Supply Chain Cyber Academy

If after using this resource, you find your question is not addressed, please direct questions and/or comments to the DIB SCC CyberAssist website.

This information is provided for your convenience and not as an endorsement by the Defense Industrial Base Sector Coordinating Council (DIB SCC) Supply Chain Task Force of the information on such External Sites. It is provided on an "as is" basis without warranties of any kind, express or implied. DIB SCC and its members or any individual participants disclaim any responsibility or liability with regards to the information or content posted on referenced external sites. This does not constitute legal advice and organizations should consult their own compliance experts or counsel.

Frequently Used Acronyms

C3PAO: CMMC 3rd Party Assessor Organization

CDI: Covered Defense Information

CMMC: Cybersecurity Maturity Model Certification

CTI: Controlled Technical Information

CUI: Controlled Unclassified Information

DIBCAC: Defense Industrial Base Cybersecurity Assessment Center

DFARS: Defense Federal Acquisition Regulation Supplement

DoD: Department of Defense

FCI: Federal Contract Information

NARA: National Archives and Records Administration

NIST: National Institute of Standards and Technology

POA&M: Plan of Action and Milestones

General Webinar Questions

GW1. Will slides be available?

Slides are available on the CyberAssist website under the CMMC Training section (note: there are separate tabs for CMMC Level 1 vs. CMMC Level 2 training content). The link to the slides was also provided in the meeting invite.

GW2. Will this webinar be recorded/will a recording be made available?

This webinar will not be recorded, but the slides are available via the CyberAssist website under the CMMC Training section (note: there are separate tabs for CMMC Level 1 vs. CMMC Level 2 training content). The link to the slides was also provided in the meeting invite.

GW3. Is the survey required?

The survey is optional, but we highly encourage you to complete it to help improve future training sessions: https://ndisac.org/dibscc/cyberassist/cybersecurity-maturity-model-certification/cmmc-training-level-2-survey/

GW4. In the content legend, what is the difference between L1 Content vs L2, etc.?

Per the legend, CMMC L1 Content pertains to security practices specific to the protection of Federal Contract Information (FCI). CMMC L2 Content pertains to security practices specific to the protection of Controlled Unclassified Information as required by DFARS 252.204-7012 and NIST SP 800-171. CMMC L3 Content pertains to security practices that are to be defined by the DoD. Non-CMMC Content/Extra pertains to content that is unrelated to CMMC, but provides additional security considerations (i.e., security best practices, risk management)

Controlled Unclassified Information (CUI)

CUI1. How are Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) defined and who decides what constitutes is CUI? Is it a flow-down from the Government/OEM or is this on the contract supplier?

Federal Contract Information (FCI) is 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. (Source: 48 CFR 52.204-21)

Controlled Unclassified Information (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. (Source: 32 CFR § 2002.4)

- Note: This 32 CFR and the CUI Registry are government resources that apply solely to government agencies. Contractor obligations regarding these are flowed down to contractors through other contractual requirements such as DFARS 252.204-7012.

What constitutes as CUI is defined by the Government and the current list can be found within the National Archives CUI registry at: https://www.archives.gov/cui/registry/category-list. Additional DoD CUI information can be found at: https://www.dodcui.mil/

Covered Defense Information (CDI) is unclassified controlled technical information or other information, as described in the 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. (Source: DFARS 252.204-7012)

Controlled technical information (CTI) means 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. (Source: DFARS 252.204-7012)

CUI2. How do I know if I'm handling CUI on a Government contract? (How are suppliers identified as handling CUI, and where is that designated?)

United State Government (USG) agencies are responsible for marking CUI that they provide and for providing marking instructions to contractors for CUI they generate. CUI should be labeled or otherwise identified in the contract as CUI. USG, DoD, or Contractors are required to mark data as CUI/CDI in accordance with contract and/or DD254 instructions. However, you may contact the USG Contracting Officer or your prime contract's point of contact (buyer) to clarify what/if any CUI is in scope for the contract / subcontract.

CUI3. How do we know if we have critical or non-critical CUI?

DoD's CMMC rulemaking process and subsequent implementation are expected to shed additional light on how "critical national security information" will be identified.

CUI4. Are DPAS DX rated orders considered critical national security information?

DoD's CMMC rulemaking process and subsequent implementation are expected to shed additional light on how "critical national security information" will be identified. Defense Priorities & Allocations System (DPAS) ratings may not directly correlate to information (e.g., CUI) but rather the type of work being done and how it impacts national security.

