training (https://securityawareness.usalearning.gov/cui/index.html)**
- **CDSE CUI Toolbox (https://www.cdse.edu/Training/Toolkits/Controlled-Unclassified-Information-Toolkit/)**

Q 5. What is DCSA's role regarding the CUI Program?

A 5. The Defense Counterintelligence and Security Agency (DCSA) role within the Controlled Unclassified Information (CUI) Mission space to provide Security Education, Awareness, Advisement, and Assistance. DCSA has established the Controlled Unclassified Information (CUI) Program Office for Industry Support (CPOIS) with the goal to provide Industry with a better understanding of the contractual requirements levied upon industry in support of CUI Safeguarding, the government's ability to communicate these requirements, ultimately strengthening DOD oversight of CUI at NISP contractor facilities.

Controlled Unclassified Information (CUI) Access

Q1. Can you discuss the safeguarding requirements for NATO Restricted? The NISPOM describes this marking as a NATO security classification level (32 CFR 117.19(g)(2)); however, it's also listed as a CUI category in the ISOO registry. NATO Instruction 1-07 may better describe the required safeguarding, but I haven't been able to locate a copy.

A1. Please follow guidance within 32 CFR Part 117.19(g) and applicable contractual requirements, the section provides the security requirements needed to comply with the procedures established by the U.S. Security Authority for NATO Affairs Instruction 1-07 for safeguarding NATO information provided to U.S. industry. Please contact your Industrial Security Representative (ISR) and Government Contracting Activity (GCA) for further assistance as Controlled Unclassified Information (CUI) safeguarding requirements outside of the 32 CFR Part 117.

Q 2. Is DOD following the same process and timeline for CUI as are other federal agencies?

A 2. Yes, The Department of Defense (DOD) has developed and is in the process of implementing a mature Controlled Unclassified Information (CUI) Program that meets the government-wide requirement directed by Executive Order 13556. Currently, each federal agency within the executive branch is in the process of implementing a CUI Program according to their respective organizational timelines.

Marking

Q 1. Does CUI include personally identifiable information (PII) and health insurance portability and accountability act (HIPAA) requirements?

A 1. Yes, PII and HIPAA fall under one of the 9 **Privacy Categories** that also have additional legal protection requirements that require consideration and may supersede Controlled Unclassified Information (CUI) requirements. Industry is encouraged to work with their Contracting Officer Representative (COR) to understand the contractual requirements for the handling safeguarding of each CUI Category.

Q 2. How is CUI marked?

A 2. At a minimum, Controlled Unclassified Information (CUI) markings for unclassified DOD documents will include the acronym "CUI" in the banner and footer of the document. Portion markings may also be used but are not required. Marking requirements apply to documents, emails and forms of media that are designated as CUI. Furthermore, marking labels are available for media such as USB sticks, hard drives, and CD ROMs to alert holders to the presence of CUI stored on the device.

Q 3. Where are CUI categories located?

A 3. There are two Controlled Unclassified Information (CUI) Registries for DOD Contractors that provide a list of approved categories.

- **DOD CUI Registry (https://www.dodcui.mil/CUI-Registry-New/)**
- **National CUI Registry (https://www.archives.gov/cui/registry/category-list)**

DoD agency personnel and contractors should first consult the DOD CUI Registry to find the Indexes and Categories of information most used within DoD. The DOD CUI Registry is a subset of the National Registry and is aligned to DoD authorities, policies and Issuances. The National CUI Registry contains Indexes and Categories for the entire Executive Branch and should be consulted for non-DOD contracts.

Q 4. If CUI is to be determined by a Gov't entity, how would a contractor who generates a document with PII mark it as CUI?

A 4. Personally identifiable information collected on behalf of the company or for the purpose of industry use should be protected in accordance with that company's policy, applicable law, and industry standard. Once the information is transmitted to the government, it will be safeguarded as Controlled Unclassified Information (CUI).

