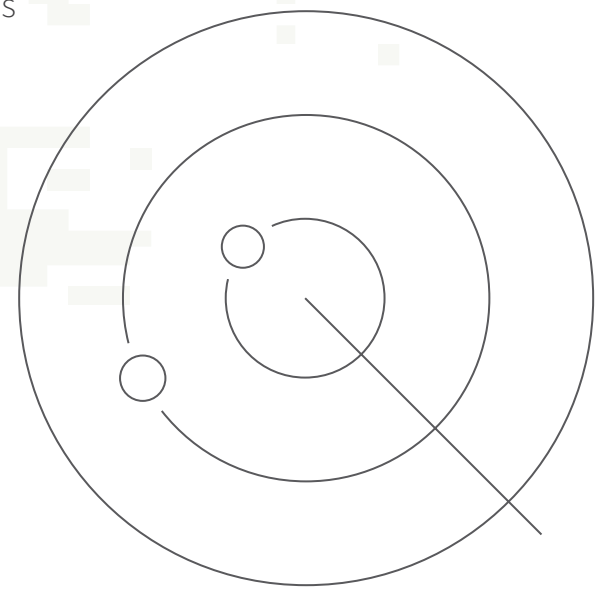
schellman
Quality. above all.

Panicked about CMMC?

Here's why you shouldn't be.

WHITEPAPER

Background



After several iterations of drafts and periods of public comment, the Cybersecurity Maturity Model Certification (CMMC) v1.0 was released on January 31, 2020. Throughout the review process, Schellman followed CMMC closely, having posted additional background in a previous blog, *CMMC – the New Protocol Droid for DoD Compliance.* More recently, Schellman also attended a CMMC Symposium in Washington, D.C. just three days before the release of CMMC v1.0, and gained valuable insight on the certification.

In the past, DFARS-mandated compliance with NIST SP 800-171 and a variety of contract-specific and agency-specific requirements were what served to protect all Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) that is processed, stored, or transmitted by the Defense Industrial Base (DIB) and ultimately the entire Department of Defense (DoD) supply chain. That resulted in a decentralized standard for defense contractors, whereas the purpose of CMMC is to provide a single, unified, and comprehensive cybersecurity framework for the protection of the same data.

Background (cont.)

With the implementation of CMMC, one of the biggest changes impacting contractors and service providers is the requirement of independent, third-party assessors to attest to or certify a contractor's maturity level. This differs from NIST SP 800-171 which allows contractors to self-attest for compliance with the requirements. Additionally, NIST SP 800-171 only holds one standard level of compliance, whereas CMMC provides five maturity levels that increase in complexity from Level 1 to Level 5. These five levels not only cover a contractor's technical security control capabilities in place, but also the maturity of its processes, policies, and procedures that support the security practices—CMMC terms this *process institutionalization.*

NIST SP 800-171 only holds one standard level of compliance, whereas CMMC provides five maturity levels that increase in complexity from Level 1 to Level 5.

In short, CMMC's focus is on the data – FCI and CUI – and the controls in place to protect and secure that data while it is being stored, transmitted, or processed by defense contractors and subcontractors.

schellman
Quality. above all.

Understanding the Relationship between CMMC and DFARS 252.204-7012

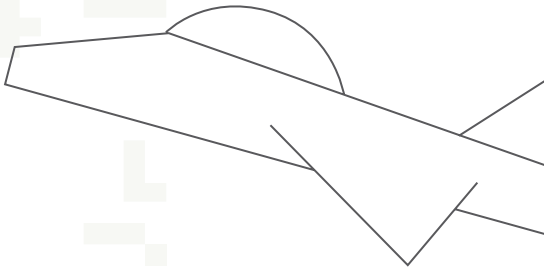
As of right now, Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 mandates a number of requirements for defense contractors, including compliance with NIST SP 800-171, specific incident response and reporting capabilities, and FedRAMP compliance for cloud service providers. Until the DFARS rule is updated and CMMC is codified, CMMC will not replace the requirement for contractors to maintain compliance with NIST SP 800-171 and any related obligations identified in contracts—all of the requirements under the current DFARS rule are still valid until updates are formally published.

