Supplier FAQs

Preparing for New DFARS Interim Rule on Assessments & Cybersecurity Maturity Model Certification

If after using this resource, you find your question is not addressed, please e-mail: lmco-cmmc.fc-eo@lmco.com

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

FCI: Federal Contract Information

NARA: National Archives and Records Administration

PIEE: Procurement Integrated Enterprise Environment

POAM: Plan of Action and Milestones

SAM: System for Award Management

SPRS: Supplier Performance Risk System

Supplier Performance Risk System (SPRS)

SP.1 ***With respect to the Supplier Performance Risk System SPRS, what action is required by suppliers, and when is it due? Is there anything in addition to my NIST 800-171 score that I need to enter into SPRS?***

For suppliers that have not undergone a DIBCAC assessment performed by DCMA, a Basic self-assessment of the NIST SP 800-171 based on NIST SP 800-171 DoD Assessment Methodology, V1.2.1 must be submitted to SPRS (or email to webptsmh@navy.mil) with the following information:

1) Version of NIST 800-171 against which the assessment was conducted
2) Organization conducting the assessment (e.g., contractor self-assessment)
3) For each system security plan supporting the performance of DoD contract –
    a. All Industry Commercial and Government Entity (CAGE) code(s) associated with the information system(s) addressed by the system security plan
    b. A brief description of the system security plan architecture, if more than one plan exists.
4) Date the assessment was completed.
5) Summary level Score (e.g., 95 out of 110, not the individual value for each requirement)
6) Date that all requirements are expected to be implemented (date that a score of 110 is expected to be achieved)

Contracts / Subcontracts that include the new DFARS NIST SP 800-171 Assessment requirement (252.204-7020), which became effective on November 30, can only be awarded to companies who have satisfied this requirement prior to contract award.

SP.2 ***How does one gain access to SPRS and how do I submit my NIST 800-171 score?***

Instructions for how to obtain access to SPRS can be found here: https://www.sprs.csd.disa.mil/access-nongov.htm.

Prior to being granted SPRS access, suppliers must register for an account in the Procurement Integrated Enterprise Environment (PIEE) by following the instructions provided here and below.

Please ensure that each of the step below is completed before you begin registering for account in PIEE (Step 9).
* indicates a mandatory step
** This is an Wide Area Workflow (WAWF) step only

1. Register with the System for Award Management (SAM) *
   Note: This step will register the supplier for a CAGE code, required to conduct business with the US Government. This step may be skipped if the vendor already has a CAGE code in SAM.
2. Establish an Electronic Business (EB) Point of Contact (POC) in SAM *
   Note: An EB POC must be established for your CAGE code in order to continue.
3. Ensure CAGE Code is added to the Procurement Integrated Enterprise Environment Vendor Group Structure *
   Note: Requires the vendor to contact Customer Support Center (1-866-618-5988) or send an email to DISA Ogden (disa.ogden.esd.mbx.cscassig@mail.mil) to have their CAGE code added to PIEE.
4. Establish an Organizational Email Address **
5. Designate a Contractor Administrator (CAM) *
6. Determine if batch feeds for data input is necessary **
7. Set up PCs to Access applications in Procurement Integrated Enterprise Environment
8. Self-Register CAM *(There must be a CAM to activate vendors.)
9. Have all users for the CAGE Code(s) self-register on the Procurement Integrated Enterprise Environment web site for one of the available Vendor Roles
   Note: User Registration process can be found here

10. Complete the Web Based Training for the applications you will use in Procurement Integrated Enterprise Environment

PIEE Vendor Customer Support can be reached here:
https://piee.eb.mil/xhtml/unauth/web/homepage/vendorCustomerSupport.xhtml#helpdesk

SPRS user guide for submitting the NIST SP 800-171 DoD Assessment can be found here:
https://www.sprs.csd.disa.mil/pdf/NISTSP800-171QuickEntryGuide.pdf

SPRS Support can be found at the bottom of their webpage:
https://www.sprs.csd.disa.mil/access.htm

SP.3 ***Will submitting a Basic submission to the SPRS system as required by Lockheed Martin trigger the DoD to conduct a Medium or High Assessment?***

No, the Government will determine who will be selected for a DIBCAC Medium or High Assessment (performed by DCMA) based on their criteria. The requirement to submit NIST 800-171 DoD Assessment to SPRS will apply broadly to prime contractors and subcontractors based on DFARS 252.204-7019, *Notice NIST SP 800-171 DoD Assessment Requirements* and DFARS 252.204-7020 *NIST SP 800-171 DoD Assessment Requirements* and is required to be completed prior to contract award.