Q 5. SF312s (Non-Disclosure Agreements) include full name and SSNs. It is a government standard form but not marked "CUI when filled in" like some other forms (for example, the PSSAR DD Form 2962). Should we the contractor be taking it upon ourselves to mark them as CUI? We have been told yes, then no, then yes again from different DCSA reps.

A 5. The Standard Form 312 is an Security Enterprise form and not used exclusively in DoD. As such, the contractor is not obligated to mark the form for DoD purposes; the form will be marked upon receipt by the US Government requiring its use. Additionally, DOD does not utilize SF-312s as a Non-Disclosure Agreement exclusively for accessing Controlled Unclassified Information (CUI)

Q 6. We have Product X that was developed for a US contract. All the source files are marked CUI. A new commercial contract comes in for Product Y and we will be using Product X as a baseline for the new design. Should the source files for Product Y be marked CUI since the design they are being derived from was CUI? Or should they not be marked CUI since the contract for Product Y is commercial?

A 6. Yes. When integrating Controlled Unclassified Information (CUI) into a new document, the new document must retain the necessary markings and controls to ensure proper safeguarding and dissemination of the newly created document.

Q 7. The CDSE Training toolkit has a tab instructing contractors how to identify CUI. I thought a contractor is not allowed to determine what CUI is and that direction must come from the government customer for marking purposes?

A 7. Controlled Unclassified Information (CUI) is defined in Section 2002.4 of Title 32 CFR as 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/organization to handle safeguarding or dissemination controls.

Q 8. DOD Prime Contractors send my company technical documents containing DISTRIBUTION STATEMENT D, but these documents are not marked as CUI or CUI/SP-CTI. Are these documents considered CUI if they are not marked appropriately as CUI?

A 8. Controlled Unclassified Information (CUI) is CUI and shall be safeguarded accordingly, please follow guidance provided in the DOD CUI Registry and specific contract requirements. Additionally, it is recommended that you work with your GCA, identifying the appropriate CUI category, Distribution D statement are to include dissemination list for government and contractor with a dissemination list that limits access to the specified individuals, groups, or agencies and must accompany the document. Reference DODI 5200.48, Section 4: Dissemination, Decontrolling, and Destruction of CUI.

Q 9. Who would we list in the designation block for controlled by? Distribution statement? POC?

A 9. When dealing with the Controlled Unclassified Information (CUI) designation indicator box, controlled by refers to the name of the DOD Component (not required if identified in the letterhead) and identification of the office creating the document. Distribution statement: identifies which group of individuals who are allowed to have CUI designated information disseminated to them. POC: name and phone number or email of POC. Organizational emails can be used.

For Example:

Controlled by: [Name of DOD Component/ Agency] (Name of GCA)
Controlled by: [Name of Office] (Company Name)
CUI Category: (List category or categories of CUI)
Distribution/Dissemination Control: (What distribution Statement or LDC)
POC: [Phone or email address] (Person / office creating documents)

Distribution statements can be found at DODI5200.48, DODM 5200.01 Vol 2, and **DOD CUI Marking Aid** (https://www.dodcui.mil/).

Q 10. If industry has a document they update annually and was originally marked as FOUO prior to CUI implementation, can industry start marking that document as CUI or is approval needed for that?

A 10. DOD legacy material will not be required to be re-marked or redacted while it remains under DOD control or is accessed online and downloaded for use within the DOD. However, the information previously marked as FOUO is incorporated into a new document, that information must be assessed to determine if it meets the criteria for continued protection as Controlled Unclassified Information. If it is determined the information meets the criteria for CUI, the information shall be appropriately marked.

Q 11. We have zero Security Classification Guides (SCGs) for unclassified contracts, but we handle some CUI and create material using that CUI. What is the link to the DTIC website where we can check for SCGs?

A 11. Security Classification Guide (SCG) can be located at the DTIC website (https://discover.dtic.mil.), it is recommended to coordinate with your GCA for the use of and or requesting SCG.

Q 12. Many forms are now often labeled as "CUI when completed". When we complete the form is it CUI immediately or as soon as it is sent to the government customer? There is no place on the form to put in a designation block. Where should we put that? On the cover page?