CUI5. Would a Purchase Order from a prime contractor for DoD parts be considered CUI?

Unfortunately, this is not a yes/no answer - although a typical purchase order (PO) will not be CUI, it depends on the information contained in the PO. You should check with the Supply Chain professional who issued the PO if you have questions on the sensitivity of information in the PO.

CUI6. We receive contracts that flow down the 7012 clause, but don't receive any files/data marked CUI causing us to treat all data received as CUI. What should we do?

Information that is not considered CUI does not apply for DFARS 252.204-7012 safeguarding requirements. What constitutes as CUI is defined by the Government and the current list can be found within the National Archives CUI registry at: https://www.archives.gov/cui/registry/category-list.

United State Government (USG) agencies are responsible for marking CUI that they provide and for providing marking instructions to contractors for CUI they generate. CUI should be labeled or otherwise identified in the contract as CUI. USG, DoD, or Contractors are required to mark data as CUI/CDI in accordance with contract and/or DD254 instructions. However, you may contact the USG Contracting Officer or your prime contract's point of contact (buyer) to clarify what/if any CUI is in scope for the contract / subcontract.

Contractors must continue to flow down DFARS 252.204-7012 requirements to their subcontractors as required by the clause.

CUI7. Does Distribution Statement D always mean the document is CDI?

For DoD programs, unclassified information marked as "Distribution Statement D" would qualify as a "restrictive marking" requiring further protections (i.e., CDI/CUI).

CUI8. How would you define whether a Security Protection Asset "processes" CUI, requiring to be FedRAMP?

Per CMMC Level 2 Assessment Scope, CUI Assets ("assets that process, store, or transmit CUI") and Security Protection Assets ("assets that provide security functions or capabilities to the contractor's CMMC Assessment Scope, irrespective of whether or not these assets process, store, or transmit CUI") will be assessed against CMMC practices. For cloud-based services that serve as either of these two types of assets, ensuring that the implemented service meets FedRAMP Moderate or equivalent would help to ensure that the required CMMC Level 2 practices can be assessed as MET.

Cybersecurity Maturity Model Certification (CMMC)

CM1. What is the status of the CMMC program?

CMMC is currently in rulemaking. There will be a proposed or interim rule released in the future. If it is a proposed rule, there will likely not be any contract with CMMC requirements until 1st quarter of 2025 at the earliest. If it is an Interim Final Rule, there will likely be contracts with CMMC requirement beginning no sooner than 1st quarter of 2024. It is possible that requirement may change based on the next round of comments in the rulemaking process.

Please see the CyberAB July 2023 townhall for more information on the rulemaking process.

CM2. Is the CMMC requirement mandatory to process any Government contract, or is this requirement for specific military companies like Lockheed Martin, BAE, etc.?

The CMMC will be a requirement for U.S. DoD contractors and subcontractors, replacing the current self-attestation model and moving towards third party certification. The DoD has indicated that over time, CMMC requirements will be incorporated into all future DoD contracts.

CM3. Is it mandatory to hire a CMMC-RP, CMMC-RPO, or CCPA for your certification?

Once CMMC 2.0 goes into effect, Organization Seeking Certification (OSC) will need to engage with a Certified Third-Party Assessment Organization (C3PAO) to complete a CMMC Level 2 assessment.

Registered Practitioners (RP) and Registered Practitioner Organizations (RPO) are members of the CMMC ecosystem that could be engaged (not mandatory) to provide consultative preparation services to the OSC. Certified CMMC Professional (CCP) and Certified CMMC Assessor (CCA) are members of a C3PAO, that have completed the training and certification requirements to be CMMC Level 1 and Level 2 assessors.

More information on the roles of members in the CMMC ecosystem can be found via the Cyber Accreditation Body (Cyber AB, formerly CMMC-AB) at https://cyberab.org/CMMC-Ecosystem/Ecosystem-roles

CM4. Are there identified certifying bodies yet where can I find more information on Certified Third-Party Assessor Organizations (C3PAO)/CMMC-RP (Registered Practitioner)?

Information regarding C3PAO/CMMC-RP should be sought via the Cyber Accreditation Body (Cyber AB, formerly CMMC-AB) at https://cyberab.org/CMMC-Ecosystem/Ecosystem-roles.

CM5. Where do you go to contact a C3PAO?