While DFARS 252.204-7012 will be updated to codify CMMC with a projected timetable of Fall 2020, the impacts to other components of the DFARS rule are not known at this time.

Still, it's important to note that, similar to NIST SP 800-171, compliance with or certification to a specific CMMC level does not automatically indicate that a contractor is fully compliant with DFARS 252.204-7012 as it's currently written.

WHITEPAPER

schellman
Quality, above all.



Understanding the Timelines in Play

Phased Roll-Out

CMMC will be rolled out in a phased manner from Q4 2020 through Q3 2025, with the expectation that all contracts will contain the CMMC requirement beginning in Q4 2025. As such, this timeline will directly impact the expected number of prime contractors and subcontractors that obtain CMMC certification over the roll-out period.

WHITEPAPER

schellman
Quality. above all.

UNCLASSIFIED

Projected CMMC Roll-Out

DoD will work with Services and Agencies to identify candidate program that will have the CMMC requirements during FY21-FY25 phased roll-out

Total Number of Contracts with CMMC requirements

FY21	FY22	FY23	FY24	FY25
15	75	250	479	479

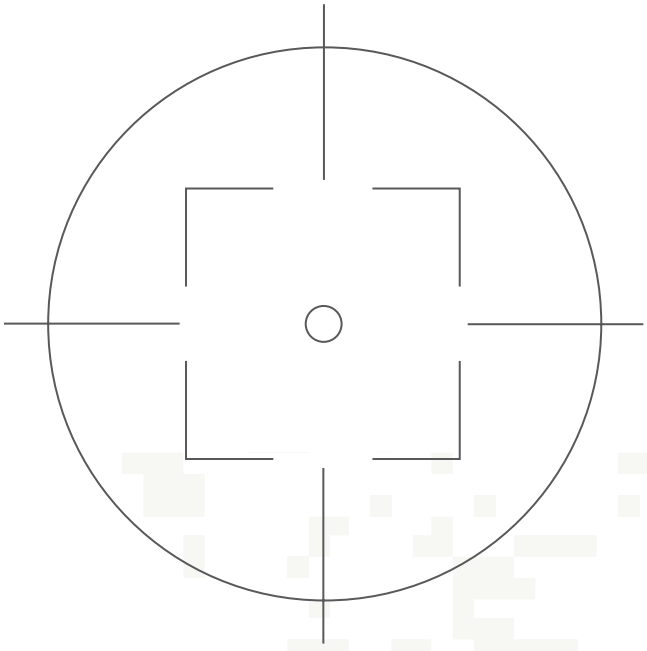
Total Number of Prime Contractors and Sub-Contractors with CMMC requirements

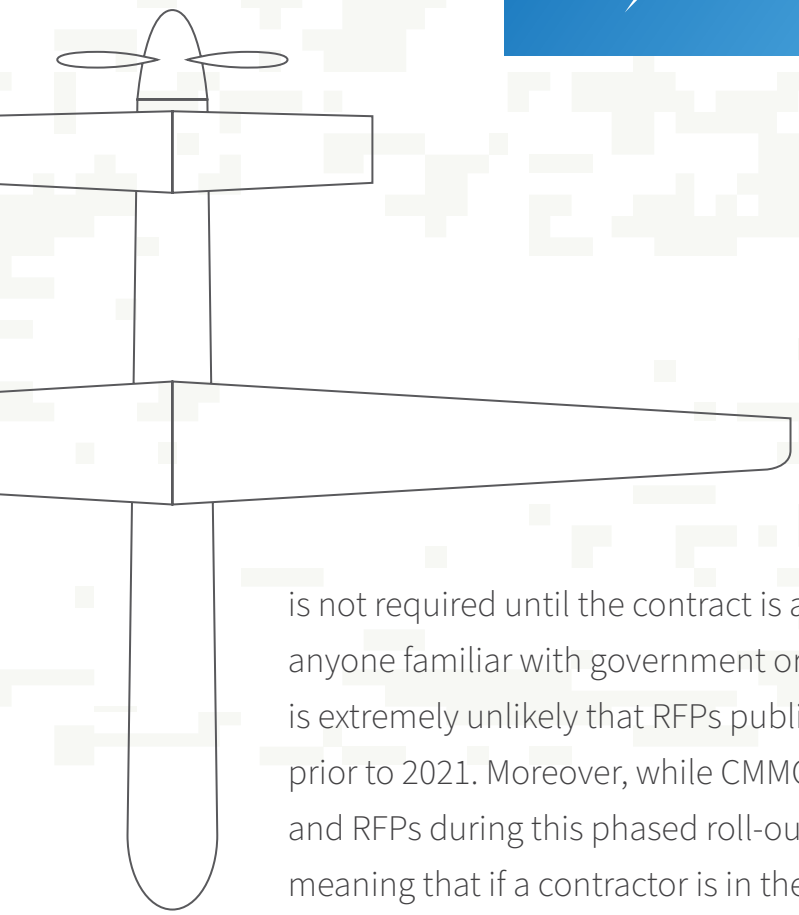
	FY21	FY22	FY23	FY24	FY25
Level 1	895	4,490	14,981	28,714	28,709
Level 2	149	748	2,497	4,786	4,785
Level 3	448	2,245	7,490	14, 357	14,355
Level 4	4	8	16	24	28
Level 5	4	8	16	24	28
Total	**1,500**	**7,500**	**25,000**	**47,905**	**47,905**