A 12. If the form being created is supporting contractual requirements and used by the government, then yes, the form should be marked as Controlled Unclassified Information (CUI). Additionally, the form creator will need to coordinate with the GCA/requester of the information to determine additional transmission guidance of the completed form.

Q 13. I am confused as it states, in writing, that CUI is originated and owned by the Government. That's in writing by the Government! So how can we, as industry, originate CUI?

A 13. Controlled Unclassified Information (CUI) is defined in Section 2002.4 of Title 32 CFR as 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/organization to handle safeguarding or dissemination controls.

Q 14. When I run a report in DISS, in order to view it, I have to download it to my computer. That's automatically CUI on my computer. Is there a way to view the report without downloading it?

A 14. Currently, we are not aware of how to view the report without downloading, it is recommended that industry contact the DISS Program Office for additional guidance.

Q 15. What is the difference between Federal Contract Information (FCI) and Controlled Unclassified Information (CUI)? FCI is information not intended for public release. FCI is provided by or generated for the Federal Government under a contract to develop or deliver a product or service.

A 15. Controlled Unclassified Information (CUI) and Federal Contract Information (FCI) share important similarities and a particularly important distinction. FCI is any information that is 'not intended for public release,' CUI is information that requires safeguarding and may also be subject to dissemination controls. FCI is defined in Federal Acquisition Regulation (FAR) clause 52.204-21, and CUI is defined in Title 32 CFR Part 2002. The **DOD CUI Quick Reference Guide** (https://www.dodcui.mil) includes additional information on the marking and handling of CUI.

Q 16. What are legacy materials, and do they need to be remarked for CUI?

A 16. Sensitive types of unclassified information (such as information marked as FOUO or SBU) that was marked prior to the implementation of the Controlled Unclassified Information (CUI) program which meets the standards for CUI is considered legacy information. Legacy documents do not need to be remarked until and unless the information is re-used, restated, or paraphrased. When new documents are created using legacy information, they must be assessed to determine if the newly created document meets the criteria and standard for Controlled Unclassified Information.

Q 17. What are the requirements for disseminating, decontrolling, and destroying CUI?

A 17. Similar to other information requiring safeguarding, there are contractual, agreements, laws, regulations, Government-wide policy and guidance, safeguarding requirements regarding dissemination, decontrol, and destruction of Controlled Unclassified Information (CUI). While the points below highlight these requirements, one should consult DoDI 5200.48 for a more comprehensive description.

- Disseminate. Authorized holders may disseminate CUI in accordance with distribution statements and applicable laws. Dissemination is allowed 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. CUI information and material can be sent via first class mail, parcel post, or bulk shipments. CUI can also be transmitted by encrypted e-mail when practical, via approved secure communications systems, or systems using other protective measures **DoD SAFE** (https://safe.apps.mil/).

- Decontrol. Once information is no longer CUI, it must be promptly decontrolled. Prior to decontrolling, the Director of the Washington Headquarters Services (WHS) will review CUI documents and materials for public release, in accordance with DoDI 5230.09. Once it is determined that the information no longer requires protection from public disclosure, the Federal Government will notify all known holders of the decontrolled information.

Destroy. If there is no longer a use for CUI documents or materials, all hard and soft copies should be destroyed rendering it unreadable, indecipherable, and irrecoverable.

Q 18. Who can create CUI?

A 18. Anyone can create Controlled Unclassified Information (CUI)as long as it is generated for, or on behalf of, an Executive Branch agency under a government contract, and it falls into one of the over one hundred DOD CUI categories.

Q 19. Is corporate intellectual property CUI?