A list of current C3PAOs can be found in the Cyber AB Marketplace at https://cyberab.org/Catalog#!/c/s/Results/Format/list/Page/1/Size/9/Sort/NameAscending.

CM6. When is it estimated that a C3PAO will be able to audit to a specific CMMC level?

CMMC assessments (e.g., Level 2) cannot begin until sometime after rulemaking is completed, including any associated updates to assessment guidance. You may visit the DoD CIO CMMC website for updates on the CMMC program.

CM7. Are the 110 practices for a CMMC level 2 org related to the max 110 points of a self-reported SPRS score?

As it stands (CMMC rulemaking is still in progress), CMMC Level 2 relates to both the existing Cyber DFARS requirements and the NIST SP 800-171 (110 controls); the SPRS score is your NIST 800-171 self-assessment score.

CM8. Are subcontractors expected to meet 100% of all NIST 800-171 controls and certified?

At this time, CMMC 2.0 will allow limited use of Plans of Actions & Milestones (POA&M) that are time-bound. Contractors/subcontractors will potentially have 180 days to address and remediate their POA&Ms. POA&Ms will not be accepted for specific controls deemed more critical.

See DoD's statement on the use of POA&Ms here.

CM9. Who or how is it decided if the suppliers fall under Level1 or Level2?

This is dependent on the type of information the organization has access to or develops. If an organization is dealing with Federal Contract Information (FCI) only, a self-assessment of CMMC Level 1 will be needed. If an organization is accessing or developing CUI identified as non-critical to national security, a self-assessment of CMMC Level 2 will be needed. CUI identified as *critical to national security* will require certification by an authorized C3PAO from the Cyber AB Marketplace.

If contractors and subcontractors are already performing under 48 CFR 52.204-21 – Basic Safeguarding of Covered Contractor Information, they should already have implemented the 15 controls (or 17 NIST SP 800-171 controls) that are likely be required for CMMC Level 1. If contractors are already performing under DFARS 252.204-7012, they should already have implemented (or have POA&Ms) the 110 NIST SP 800-171 security controls that are likely required for CMMC Level 2.

CM10. What are organizations seeing for the cost of an assessment?

Cost for assessments will vary depending on the size and scope of the assessment. Recommend that you engage a C3PAO to get a more accurate estimate than we can provide at this time.

CM11. Will contractors be able to recoup money spent on CMMC certification?

The expectation is that the contractor's investments in cybersecurity are allowable costs – though they most likely should be treated as overhead vs. directly chargeable to the DoD customer**.** See FAQ 12 and 13 from DoD Procurement Toolbox.

CM12. Is it common for an organization to have separate boundaries for CMMC Level 1 and Level 2, where CUI is limited to certain systems, but FCI is used on more systems?

It is not uncommon for contractors to segment their systems (with logical and/or physical boundaries) with more sensitive (e.g., CUI) information contained within more limited boundaries than less sensitive information. However, contractors will need to pursue assessment and certification at the highest CMMC Level appropriate to the types of information managed on their systems.

CM13. What level is required for suppliers not producing fly away parts such as perishable tooling or COTS?

The CMMC level depends on the information managed (received, stored, generated, etc.) in your IT systems. If CUI is in scope for your organization's IT systems, then level 2 is appropriate, regardless of the products/services you provide to the customer.

CM14. Assume the prime sends the CUI encrypted via secure portal and we take the CUI and store it on a cloud-based CMMC compliant service. The CUI is stored in the cloud encrypted and our team will view the CUI documents as needed - but they are not stored on our network - are we exempt?

When using Cloud Service Providers (CSP) to manage CUI, it becomes an extension of the contractor's IT/security architecture and does not exempt contractors from CUI safeguarding requirements. CSPs utilize a Shared Security Model concept which includes responsibilities for both CSPs and customers in maintaining security compliance. Generally, CSPs are responsible for the security of the cloud infrastructure while customers are responsible for ensuring consumed resources are securely configured and maintained. See DIB SCC CyberAssist Cloud FAQ for more information.

CM15. Are employee background checks a CMMC requirement?

Control 3.9.1 of the NIST SP 800-171 requires organizations to conduct security screening of personnel prior to authorizing access to organization systems containing CUI/CDI. The organization should ensure that all employees who need access to CUI undergo organization-defined screening before granting access. Base the types of screening (i.e., criminal, background checks) on the requirements for a given position and role.