SP.4 ***How can I know if I have a CAGE Code and determine what my company CAGE Code is? Are the NIST and CMMC statuses associated with the CAGE Code(s)?***

The System for Award Management (SAM) provides the following quick start guide with a link to the DLA Business Identification Number Cross-Reference System (BINCS) CAGE search page.

SP.5 ***If a company has more than one CAGE Code, does the company need to enter scores in SPRS for each SAM-registered office?***

As part of the submission to SPRS, contractors will be able to submit a single entry for all industry CAGE Code(s) associated with the information system(s), provided it is addressed in the system security plan. It is up to the suppliers to work with their assessment teams to define the boundaries of the IT systems being assessed.

SP.6 ***What is the difference between PIM and SPRS? Do we need to enter our assessment score for NIST 800-171 in PIM on Exostar and SPRS?***

PIM is an Exostar managed system and SPRS is a government-owned system. Lockheed Martin suppliers are required to complete the NIST 800-171 questionnaire in Exostar, if they handle Controlled Unclassified information (CUI) as part of their performance on Lockheed Martin subcontracts. The current scoring of the Exostar NIST questionnaire is not based on NIST SP 800-171 DoD Assessment Methodology, V1.2.1, which is the weighted scoring required by interim rule (DFARS 252.204-7019).

Completion of the NIST SP 800-171 questionnaire in Exostar does not satisfy the requirement for the supplier to submit a Basic NIST SP 800-171 DoD Assessment to SPRS.

SP.7 ***I've already completed the NIST 800-171 assessment on the Exostar website. Does it automatically populate my score into SPRS?***

No, contractors need to conduct a self-assessment based on NIST SP 800-171 DoD Assessment Methodology, V1.2.1. Upon completion of the self-assessment, the contractor must register for a vendor account with SPRS and upload the information into the system.

SP.8 ***Do we need to flow the Interim rule down to our suppliers and do our suppliers also need to enter and manage their scores in SPRS?***

Both DFARS 252.204-7020 *NIST SP 800-171 DoD Assessment Requirements* and DFARS 252.204-7021 *Cybersecurity Maturity Model Certification Requirement* are required to be flowed down to subcontractors at all tiers, based on the sensitivity of the unclassified information flowed down to each contractor. Prior to awarding to a subcontractor, the contractor must ensure that the subcontractor has a current (i.e., not older than 3 years) NIST DoD Assessment (252.204-7020) or CMMC certificate (252.204-7021) that is appropriate for the information that is being flowed down to the subcontractor.

SP.9 ***If you do not bid on DoD work, instead are simply awarded DoD work, do you need to have a NIST 800-171 assessment in the SPRS?***

Yes, if the DFARS cyber provisions (252.204-7012 and 252.204-7019/7020) apply and the DoD work involves CUI. DFARS provision 252.204-7019 advises offerors required to implement NIST SP 800-171 standards of the requirement to have a current (not older than three years) NIST SP 800-171 DoD Assessment on record in order to be considered for award. The results of the Assessments must be uploaded and documented in the Supplier Performance Risk System (SPRS) to provide DoD Components with visibility into the scores of Assessments already completed; and verify that an offeror has a current (i.e., not more than three years old, unless a lesser time is specified in the solicitation) Assessment, at any level, on record prior to contract award.

SP.10 ***Does entry for SPRS have a downloadable form that can be filled in prior to submission?***

The following information is required for submission to SPRS. SPRS user guide for submitting the NIST 800-171 Assessment can be found here:
https://www.sprs.csd.disa.mil/pdf/NISTSP800-171QuickEntryGuide.pdf

1) Version of NIST 800-171 against which the assessment was conducted
2) Organization conducting the assessment (e.g., contractor self-assessment)
3) For each system security plan supporting the performance of DoD contract –
    a. All Industry Commercial and Government Entity (CAGE) Code(s) associated with the information system(s) addressed by the system security plan
    b. A brief description of the system security plan architecture, if more than one plan exists
4) Date the assessment was completed
5) Summary level Score (e.g., 95 out of 110, not the individual value for each requirement)
6) Date that all requirements are expected to be implemented

SP.11 ***Regarding the DoD assessment scoring and how partially meeting a requirement will be scored. Also are there any exceptions allowed? Is there any detailed guidance on the scoring available?***

The NIST SP 800-171 DoD Assessment Methodology, V1.2.1 provides the scoring template and information on how to submit the Assessment to SPRS.