A 19. By default, No. Controlled Unclassified Information (CUI) is not corporate intellectual property unless created for or included in requirements related to a government contract. This includes information and material related to or associated with the following categories when created specifically for the DOD:

A company's products, business, or activities, including but not limited to financial information

- Data or statements
- Trade secrets
- Product research and development
- Existing and future product designs and performance specifications
- Marketing plans or techniques
- Schematics
- Client lists
- Computer programs
- Processes

Also, be aware of how these categories have been identified and properly marked by the company as proprietary information, trade secrets, or company confidential information. The information must have been developed by the company and not be available to the Government or to the public without restriction from another source. When these conditions are met the information falls into the Proprietary Business Information category of CUI.

Q 20. What if an agency doesn't use CUI markings and continues to use FOUO (like NSA)?

A 20. Not every Executive branch agency has implemented Controlled Unclassified Information (CUI), so you may receive documents marked as FOUO. Documents with other markings should be handled in accordance with guidance from that government entity.

Q 21. What do we do if the document is a .pdf form that we cannot remark it from FOUO to CUI?

A 21. DOD legacy material will not be required to be re-marked or redacted while it remains under DOD control or is accessed online and downloaded for use within the DOD. However, any such document or new derivative document must be marked as Controlled Unclassified Information (CUI) if the information qualifies as CUI and the document is being shared outside DOD.

Q 22. I see where PII should be marked as CUI. As security officers we constantly pass PII through email (pw protected docs). Should we be marking the doc and email CUI?

A 22. Personally identifiable information collected on behalf of the company or for the purpose of industry use should be protected in accordance with that company's policy, applicable law, and industry standard. Once the information is transmitted to the government, it will be safeguarded as Controlled Unclassified Information (CUI).

Q 23. NSA has said they will not transition from FOUO to CUI - are there plans to force them to convert?

A 23. The IC has decided to continue to use FOUO for marking their information, if they are accessing DOD information then they will follow the marking requirements outline in DODI 5200.48.

Q 24. Do we need to mark all PII as CUI?

A 24. Personally identifiable information collected on behalf of the company or for the purpose of industry use should be protected in accordance with that company's policy, applicable law, and industry standard. Once the information is transmitted to the government, it will be safeguarded as Controlled Unclassified Information (CUI).

Q 25. DISS Reports are labeled as "CUI." These reports must be downloaded to 'VIEW' them. DCSA must recognize that not all DIB contractors are required to meet the 7012 FAR Clause (if it is not flowed down in the contract) and/or are not approved for CUI handling. Does DCSA plan to make the reports VIEWABLE so that contractors can continue to use the reports feature? (Regarding the DISS reports, the excel version is not marked as CUI only the PDF version of the DISS subject report has CUI markings).

A 25. As of Today all documents in DISS are considered Controlled Unclassified Information (CUI) unless otherwise marked. It is the responsibility of the Authorized Holder (AH) to ensure that the company system meets the minimum CUI safeguarding requirements prior to download.

Q 26. If a company (Acme, Inc) is creating CUI (Technical report, Test data, Blueprints, etc.) on behalf of a contract that was issued by a branch of the DOD where the 7012 clause is flowed down. a. Who is the controlled by line in the Designation Indicator? Would it be Acme, Inc or the Agency or branch who issued the contract?

A 26. Please follow the guidance in DODI5200.48, DODM 5200.01 Volume 2, and **DOD CUI Marking Aid.** (https://www.dodcui.mil/)

For Example:

Controlled by: [Name of DOD Component/ Agency] (Name of GCA)
Controlled by: [Name of Office] (Company Name)
CUI Category: (List category or categories of CUI)
Distribution/Dissemination Control: (What distribution Statement or LDC)
POC: [Phone or email address] (Person / office creating documents)

Training

Q 1. The presenter mentioned that if CUI is checked on the DD254 then CUI training is required. Who should receive that training? All employees, those with access to the CUI, or a different group/different person?

A 1. All employees are to complete Controlled Unclassified Information (CUI) training initially and annually thereafter, based on requirements outline in the DODI 5200.48, contractual requirement documents, and that are consistent with law, regulation and government wide policy.

Q 2. Could you please repeat the website that has CUI training? I believe you said we need an account. can you drop the link to the CUI section / resources of the DCSA website?