CM16. What is the buffer time to get an audit once CMMC controls are finalized by the DoD?

Once the DoD finalizes CMMC rulemaking, Organizations Seeking Certification (OSCs) can engage Certified Third-Party Assessment Organizations (C3PAO) from the Cyber Accreditation Body (AB) Marketplace for their assessment. Time from engagement to audit may vary depending on the availability of the C3PAO and OSCs, scope of the assessment, and the level of preparedness of the OSC.

CM17. How can they audit when the CMMC is not fully defined?

The current assessments that are being done through the Joint Surveillance Voluntary Assessment (JSVA) programs are considered assessments under the DoD NIST SP 800-171 Assessment Methodology and not an official "CMMC Audit". The intent is to have these JSVA converted to CMMC assessments once CMMC goes through rulemaking - as CMMC Level 2 requirements are based on the NIST SP 800-171, though this determination has not been finalized yet.

CM18. Is there a CMMC Level 2 Assessment Checklist similar to the ISO 9001 audit checklist?

We recommend reviewing the following resources as the guidelines for CMMC Level 2 Assessment: NIST SP 800-171A from NIST website, the CMMC Level 2 Assessment Guide from the DOD CIO Website, or other resources provided by DCMA DIBCAC team.

CM19. I read somewhere that CMMC 2.0 LVL 2 incorporates all of the NIST 800-171 requirements, so there is no need to have separate policies as long as the policy control references the correct control family. Is that correct?

Level 2 of CMMC 2.0 encompasses all 110 security requirements for safeguarding CUI specified in NIST SP 800-171 Rev 2 per DFARS 252.204-7012. Developing your policies and System Security Plans (SSP) to NIST SP 800-171 requirements will prepare your organization for CMMC 2.0 Level 2. Your SSP should be used to describe how your policies and controls meet each of the NIST control

families and its security requirements. Additional information on CMMC Level 2 requirements can be found on the DOD CIO Website.

CM20. When will contracts requiring specific CMMC levels be awarded?

The answer to this is dependent on when CMMC rulemaking is completed. Upon completion, we do expect the DoD to take a phased approach in requiring them on contracts.

CM21. How far must we go to ensure our sub-contractors have their required certification? Can we just give them a survey? Do we have to catalog their responses to the survey? Can you give examples of how this could work?

Requirements (and methods) for contractors to verify their subcontractors' CMMC certifications are currently unknown since contractor access to SPRS is limited to their own information. The outcome of rulemaking is expected to clarify expectations and processes for contractors to verify the certification status of their subcontractors.

CM22. Will there be a centralized site to view subcontractors' level of certification (e.g., OASIS (used for AS9100))?

The DoD has not provided guidance on how or if CMMC results will be shared with the DIB.

CM23. In context to removable media, do removable media ports need to be completely disabled throughout all devices? Can blocking direct execution from removable media check that box for Level 2 CMMC compliance?

NIST 800-171 doesn't specifically answer that question, but you should determine what can reasonably be blocked without major impact to your business. There may be cases where users need access to removable media, so having a process established (such as a documented policy exception) to address those one-off circumstances is important. The important part is to have control and visibility into the use of removable media by your end users.

CM24. How will MSP/MSSP's be handled during these assessments? Does our MSP who handles all of our IT needs also need to be L2 certified?

The Managed Service Provider (MSP) or Managed Security Service Provider (MSSP) may not be required to obtain a CMMC certification. However, the assets used by the MSP/MSSP for the handling (process, store, or transmit) or protection (Security Protection Assets) are part of the contractor's assessment scope, regardless of their physical or logical placement. For example, an MSP that provides a security information and event management (SIEM) service may be separated logically and may process no CUI, but the SIEM does contribute to meeting the CMMC practice requirements.

Contractors and MSP/MSSPs generally use Service Level Agreements (or other contract documents) that provide the roles and responsibilities for both MSPs and customers in maintaining security operations and compliance.

See CMMC Scoping Guidance for more details.

CM25. Due to flow down requirements, can a company get a CMMC certification without their subcontractor(s) being certified?

Subject to any clarifications during rulemaking, each organization seeking certification (OSC) is expected to be independently assessed against the CMMC requirements. Contractors must ensure that they are flowing down the Cyber DFARS and/or CMMC (once rulemaking is complete) requirements to their subcontractors. If the subcontractor(s) will be generating or handling CUI/FCI as part of their subcontract work, then they will need to have the appropriate CMMC level certification for the type of information they are handling before the sub/contract can be awarded.