The NIST SP 800-171 DoD Assessment requirements will be required on new solicitation and contracts, task orders, or delivery orders, including those using FAR Part 12 procedures for the acquisition of commercial items, except for those that are solely for the acquisition of commercially available off-the-shelf (COTS) items or receiving contracts or orders valued at or below the micro-purchase threshold.

Controlled Unclassified Information (CUI)

CU.1 ***How are Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) defined?***

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. General assumption should be that data is at least FCI unless it is specifically labelled publicly releasable or is spelled out in the contract as publicly releasable. (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)

- A DoD CUI Registry has been published and can be found at: https://www.dodcui.mil/Home/DoD-CUI-Registry/ in addition to the NARA CUI Registry at: https://www.archives.gov/cui/registry/category-list. Additional DoD CUI information can be found at: https://dodcui.mil
  - 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)

CU.2 ***How do I know if I'm handling CUI on a Lockheed Martin contract? (How are suppliers identified as handling CUI and where is that designated?)***

Refer to CU.1 for CUI definition

CU.3 ***How does a supplier determine if data they generate is CUI and what guidelines exist for proper marking?***

Prime contractors and sub-tier suppliers are required to not only retain DoD CUI markings but also mark any derivatives (DoD CUI generated by, or on behalf of, the contractor in support of the performance of the contract)

- Refer to CU.1 for CUI definition
- DoD Instruction (DoDI) 5200.48 Controlled Unclassified Information (CUI), was published on March 6, 2020, replacing and cancelling DoD Manual 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information."
- DFARS 252.204-7012 and DoDI 5230.24

Additional government references:

- National Archive and Records Administration CUI Registry: https://www.archives.gov/cui/registry/category-list
- NARA CUI Marking Handbook: https://www.archives.gov/files/cui/20161206-cui-marking-handbook-v1-1.pdf

Cybersecurity Maturity Model Certification (CMMC)

CM.1 ***What is the expected timeline to require suppliers to be Cybersecurity Maturity Model Certification (CMMC) Level 3?***

Starting November 30, 2020, DoD began to include CMMC requirements on selected prime contracts. DoD has communicated a plan for a phased rollout of CMMC through government FY2026, at which time all DoD contracts will include CMMC requirements. Contractors in receipt of these contracts (prime and subcontracts) will be required to have a current (i.e., not older than three years) certification for the required level at the time of award. Contracting Officers will not make an award, or exercise an option on a contract, if the contractor does not have a current certification for the required CMMC level.

CM.2 ***Are there identified certifying bodies yet where can I find more information on Certified Third-Party Assessor Organizations (C3PAO)?***

The CMMC Accreditation Body (CMMC-AB) will provide a listing of C3PAO and Assessors on the CMMC-AB Marketplace once these groups/members are identified.

CM.3 ***Will the first CMMC RFI be identified before the third-party assessors are in place?***

The DoD has been working closely with the CMMC Accreditation Body (CMMC-AB) and industry, and they are very aware of the availability of (or lack thereof) CMMC assessors. Lockheed Martin would not expect DoD to issue any formal requirements (RFI/RFP) for CMMC Levels before contractor organizations can obtain those certifications.

CM.4 ***What is the difference between CMMC Level 1 and Level 2?***

- CMMC Level 1 includes 17 practices which map directly to the basic safeguarding requirements specified in the clause FAR 52.204-21 – *Basic Safeguarding of Covered Contractor Information Systems* (aligns to 17 NIST 800-171 controls).
- CMMC Level 2 includes 72 practices which are comprised of 65 security requirements from NIST SP 800-171 (implemented via DFARS clause 252.204-7012), 7 CMMC practices, and 2 CMMC processes. CMMC Level 2 is intended as an optional intermediary step for contractors as part of their progression to Level 3. To date, DoD has indicated that they do not expect to issue any prime contracts requiring CMMC Level 2 (Contracts with only FCI data will be issued with CMMC Level 1 requirements; contracts with CUI data will be issued with CMMC Level 3 (or higher) requirements).