All new DoD contracts will contain the CMMC requirements starting FY26.
https://www.hklaw.com/en/events/2020/01/cmmc-impact-on-govcon-now-and-in-2020

So what about right now, in 2020? Will CMMC requirements be published in RFIs beginning in June and in RFPs beginning in August? Yes and no.

While the DoD has identified this five-year timeline for overall implementation, candidate programs to include contracts and contractors will also be selected for an imminent, limited roll-out. So yes, a very small number of selected contractors will see CMMC requirements in 2020. For this, the DoD will select a "Pathfinder" group of contractors and assessors in 2020 to perform CMMC assessment activities with the goal of refining the greater CMMC roll-out, assessor training, and accreditation steps. The identification and selection process will remain in place for the remainder of the phased roll-out through Q3 2025.





The overall phased roll-out also means that 99.99% of defense contractors *will not* need to be CMMC certified in 2020. Additionally, CMMC certification is not required until the contract is awarded—an important distinction, as anyone familiar with government or defense contracting will agree that it is extremely unlikely that RFPs published in August 2020 will be awarded prior to 2021. Moreover, while CMMC requirements are slowly added to RFIs and RFPs during this phased roll-out, *they will not affect existing contracts;* meaning that if a contractor is in the middle of a multi-year contract that does not expire until 2022, then the contractor would not be required to be certified at a specific CMMC level until the next RFP for that contract.

So while the looming 2020 milestones are accurate, they only apply to less than 0.01% of defense contractors, and even for that 0.01%, certification is not required until the contract is *awarded.* For most contractors, CMMC requirements will probably not come into play for a while.

Moreover, while CMMC requirements are slowly added to RFIs and RFPs during this phased roll-out, they will not affect existing contracts.

C3PAOs & Assessors

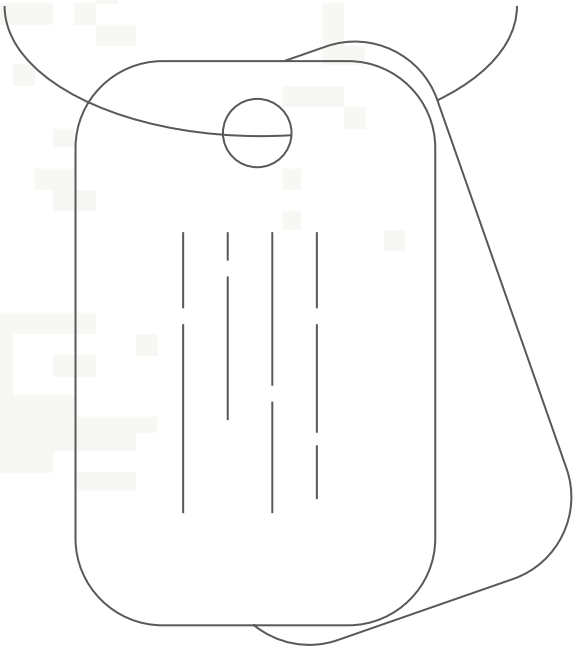
As previously noted, CMMC assessments are required to be performed by an independent third party, including certified third-party assessment organizations (C3PAO) and licensed assessors. To assist in the implementation of the new requirements, a non-profit CMMC Accreditation Body (CMMC-AB) was created in January to oversee and develop the community of C3PAOs and assessors, assessment criteria and methodology, and related training programs. The DoD and CMMC-AB require that assessors be trained and licensed to perform CMMC assessments in accordance with the to-be-determined assessment criteria. Assessors must also obtain a security clearance, though the specifics of the clearance—including type, timeline, sponsorship, etc.—are unknown at this time. All of these developments are planned to take place concurrently in order to meet the planned phased roll-out timeline.