CM26. It was mentioned that POA&Ms will not be permitted. The Cyber AB townhall mentioned that only certain objectives would not be permitted a POA&Ms. Can you provide the link to this statement?

At this time, CMMC 2.0 will allow limited use of Plans of Actions & Milestones (POA&M) that are time-bound. Contractors/subcontractors will potentially have 180 days to address and remediate their POA&Ms. POA&Ms will not be accepted for specific controls deemed more critical.

See DoD's statement on the use of POA&Ms here.

CM27. How will international/non-US suppliers doing work on a USG DoD contract be impacted by CMMC?

CMMC is expected to impact international/non-US suppliers the same way it impacts US domestic suppliers. There is a process for assessment organizations outside of the US to become certified assessment organizations. The assumption is that international/non-US suppliers will contract with one of these assessment organizations that are licensed to operate in their country. Specifics of CMMC applicability to international/non-US organizations are being evaluated, but at present is still to be determined.

Note that there is currently ongoing discussion between the USG and foreign Governments (e.g., UK and Canada) regarding cyber regulatory reciprocity.

CM28. What if my organization cannot afford to be certified, does that mean my organization can no longer work on DoD contracts?

As the requirements phase in, *CMMC will be a cost of doing business for any defense industrial base (DIB) contractor (large, mid-size, or small).* The costs of satisfying CMMC Level 1-3 requirements scale with the organization's IT footprint and for Level 2-3, the complexity of the organizations CUI network environment (which may be the full enterprise network, or an enclave associated with one or more specific DoD contracts). Organizations of all sizes need to assess and determine the best approach to securely managing DoD information in their IT environment. Per the regulations, businesses that do not satisfy DoD cybersecurity requirements will not be eligible for contract awards.

CM29. What is a POA&M and what does it mean to burn them down?

POA&M stands for Plan of Action and Milestones. It is documentation that identifies tasks needing to be accomplished. It details resources required to accomplish elements of the plan, any milestones in meeting the tasks, and scheduled completion date for the milestones as it relates to implementing the NIST SP 800-171 controls. Burn down refers to the completion of all identified tasks within the POA&M. As a reminder, the expectation is CMMC 2.0 will allow limited use of Plans of Actions & Milestones (POA&M) that are time-bound. Contractors/subcontractors will potentially have 180 days to address and remediate their POA&Ms. POA&Ms will not be accepted for specific controls deemed more critical.

See DoD's statement on the use of POA&Ms here.

CM30. Over the years small businesses have greatly invested in new infrastructure with NIST and CMMC in mind. We are much stronger and nimble to react to attacks but improving CMMC scores have presented challenges. How can a small business address policy deployment, training, and proof subjective evidence when the rules continue to be amended?

We recommend focusing on implementing the controls in the NIST SP 800-171 and burn down any open POA&M items (see CM28). As CMMC is in rulemaking, we do not recommend attempting to anticipate what the USG will be asking for but rather focus on what we know is required (i.e., DFARS 252.204-7012 and NIST SP 800-171 requirements).

CM31. If the network that houses the CUI data and access to that data is separated from the rest of the company network by a hardware firewall, does the entire company network need to be secured under the CMMC guidelines?

If the isolated network or enclave has a firewall as the security boundary that prevents CUI from crossing the boundary, then only those systems that will store/process CUI will need to comply with the NIST 800-171. The security boundary will need to be described in the System Security Plan and ultimately, evidence will need to be provided to the CMMC assessor proving that the two networks are logically and/or physically separated preventing CUI from being accessed by the "other" network. If the device and/or local network has no external connection(s), it still needs to comply with the requirements for safeguarding CUI.

CM32. How would NIST SP 800-171 Rev 3 impact CMMC?

NIST SP 800-171 Rev 3 is still in draft, and we do not expect it to be finalized until at least 1st Quarter of 2024. It is unknown how the DoD will implement the new revisions with DFARS Clause 252.204-7012. Furthermore, impacts to CMMC (still in rulemaking) is less understood. Industry will continue to seek guidance from the USG, DoD, and NIST on these updates.

General Cybersecurity Questions

GC1. What standard is recommended for storing data in off-site backups?

We can't make specific recommendations as it will depend on your business and the specific needs of your organization. You may review the CyberAssist Media Protection section to learn more about safeguarding backups.