CM.5 ***How will international suppliers doing work on a DoD contract be impacted by CMMC?***

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

CM.6 ***What is the cost of CMMC and how large is the hurdle for a company that is currently NIST compliant to becoming CMMC compliant in effort and dollars?***

The costs and efforts of satisfying CMMC Level 1-3 requirements scale with the organization's IT footprint and for Level 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.

Note: The DFARS interim rule publication in the Federal Register provides a DoD estimate of recurring and non-recurring costs to obtain each CMMC certification level.

CM.7 ***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 (expected to be fully rolled out by government FY 2026), *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 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.

CM.8 ***Will a supplier need one certification that applies to all facilities or will each facility need to be certified individually?***

CMMC Certifications can be applied to all industry CAGE Code(s) associated with the information system(s) addressed by the system security plan. It is up to the suppliers to work with their assessment teams to define the boundaries of the IT systems being assessed.

CM.9 ***What is a POAM and what does it mean to burn them down?***

POAM 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 POAM. As a reminder, POAMs will not be considered adequate for CMMC.

CM.10 ***Will POAMs be acceptable for CMMC and how does this differ from NIST 800-171?***

No, CMMC Level 3 certification requires that all 110 NIST SP 800-171 controls are fully implemented (no open POAMS), in addition to 20 (7 Level 2 / 13 Level 3) CMMC practices and 3 (2 Level 2 and 1 Level 3) Maturity processes.

CM.11 ***How does CMMC apply to sub-tier suppliers?***

The DFARS interim rule establishes 252.204-7021 *Contractor Compliance with the Cybersecurity Maturity Model Certification Requirement (Nov 2020)* – Prior to subcontract award, the contractor must ensure that their subcontractors have a current (i.e., not older than 3 years) CMMC certificate at the CMMC level that is appropriate for the information that is being received, stored, and generated by the subcontractor.

CM.12 ***Lockheed in the past has used Exostar's Cyber Security Questionnaire to determine supplier standing. How does the CSQ correlate with CMMC and is there a resource that links CSQ requirements with the standards of the CMMC?***

The Cybersecurity Questionnaire (CSQ), 194 questions, is much broader than the NIST SP 800-171 questionnaire and is Lockheed Martin's risk-based approach in assessing our suppliers' cybersecurity controls for protection of Lockheed Martin Sensitive Information against more advanced and persistent threats. There are overlaps of security practices between the CSQ and NIST SP 800-171, however it is not a one-for-one match.

The CSQ was adopted from the Center of Internet Security Critical Security Controls version 5.1 and the mapping of these controls to the 110 NIST SP 800-171 (subset of CMMC practices) can be found here: https://www.cisecurity.org/white-papers/cis-controls-and-sub-controls-mappings-to-nist-special-publication-800-171-r2/

CM.13 ***Who can I speak with for additional guidance on CMMC and related topics and where can I find additional resources?***

See the Defense Industrial Base (DIB) Sector Coordinating Council (SCC) Cyber Assist website for resources on the implementation and assessment of cybersecurity controls. These resources include guides, standards, sample policies and procedures, videos, example tools, lesson learned, and other helpful information.

See Appendix B of CMMC Model for additional information about each capability.

CM.14 ***Is there a minimum score that is required for the DFARS Interim Assessment rules to be considered for DoD contracts until CMMC is fully rolled out?***

The DFARS interim assessment rule does not define a minimum score for contract award. The requirement is for the contractor to have a current Assessment (i.e., not older than 3 years) in SPRS based on the NIST SP 800-171 DoD Assessment Methodology, V1.2.1.

Prime Contracts and subcontracts with CMMC requirements that include DoD controlled unclassified information (CUI) will require CMMC Level 3 (minimum). Prime Contracts and subcontracts with CMMC requirements that do not include CUI will require CMMC Level 1 (unless the contract is only for COTS or under the FAR micro-purchase threshold).

CM.15 ***Are there e-mail and software (i.e. Microsoft Office 365) solutions that are currently compliant with CMMC?***

Currently, there are no organizations that have been CMMC certified. However, just as cloud IT service providers have satisfied current DFARS 252.204-7012 requirements through FedRAMP authorization, they will be able to pursue and obtain certifications for CMMC Levels. Reciprocity between FedRAMP and CMMC is being evaluated, but at present is still to be determined. More information on FedRAMP can be found here.