A summary timeline of CMMC-AB activities related to assessment methodology, training, C3PAO certification, etc. is noted below:

Activity / Milestone	Expected Schedule (Draft)	
	Levels 1-3	Levels 4-5
CMMC Assessment Guides	Mid Q1 2020	Late Q1 2020
Draft CMMC Training Materials	Start of Q2 2020	Start of Q3 2020
Train the trainers; CMMC classes for assessors	Start of Q3 2020	Late Q3 2020
Certification of C3PAOs	Start of Q2 2020	

https://www.hklaw.com/en/events/2020/01/cmmc-impact-on-govcon-now-and-in-2020

Contractors

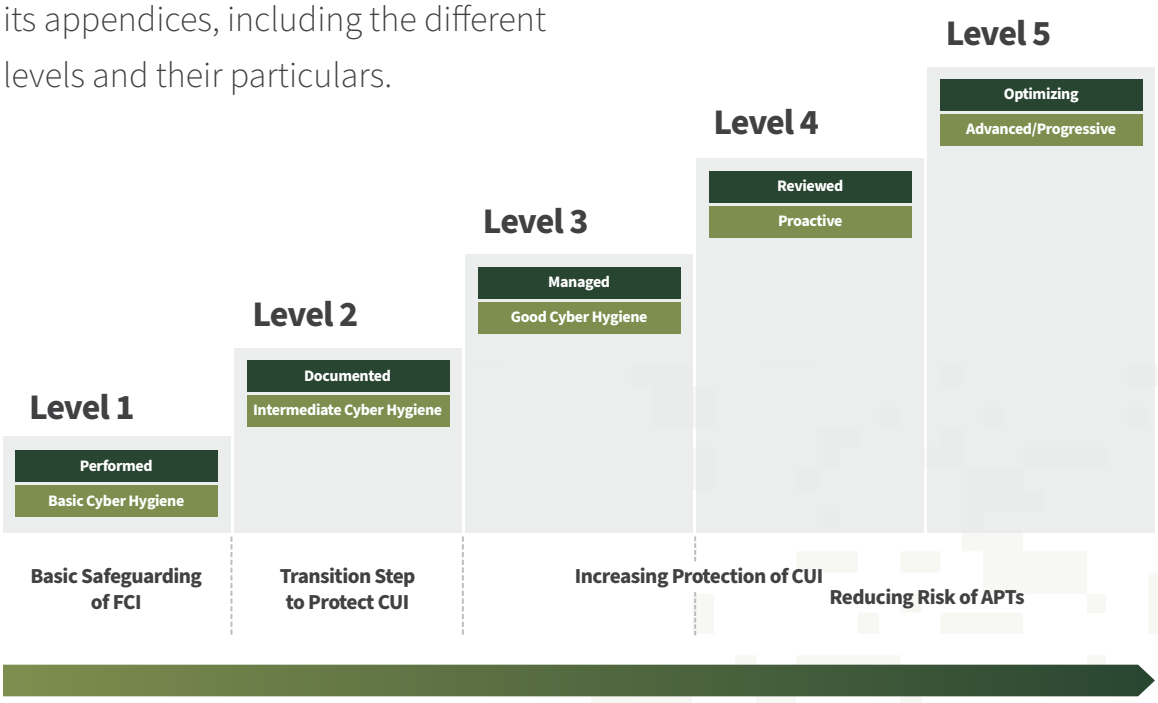


Because CMMC will require third-party assessments and contractors will not be permitted to self-assess, contractors should take note of the timelines for C3PAOs and assessors, as they will direct affect the ability and timeline for contractors to be certified. The complex activities associated with implementing CMMC do not happen in a vacuum, and contractors may request C3PAOs to begin assessment activities or to perform gap or readiness assessments. In order for formal CMMC certification assessments to occur, C3PAOs and assessors must be trained and credentialed by the CMMC-AB, which also means that the assessment