GC2. An employee can start exfiltrating data at any time in their career - What products will monitor for data exfiltration and aggregation? This is probably the single biggest threat once your perimeter is secure.

There are many different Data Loss Prevention (DLP) tools available in the marketplace. These tools help with the classification and categorization of data. Use them to identify security violations of policies defined by the organizations. Additional information on Insider Threat awareness and mitigation information can be found via CyberAssist at: https://ndisac.org/dibscc/cyberassist/search/?skey=Insider+Threat&tag=&cat=

GC3. What safeguards need to be applied to working from home, as an alternate work site?

Many people work from home or travel as part of their job. Organizations should define and implement safeguards to account for protection of information beyond the enterprise perimeter. Safeguards may include physical protections, such as locked file drawers, as well as electronic protections such as encryption, audit logging, and proper access controls. NIST SP 800-46 and NIST SP 800-114 provide guidance on enterprise and user security when teleworking.

GC4. Being in a completely remote work environment, users have local admin rights to their computers. Does this directly put the company out of compliance with NIST controls? Or is this a risk that the company is able to accept, based on SOC/SIEM tools and audit logging/monitoring and still be considered "compliant"?

Local administrative rights significantly increase the risk and impacts to the organization should the account be compromised. Though local admin rights give users the freedom to add/remove programs, install printers, etc., it also gives attackers unfettered access to the local device and to weaponize the system against the organization. Although the NIST requirements do not prohibit the use of local admin accounts, organizations should consider alternative methods like a Just-in-Time privilege escalation management tool, that would allow users to request local admin privileges for a set duration.

GC5. In Risk Analysis, shouldn't we ask how our backups are tested?

A risk assessment should evaluate how backups are audited and protected. Testing will help verify that your backup data is complete, accurate, and accessible. Additional information on backup and disaster recovery testing can be found via CyberAssist at: https://ndisac.org/dibscc/implementation-and-assessment/data-protection/backups/.

GC6. How should we address separation of duties in small companies where there's only 1 person supporting and managing servers?

The practice of separation of duties is to ensure that not one individual has all "the keys to the kingdom" (splitting up responsibilities). Unless this is a one-person organization, steps should be taken to inject another person into processes to ensure, at a minimum, that changes to IT/systems are properly reviewed, tested, and approved before implementation. (i.e., adding a manager/owner to the approval process).

GC7. How can a company handle contractors and vendors that have permanent/unescorted access to our facilities (e.g., cleaning staff that we have assigned entry badges to)? Is it necessary to perform background checks on them?

Typically, contractors/vendors who are supplying permanent staff to your facilities should have their own processes in place for background checks. Please consult with them to understand what background check processes, and termination/transfer processes they have in place. As a result, you should determine if these background checks align with your security policy.

Additionally, physical and logical access control measures need to be in place to prevent on-site vendors and contractors from unauthorized access to sensitive information or CUI (e.g., hard copy).

Key Points and Additional Resources

- CUI practices and legacy markings, such as For Official Use Only (U//FOUO), Sensitive But Unclassified (SBU) and other warning labels, will co-exist until all control markings are transitioned to the new control markings per NARA's CUI Marking Handbook - https://www.archives.gov/files/cui/20161206-cui-marking-handbook-v1-1.pdf

- DoD CUI that is marked/labeled as Distribution Statement C or D indicates information requiring safeguarding and subject to export control, such as Department of State International Traffic in Arms Regulations (ITAR) and the Department of Commerce Export Administration Regulations (EAR) – DoD Instruction (DoDI) 5200.48

- DoD published Cybersecurity Frequently Asked Questions can be found at: https://dodprocurementtoolbox.com/faqs/cybersecurity

- Defense Acquisition University (DAU) hosts events on Cybersecurity Regulations to include NIST 800-171 and the Cybersecurity Maturity Model Certification (CMMC) – https://www.dau.edu

- Exostar Webinar “Get a Handle on CUI Before It’s Too Late” - https://landing.exostar.com/en-us/understanding-cui-life-cycle

- Defense Contract Management Agency > DIBCAC (dcma.mil) - Resources provided by the DCMA DIBCAC team to help organizations prepare for a NIST SP 800-171 / CMMC assessment.

- Supplier Performance Risk System (disa.mil) - Website with resources on how to submit a NIST Assessment score to DoD’s SPRS system.