CM.16 ***For those who are already on NIST800-171 with no open POAM items, what is the next immediate action item for them and what is the deadline for that?***

- Take advantage of any opportunity to have DCMA perform a DIBCAC Medium or High confidence assessment. The external assessment will not only document your score in SPRS, but it will also help your organization prepare for CMMC (third-party) assessment.
- At a minimum, determine your score through the basic assessment (self-assessment), and submit it to DoD SPRS following the regulatory guidelines. (See Annex B within NIST SP 800-171 DoD Assessment Methodology, V1.2.1)
- Focus on implementing the additional 20 (7 Level 2 / 13 Level 3) CMMC practices and 3 (2 Level 2/ 1 Level 3) CMMC maturity processes

CM.17 ***I am still not clear if my company needs to be CMMC level 3. How do I know if my company will need CMMC Level 3? Will prime contractors require CMMC level 3 even if it is not a new DOD contract or modification?***

CMMC Level requirements will be driven by the prime contract and by the data in scope for the subcontract. Prime Contracts and subcontracts with CMMC requirements that include DoD controlled unclassified information (CUI) will require CMMC Level 3 (minimum). Review your existing contracts with Lockheed Martin to determine whether DoD CUI is in scope and discuss with your procurement representative, if needed.

DoD has communicated that the CMMC requirement will not be applied retroactively to existing contracts; it will only apply to new DoD contracts, modifications, or renewal.

CM.18 ***When will CMMC be applicable on existing Lockheed Martin contracts?***

Starting November 30, 2020, DoD will begin to include CMMC requirements on selected new solicitations and contracts. Contractors in receipt of these contracts, including subcontracts, will be required to have a current (i.e., not older than three years) certification for the required level at the time of award. Prior to awarding to a subcontractor, the contractor must ensure that the subcontractor has a current CMMC certificate that is appropriate for the information that is being received, stored, and generated by the subcontractor.

CM.19 ***Will other certifications (e.g. ISO) be considered for CMMC?***

At this time the DoD has not provided guidance on reciprocity for other cybersecurity certifications, except for DoD DIBCAC high confidence assessments.

Lockheed Martin Status Request

LM.1 ***What are the actions Lockheed Martin is asking of suppliers who exchange CUI?***

To avoid disruptions to future business, contractors need to begin taking the following actions immediately:

- **Ensure that you have a current DoD Assessment score in SPRS (for all CAGE Codes covered by your System Security Plan (SSP)).**
  - If your organization's NIST 800-171 implementation was already assessed by the DCMA (DIBCAC medium or high assessment) and you have received your score you should have satisfied this requirement.
  - Take advantage of any opportunity to have DCMA perform a DIBCAC Medium or High confidence assessment. The external assessment will not only document your score in SPRS, but it will also help your organization prepare for CMMC (third-party) assessment.
  - At a minimum, determine your score through the basic assessment (self-assessment), and submit it to DoD SPRS following the regulatory guidelines. (See Annex B within NIST SP 800-171 DoD Assessment Methodology, V1.2.1)

- **Address the Additional CMMC Practices and Processes Now.**
  - To achieve CMMC Level 3 certification by a CMMC Third-Party Assessor Organization (C3PAO), organizations need to demonstrate implementation of all 130 Level 3 practices (NIST 800-171's 110+20), as well as the three processes associated with Maturity Level (ML) 3 (inclusive of ML2). **Plans of Action and Milestones (POAMs) will not satisfy the certification requirement**.

- **Provide Status to Lockheed Martin.**
  - In order for Lockheed Martin to assess risk and preparedness for the November 30 effective date of the new rules, we must receive the status of our applicable suppliers. Survey links were emailed on Thursday, October 29 asking to provide the following.
  - Confirmation of NIST 800-171 Assessment Score in SPRS
  - POAM ECD for any unimplemented NIST 800-171 requirements
  - Status/ECD for additional 20 (7 Level 2 / 13 Level 3) CMMC practices
  - Status/ECD for Level 2/3 maturity processes

LM.2 What expectation does Lockheed Martin have for on-going status updates?

