Suppliers CMMC FAQ

Additional FAQs can be found here.

1. Do you have to have CMMC per individual cage code?
    a. No, you can include all under parent cage code. For example, with SRC, we have a primary cage code, but included other locations of performance (i.e. remote offices) which have their own individual cage code. DCMA also recommends a master system security plan (SSP) vs a separate SSP for contract.
2. What are the ground rules for transferring externally?
    a. Any external communication of CUI must be encrypted using FIPS 140-2 validated crypto modules. 'Validated' is the key word. An application or appliance may claim to use AES-256, but unless the crypto module is 'validated' here, it is not compliant. For example, some applications use the built-in crypto module that comes with Microsoft Windows. This is acceptable as Microsoft's crypto module is validated. However, you must show proof from the vendor that it is indeed using Microsoft's crypto module, and not a home built one. If the application or appliance is using its own crypto module, it itself must be validated. Please refer to 5.I.3 in the NIST SP 800-171 Assessment Methodology.
3. Is Google suite not CMMC compliant?
    a. CUI requires cloud services to be Fedramp High compliant and DoD Impact Level 4 compliant. The Fedramp Marketplace doesn't specifically call out Google (G) suite but does call out Google services. It is unclear if this accreditation includes Google suite or not. Recommend contacting them and get a link that states this or an official email. You would need it during an audit.
    b. One supplier indicated G suite is FedRAMP Moderate.
        i. If this is true, it is compliant for CUI basic, but not CUI specified (controlled technical information or export-controlled information).
4. Is there a resource you can provide for obtaining either a DoD or CAC card?
    a. https://www.cac.mil/common-access-card/getting-your-cac/
    b. DoD ECA digital certificates can be obtained here.
5. How do we know how far down the CUI requirement flows?
    a. The requirements flow from the Prime to Tier 1 to Tier 2 as of now.
6. If we build an SRC product, but the lower-level drawings are our design, would our suppliers still need to be CMMC certified to have access to our drawings?
    a. If your design is being funded by the contract, then it's possible they are considered CUI and would require Tier 2 suppliers to also be certified. This is a discussion with contracts and program managers.
7. Is there any tax write-offs/deductions/discounts/etc. that can be claimed for spending money to become compliant?
    a. Refer to the CMMC website for this detail. It is yet unclear what the process is or how much can be reimbursed, and it may differ by CMMC level.
8. Is packaging considered COTS even if it is made to specific dimensions and material specs. Packaging is considered exempt for ITAR registration.
    a. Packaging should be considered COTS. It is not technical parts or information.
9. I presume Tier 2 suppliers are distributors. How deep will the distributors have to flow down CMMC, for example, do foreign suppliers to the distributors have to comply with CMMC?
    a. As of now, CMMC applies to the Prime and their Tier 1 and Tier 2 suppliers. For example, SRC (Prime) -> You (Tier 1) -> Distributors (Tier 2). In this example, suppliers to

Distributors (which would be Tier 3 and below) do not (currently) require certification under CMMC.

10. On slide 11 it reads "Are you providing COTS only? – certification not required. Can you elaborate on what that means and what certs we need as a COTS only provider?
    a. If you are a COTS ONLY supplier, CMMC does not apply to you. You do not have to be certified and do not need to go any further.
11. Will all your drawings be marked?
    a. Over time, yes. Legacy material will retain its original markings. New markings may be required on new documents. If new documents are derived from legacy documents, new markings would be required. There is DOD CUI handling and marking training available here. SRC will provide guidance as available.
12. Will all quote requests include a note stating that the effort requires CMMC and what level?
    a. Yes, all RFIs and RFPs will indicate if CMMC is required in advance of contract award.
13. Current understanding is that there may not be CMMC Assessors. Where do we locate certified assessors?
    a. The CMMC accreditation body was formed last year. They are currently training assessors for pilot DOD contracts which will include CMMC. Details are here.
14. CMMCAB is scheduled for their formal accreditation around the end of summer 2021, then they can certify other bodies (like Intertek). If an award is flown down with CMMC and a company is ready but could not get a certificate due to the constraints mentioned above, will that cancel the order?
    a. No, it should not. In fact, only (15) pilot contracts will have CMMC in FY21. At this time, none of them relate to SRC business. Another (75) pilot contracts are slated for FY22.
15. Does COTS exemption apply to software provided to SRC for SRC internal usage?
    a. If the software itself is COTS, yes, it would be exempt. If the software is developed for the contract, it could be CUI and require CMMC.
16. Are there resources to break down the controls needed to be implemented to meet full accreditation per level/control?
    a. Yes, visit the CMMC website. Looks for the "CMMC Appendices" which detail the required controls. This is a supplement to the existing NIST SP 800-171 controls.
17. Are machine programs created from CUI drawings still considered CUI?
    a. Possibly. Recommend discussion with Contracts and program managers.
18. Our interpretation as a Circuit Card Assembly provider that builds to your drawings, is that we do not need to flow down this to component distribution, but would need to flow this to any Printed Circuit Board vendors who view your drawings and any metal/fab house that your drawings were sent to? Or are they exempt as far enough down the supply chain?
    a. If your vendors who receive our drawings are Tier 2 suppliers under the Prime, then they would be subject to CMMC.
19. For those doing COTS only should we still comply with "Basic"? I would think we still need to have some level of compliance.
    a. It would be ideal to do this. Cyber requirements will change over time and could become more stringent. Any cyber security measures you can implement could only benefit your company in the long run.
20. How are COTS or MOTS parts suppliers held to comply? Is there a contract dollar amount that impacts whether or not you must comply?
    a. Compliance is not driven by contract value. COTS ONLY suppliers are not required to comply with CMMC.