A 2. Training resources are available on the **CDSE/STEPP** website (https://www.cdse.edu). You can also visit **DOD CUI Program Office** (https://www.dodcui.mil/Training) for additional Controlled Unclassified Information (CUI) training resources.

Q 3. Is CUI training available? Is it mandatory?

A 3. The Center for Development and Security Excellence (CDSE) provides Controlled Unclassified Information (CUI) training that is available to Industry. Per DoDI 5200.48 and pursuant to contractual requirements, DOD contractors require initial Controlled Unclassified Information (CUI) training and annual refresher training thereafter.

Safeguarding (Contracts, DD-254)

Q 1. When would PII be considered CUI. We have been told that not all PII is CUI? Would it be CUI ONLY when the PII is created, or if it is provided in support of the contract?

A 1. Personally identifiable information collected on behalf of the company or for the purpose of industry use should be protected in accordance with that company's policy, applicable law, and industry standard. Once the information is transmitted to the government, it will be safeguarded as Controlled Unclassified Information (CUI).

Q 2. We are (still) seeing contracts that specify CUI applies, but not specifically identifying what CUI is (as it pertains to this contract). Is there a plan in place to verify contracts properly including the appropriate information so we don't have to keep asking the customer to clarify?

A 2. As agencies are in different stages of implementing Controlled Unclassified Information (CUI) programs it is recommended to continue to work with your GCA on identifying the type of CUI that you are handling per your contractual requirements. CUI is identified in your DD-254 (Block 10 (J), Block 11 (I) & Block 13), section K of your contract, and other contractual documentation (SOW/ SCG) that may outline safeguarding requirements.

Q 3. If we want to send CUI to a vendor to fabricate a part, how do we verify that the vendor can safeguard the CUI other than them just saying they can.

A 3. The Industry Partner should validate subcontractor contractual requirements by asking the subcontractor or with their GCA to validate the subcontractor meets contractual Controlled Unclassified Information (CUI) safeguarding requirements.

Q 4. If we have FCI or CUI and disassociate the contract/program number/name and platform, is the information still considered CUI? For Example, would we be able to flow the information to subs without flowing down the CUI requirement?

A 4. No. Controlled Unclassified Information (CUI) is CUI and shall be safeguarded accordingly, please follow the guidance provided in the DOD CUI Registry and flow down the specific contract requirements to subcontracts. Additionally, it is recommended that you work with your GCA, identifying the appropriate CUI category.

Q 5. If we have a document pertaining to a contract and we believe it should be marked CUI (but isn't), can we mark it CUI?

A 5. Yes, if you believe that the document is Controlled Unclassified Information (CUI), please safeguard it as such and contact your GCA immediately to verify if the document contains CUI.

Q 6. Question that just came up at my facility today regarding CUI. Does CUI need to be removed/hidden in a room like you would for secret/top secret before catering/cleaning staff enter?

A 6. Actions should be taken to prevent an unauthorized disclosure of Controlled Unclassified Information (CUI. Additional guidance may be found at DODI 5200.48, Section 4.1.e.2, specific CUI category, and or contractual requirements provided by the GCA.

Q 7. Is it mandatory to report CUI mishandling at https://dibnet.dod.mil/dibnet or is it a best practice? I have followed the requirements of the DD254 in the past.

A 7. If DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting, is required by contract shall rapidly report cyber-incident that affects a covered contractor information system or the covered defense information or that affects the contractor's ability to perform the requirements of the contract. Cyber-incident reports shall be reported to **Defense Industrial Base (DIB) Cybersecurity Portal** (https://dibnet.dod.mil/dibnet), the Government Contracting Activity (GCA) and in accordance with law, regulation or government wide policy. DODI 5200.48, General DOD Controlled Unclassified Information (CUI) Administrative Requirements Paragraph 3.5.a(4) Report misuse, mishandling, or UD of CUI to the Unauthorized Disclosure Program Management Office.

Q 8. Where does industry go with questions or concerns about how CUI is being implemented for existing contracts?