Going forward, we are requesting you provide updates via the survey until your NIST SP 800-171 assessment score is loaded into SPRS and all outstanding controls, practices and processes are implemented.

NIST SP 800-171 (NIST)

NI.1 ***Can we update our Exostar Questionnaire at any time to reflect our progress toward compliance?***

Yes, suppliers are required to update their Exostar questionnaires annually but are encouraged to update the questionnaires as frequently as possible to account for any changes to their systems, policies, and processes that fall within the required update cycle.

NI.2 ***How do we know which NIST controls require a written policy?***

Within CMMC, practices and processes are defined. A practice is defined as a specific technical activity or activities that are required and performed to achieve a specific level of cybersecurity maturity for a given capability in a domain. A process is a specific procedural activity that is required and performed to achieve a maturity level. To achieve CMMC Maturity Level 2 (precursor to CMMC Level 3 Certification), the organization must have a guiding policy that establishes the objectives and importance of the practice domain. In addition, the organization must establish and document the practices within that domain.

More information on process maturity can be found here: https://insights.sei.cmu.edu/sei_blog/2020/06/cybersecurity-maturity-model-certification-cmmc-part-2-process-maturitys-role-in-cybersecurity.html

Small Business Focused

SM.1 ***What guidance can be given for smaller companies with less than 100 employees and only one IT Resource?***

Each organization needs to consider their IT environment, and how DoD information (e.g. FCI/CUI) is currently managed in that environment to satisfy the required security controls/practices. Contractor compliance with the current DFARS 252.204-7012 clause requires a System Security Plan and Plans of Action and Milestones (POAM) for any unimplemented controls. Consider where your organization is on the path to closing out any open POAM and the incremental effort to satisfy CMMC requirements (i.e. 20 additional CMMC Practices and 3 Maturity Processes). To compete for and be awarded contracts with CMMC

requirements, organizations will need to be certified to the required CMMC level regardless of organization size.

SM.2 ***How are small businesses going to be protected from being "priced out" of bidding on government projects?***

As the requirements phase in (expected to be fully rolled out by government FY 2026), **CMMC will be a cost of doing business for any defense industrial base (DIB) contractor (large, mid-size, or small).** Per the DoD CMMC FAQ number 18, "The costs associated with implementing CMMC requirements, supporting the CMMC assessment, and contracting with the C3PAO will be considered an allowed cost. For contracts that include the CMMC requirement, you will not be awarded the contract if you are not certified at the appropriate CMMC level at the time of contract award." The costs will need to be addressed consistent with each company's financial processes and may not be directly allocable to an individual contract / program (e.g. OH rates vs. direct charges). Additionally, the costs and efforts of satisfying CMMC Level 1-3 requirements scale with the organization's IT footprint and for Level 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.

SM.3 ***We are a small business supplying components to Lockheed Martin. How do we know if we need CMMC level 2 or 3?***

CMMC Level requirements will be driven by the prime contract and by the data in scope for the subcontract. Prime Contracts and subcontracts with CMMC requirements that include DoD controlled unclassified information (CUI) will require CMMC Level 3 (minimum). Review your existing contracts with Lockheed Martin to determine whether DoD CUI is in scope and discuss with your procurement representative if needed.

CMMC Level 2 is considered a "transitional" level between Level 1-Basic Hygiene, and Level 3-CUI Protection. It allows contractors to target and make CMMC Level progress between these two major levels. DoD has indicated that they do not expect to issue any prime contracts with CMMC Level 2 requirements.

SM.4 ***Are there special considerations for a one-person organization?***

Considerations for CMMC requirements are not directly related to the number of employees in an organization (generally speaking). A one-person organization would also be expected to have a very simplified IT footprint, so the effort to implement the necessary cyber controls should scale accordingly.

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: http://dodprocurementtoolbox.com/cms/sites/default/files/resources/2020-08/Cyber%20DFARS%20FAQs%20rev%203%20%207.30.2020.docx

- 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

- DAU Webinars/Presentations from Past Events:
  - https://www.dau.edu/Lists/Events/Attachments/272/CMMC%20Webcast%208.25.20.pdf
  - https://media.dau.edu/media/Cybersecurity+Maturity+Model+Certification+Migration+from+NIST+SP+800-171+to+the+new+CMMC+process+8.25.20/1_19qnl7cx/62971151

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