21. How did you explain to your users such as engineers on how to determine if the drawings or documents they create are CUI?
    a. We are developing an internal program and process to educate engineers on identifying CUI. This is in conjunction with Contracts, Purchasing, Legal, Program Managers, and other internal parties. Additional information can be found on the CUI Registry.
22. If we have a DoD contract which requires CMMC, do contractors (individuals) hired to assist in the effort (such as write software) on or off-site, does that individual need to be CMMC compliant themselves?
    a. Yes, if they are accessing, storing, or processing CUI.
23. When will SRC start labeling prints with CUI label?
    a. Currently, SRC is in the process of determining that timeline. More information will be communicated as it is defined.
24. Will other Primes be rolling this out as well?
    a. Yes, many Primes are rolling this out in preparation. CMMC could impact over 300,000 companies that do business with the DOD and other agencies.
25. Do you know of any forums or chat rooms that are available for people who are trying to implement CMMC to go and bounce implementation ideas and resources off of together?
    a. Obtain access to the DIBNET portal and join the cyber security working group.
    b. Join the CMMC Academy at Celerium.
26. On the topic of varied implementations for different controls, are there lists with "recommended technologies" to use? That way we can all sort of get on the same page across industry.
    a. We encourage everyone to get involved with the entities referenced above. They send out periodic surveys to compile what tools companies use.
27. Are you moving entire organizations from commercial to Gov cloud or just users who need to email CUI?
    a. Because Microsoft 365 tenants cannot share domains, we were forced to move everyone to GCC High. Otherwise, those with access to CUI would need a new @domain for email within GCC High.
28. What is the responsibility of the tier 1 suppliers when it comes to CMMC flow down to sub-contractors/outside service?
29. Can you detail the Microsoft 365 compliant system?
    a. Here is a link to the Understanding Compliance Between Commercial, Government and DoD Offerings - February 2021 Update - Microsoft Tech Community.
30. What is IL-4 and where does that requirement come from?
    a. IL-4 refers to the DoD Impact Level 4. **Impact Level** - The identification (i.e., low-impact, moderate-impact, high-impact) is based on the federal government's requirements for the Confidentially, Integrity, and Availability (CIA) of the information or information systems accessed or processed by the cloud product or service per the Federal Information Processing Standards Publication 199 (FIPS PUB 199) - Standards for Security Categorization of Federal Information and Information Systems.
31. Is SRC GCCHigh?
    a. Yes, SRC utilizes Microsoft 365 GCC High for email, SharePoint, OneDrive, office, etc. Please note, due to cyber security requirements, not all features are available in GCC High as they are in the commercial cloud. Each new feature must be vetted for compliance. There is typically a delay in new features for GCC high spanning several months.

32. Have you experienced challenges connecting to Commercial tenants for SharePoint and Teams from the GCCHigh?
    a. Yes. Microsoft is aware of this and actively working on this. However, there are implications of need-to-know and cross-tenant access. GCC High has specific requirements for access.
33. Would T3 need to have Microsoft 365 GCC High for exchange email?
    a. Technically, CMMC is not being flowed down to Tier 3 or below (yet). I would encourage any company to protect CUI to the requirements under NIST SP 800-171 and CMMC.
    b. There are options you could implement, such as DOD ECA digital certificates for encrypting CUI, without moving your email to GCC High. SRC moved to GCC High to utilize its full suite of tools, not just email.
    c. SRC also has a Secure File Transfer system (sfs.srcinc.com) for securely transmitting files to/from suppliers. If you would like to use this, please contact us.
34. Is there a list of secure cloud services? FedRAMP? We are using Oracle.
    a. The FedRamp Marketplace lists all approved FedRamp cloud services and to what level.