methodology and training program must be in place with enough time allowed for C3PAOs and assessors to complete the programs and all related requirements to obtain the credentials. There are many dependencies in this process, and getting it off the ground will require coordination and patience from all involved. Currently, there are no certified C3PAOs or assessors.

schellman
Quality. above all.

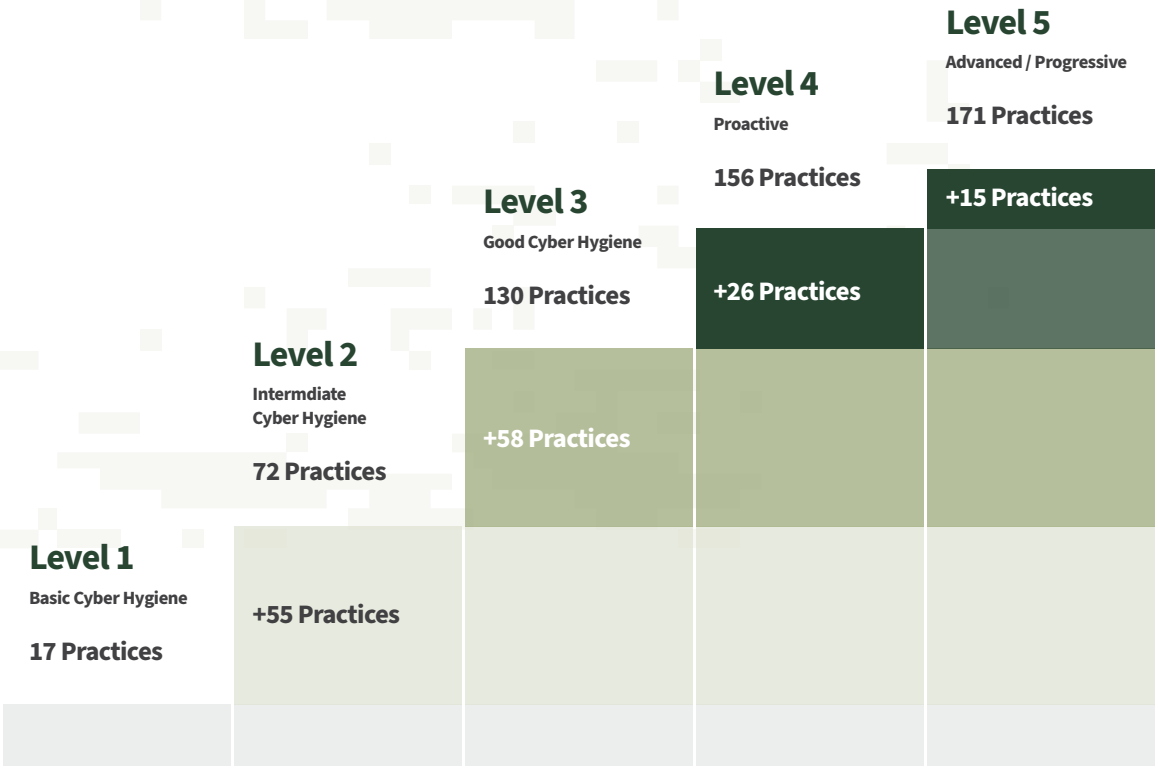
Overview of CMMC: Summary of the Maturity Levels and Relationship to NIST SP 800-171

In general, the published CMMC v1.0 does an excellent job presenting the domains, capabilities, practices, and processes in a variety of digestible ways. There are some details that should be paid specific attention within the information provided in the CMMC Model and its appendices, including the different levels and their particulars.



https://www.acq.osd.mil/cmmc/docs/CMMC_Model_Main_20200203.pdf

WHITEPAPER



CMMC Model v1.0

https://www.acq.osd.mil/cmmc/docs/CMMC_Model_Main_20200203.pdf

Level 1 is the minimum basic CMMC level, focused on protected FCI. It includes 17 of the NIST SP 800-171 requirements with no additional practices or processes.