A 8. When contract-specific questions or concerns arise, Industry is encouraged to work with their Government Contracting Activity (GCA) and follow guidance issued by the DOD Contracting Authority and DFARS 252.204-7012. As with all security issues, Industry Facility Security Officers (FSOs) should ensure their organizations appropriately implement Controlled Unclassified Information (CUI) requirements. They are encouraged to work with DCSA Controlled Unclassified Information (CUI) Program Office for Industrial Support (CPOIS) and their assigned Industrial Security Representatives (ISR) as appropriate.

Q 9. What can industry do to prepare for CUI if it currently has no contracts that specifically require it?

A 9. Even if an Industry partner currently has no contracts with Controlled Unclassified Information (CUI) requirements, they are encouraged to understand that unclassified engagements with the DOD can also include Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) data that are not necessarily a part of a classified DOD contract. Industry should also ensure they understand CUI policies and safeguarding requirements for future work.

Q 10. What responsibility does a prime contractor have to ensure its subcontractors and suppliers comply with the CUI program?

A 10. As with most compliance requirements, a prime contractor is responsible for ensuring that all teammates, including subcontractors, and suppliers, meet applicable security requirements. Prime contractors should refer to 32 CFR Part 117, DoDI 5200.48, FAR 52.204-21, and DFARS 252.204-7012 to understand their obligations.

Q 11. How will industry know its contracts require CUI?

A 11. The federal entity requesting services shall determine CUI requirements for both unclassified and classified contracts. Controlled Unclassified Information (CUI) shall be identified in the issuing DD

FORM 254, Request for Quote (RFQ), Request for Proposal (RFP), and supporting contract documentation when they exist. For existing contracted efforts, Industry should review current contracts and engage with Government Contracting Activity (GCA) to determine which, if any, Controlled Unclassified Information (CUI) requirements are applicable to current contracts and the appropriate way forward.

Q 12. Who is responsible for controlling CUI?

A 12. Anyone who creates information that is considered Controlled Unclassified Information (CUI) is responsible for safeguarding and correctly handling it. DOD contracts are required to use the DOD CUI Registry, identify DOD contractual requirements, and continuously work with Government customers to ensure that they meet all CUI safeguarding requirements within the contract.

Non-Federal Systems Requirements (CMMC, FEDRamp)

Q 1. Can CUI be processed through Artificial Intelligence programs?

A 1. Currently DOD does not have an official policy for AI processing of Controlled Unclassified Information (CUI), however, some GCAs and CSAs may require ATOs and compliance with existing safeguard regulations such as NIST SP 800-171. We recommend caution and or avoidance when considering the use of AI programs until authorizing law, regulation, or Government-wide policy implements specific safeguarding requirements. We also recommend coordinating with the GCA if further information or guidance is required.

Q 2. When will DCSA begin conducting CUI-related inspections?

A 2. DCSA will **NOT** be conducting Controlled Unclassified Information (CUI)-related Security Reviews. Industry is urged to implement CUI safeguards if it has not already done so and ensure they are aware of CMMC requirements.

Q 3. Have you heard of any update that if you had a DIBCAC high assessment you will be granted CMMC level 2 cert?

A 3. The (Cybersecurity Maturity Model Certification) CMMC process falls under the DOD OCIO cognizant, and it is recommended to contact them directly for further clarification as it relates to details of the **CMMC** (https://dodcio.defense.gov/CMMC/).

Q 4. For your first Level 2 assessment, how many years of records are assessed? (How many years of historical records do you need to provide for the assessment)?

A 4. The (Cybersecurity Maturity Model Certification) CMMC process falls under DOD OCIO cognizance, and I would recommend contacting them directly for further clarification as it relates to details of the **CMMC** (https://dodcio.defense.gov/CMMC/).

Q 5. Our CUI machines are standalones without network access. Is there an overlay, like for classified machines, that removes the network related controls from 800-171 for CUI?

A 5. Currently unaware of NIST SP 800-171 overlay guidance for Controlled Unclassified Information (CUI) certified systems.

Q 6. In the DCSA CUI Branch updates presentation, does Slide 8 references DoD OCIO? Does that stand for Dept of Defense Office of Chief Information Officer?

A 6. It stands for **The Office of the Chief Information Officer** (https://dodcio.defense.gov/).

Q 7. How does CUI align with cybersecurity maturity model certification (CMMC)?

A 7. Cybersecurity Maturity Model Certification (CMMC) aims to enhance the cybersecurity posture of the Defense Industrial Base (DIB) by establishing a standardized set of requirements for safeguarding Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

Q 8. How can industry learn more about the approved systems and services available for handling CUI?

A 8. When establishing a non-federal systems baseline, Industry may reference the NIST SP 800-171 and the Cybersecurity Maturity Model Certification (CMMC) to learn more about systems requirements for handling of Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

When considering the selection of services, for example, Cloud Service Provider (CSP), Industry should contact their Government Contracting Authority (GCA) to request guidance on FedRAMP approved products/services provided by the CSP is used to process, store, or transmit FCI and CUI. The Cloud Service Offering (CSO) must meet FedRAMP Moderate, or equivalency requirements as determined by DoD policy.

Encryption (DOD SAFE, Password Protection)

Q1. Will DoD SAFE be available for Industry to use for CUI transfers?

A1. DOD SAFE is available for industry use, when the established communication comes from the government transmitting Controlled Unclassified Information (CUI) to industry. However, when the contractor downloads the CUI information, they are stating that their system meets the minimum requirements that are required for safeguarding CUI.

Q2. If I'm able to encrypt PII, do I need to use CUI email or only CUI markings?

A2. Personally identifiable information (PII) collected on behalf of the company or for the purpose of industry use should be protected in accordance with that company's policy, applicable law, and industry standard. Once the information is transmitted to the government, it will be safeguarded as Controlled Unclassified Information (CUI).

Q3. Is password protection sufficient for transmitting CUI attachments from contractor to contractor when the IT system is not approved for handling CUI?

A3. No. An approved method for securely transmitting Controlled Unclassified Information (CUI) between entities is DOD SAFE (https://safe.apps.mil/).

Q4. I have a question regarding protecting CUI when transmitting via EMAIL. I have been told that by transmitting CUI on our email cloud (FEDRAMP High) the transmission between our employees the CUI is protected because it is on our servers and in compliance with NIST rules and policies. My bigger question is if there is a level of encryption that must be used between two FEDRAMP High systems when transmitting between the two (two separate companies and not on the same FEDRAMP High cloud system. Where would I go to find out what is TRULY required to transit CUI via email between two entities whether it is GOV to Contractor, Contractor to GOV, GOV(Navy) to GOV(Army), or Contractor to Contractor?

A4. An approved method for securely transmitting Controlled Unclassified Information (CUI) between entities is DOD SAFE (https://safe.apps.mil/).

Q5. If someone sends CUI unencrypted, wouldn't that be a security violation?

A5. Unauthorized disclosure occurs when an Authorized Holder (AH) of Controlled Unclassified Information (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.

Q6. Do you need to encrypt emails to others in your organization if your network/environment is CUI complaint?

A6. Yes, per DOD CUI policy, all emails containing Controlled Unclassified Information (CUI) should be encrypted. An approved alternate method for sending CUI securely is through DOD SAFE (https://safe.apps.mil/).

Q 7. What type of reporting requirement is needed when a government customer sends a CUI document via e-mail, but they fail to place the required CUI marking?

A 7. Industry partners should coordinate and work with the GCA to properly report this potential unauthorized disclosure incident.

Q 8. If a government customer sends a contractor an e-mail unencrypted, what if there is any clean up procedure from the contractor side? Is there a cleanup requirement for CUI?

A 8. If DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting, is required by contract shall rapidly report cyber-incident that affects a covered contractor information system or the covered defense information or that affects the contractor's ability to perform the requirements of the contract. Cyber-incident reports shall be reported to DOD at https://dibnet.dod.mil, the GCA and in accordance with law, regulation or government wide policy. DODI 5200.48, General DOD CUI Administrative Requirements Paragraph 3.5.a(4) Report misuse, mishandling, or UD of CUI to the Unauthorized Disclosure Program Management Office.

Q 9. What do we do when the government is not sending CUI documents or information encrypted? This happens all the time, or they are sending it Password protected through Adobe but that does not meet the requirement.

A 9. Industry partners should coordinate and work with the Government contracting activity (GCA) and Contracting Representative Officer (COR) to properly report this as a potential unauthorized disclosure. One approved method for securely transmitting Controlled Unclassified Information (CUI) between entities is DOD SAFE (https://safe.apps.mil/).

Q 10. We have someone that wants to send us a document marked CUI. What are the requirements to be able to receive CUI via email?

A 10. Currently an approved method to send Controlled Unclassified Information (CUI) to Industry is through DOD SAFE, as all CUI communications are to be encrypted. Additional information for disseminating CUI reference 32 CFR Part 2002: 16 Accessing and disseminating. (c) Methods of disseminating CUI, (2).

Personnel Security (Clearance, Citizenship)

Q 1. Are dual citizens authorized to access CUI?

A 1. Dual citizens with U.S. citizenship, are afforded the same rights of a U.S. citizen and may not be considered a foreign national. As a citizen of a foreign country that doesn't present a risk to the national security of the United States, a U.S. Dual citizen may be granted access to Controlled Unclassified Information (CUI) for a lawful government purpose, when authorized by and coordinated with the GCA and associated with a government contract. Access to CUI may be limited by agreement, law, regulation, Government-wide policy, or by specific safeguarding requirements that may restrict the access of dual citizens and or foreign nationals.

Q 2. Our government customers will not allow access to CUI without a SECRET clearance. Are you saying this is not, correct?

A 2. Controlled Unclassified Information (CUI) safeguards are contractually based, companies should reach out to their Government Contracting Activity (GCA) to gain a better understanding of the additional contractual requirements.

Q 3. We have a contract that has CUI-Controlled Nuclear information, and they are requiring employees or subcontractors to have a Tier 3 investigation for access to this information. Is the government allowed to require investigations for CUI even though there is no policy for it?

A 3. Controlled Unclassified Information (CUI) safeguards are contractually based, companies should reach out to their GCA to gain a better understanding of additional contractual requirements that may be driving the requirements for having contractors processed for Tier 3 investigations.

Q 4. Am I correct that CUI cannot be shared with foreign nationals without the permission of the government customer? Or is that only for CUI marked NF?

A 4. DOD Personnel may provide Controlled Unclassified Information (CUI) to foreign entities to conduct official business for DOD and the United States Government if there is a lawful government purpose. Additionally, the Authorized Holder must ensure that the specific CUI category of information does not restrict the release to Foreign Nationals. (Example: EXPT) Consult with GCA for concurrence prior to sharing CUI with foreign entities. Additional CUI Policy Memoranda, the **Revised Policy on Sharing CUI with Foreign Entities, 20240131** (https://www.dodcui.mil/) and **Clarification to Controlled Unclassified Information Policy Regarding Disclosures to Members of Foreign Governments, 20211129** (https://www.dodcui.mil/) are available on the **DOD CUI Program Office Website** (https://www.dodcui.mil/).

Q 5. We had a government entity tell us that we could not let someone with a secret clearance see CUI information. Is that correct?

A 5. Unlike classified information, an individual or organization does not need to demonstrate a need-to-know to access Controlled Unclassified Information (CUI). Access to CUI is limited by a lawful government purpose or otherwise prohibited by any other law, regulation, or government-wide policy.

Q 6. If CUI is unclassified why does the person need a favorable adjudication?

A 6. Unlike classified information, an individual or organization does not need to demonstrate a need-to-know to access Controlled Unclassified Information (CUI). Access to CUI is limited by a lawful government purpose or otherwise prohibited by any other law, regulation, or government-wide policy.