Level 2 is a steppingstone to meeting Level 3 requirements of protecting CUI. It includes 65 of the NIST SP 800-171 requirements with an additional seven practices and two processes.

Level 3 is the closest equivalent to NIST SP 800-171. CMMC Level 3 includes all the NIST SP 800-171 requirements with an additional 20 practices and three processes.

Levels 4 and 5 are focused on protection of CUI from Advanced Persistent Threats (APTs), and will represent a very small number of contract requirements and contractor certifications. Specifically, the DoD estimates that 130,000 contractors will have CMMC requirements during the phased roll-out. Of these 130,000 contractors, only approximately 80 will see requirements for Level 4 and an additional 80 for Level 5, which equates to approximately 1% of contractors at Levels 4 and 5 combined for the phased roll-out.

Given all this, Level 3 certification may be a concern for many contractors. If so, determine whether or not there is an actual need to meet Level 3 requirements, as it's possible that Level 3 will not be required for the contracts in contractors' pipelines. Consider discussing such with contracting agencies, but do understand that they may not have an answer at this point in time.

Plus, 85% of Level 3 practices are carried over from NIST SP 800-171, which contractors have already attested to meeting, either via self-assessment or previous third-party assessment. If all claims to NIST SP 800-171 compliance were accurate and truthful, those contractors are *starting* at 85% compliant with CMMC Level 3. Meeting the remaining 15% of practices over the course of at least one year (or until required by RFP-designated CMMC requirement) should not be problematic or prohibitive. Nevertheless, there are nuances to the CMMC practices that should be reviewed in detail—even those carried over from NIST SP 800-171 requirements. See CMMC v1.02 Appendix B under "CMMC Clarification" for the specific practice.

Common Questions

The DoD has put together an FAQ section that is very useful. In addition, we've answered common questions our clients have asked below.

We don't touch CUI—does CMMC apply to us?

- Yes. CMMC focuses on FCI as well as CUI. If you are a defense contractor, you definitely store, transmit, or process FCI at a minimum.

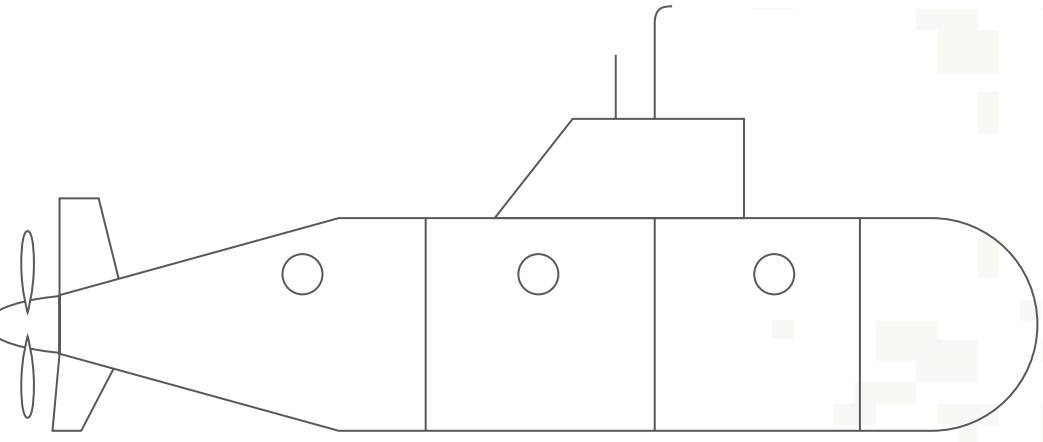
What about my subcontractors? Do they have to be certified too?

- Yes. Subcontractors must also be certified at the CMMC level required by the contract. CMMC targets the entire DoD supply chain, so primes are responsible for the status of their subs. The DoD is aware that there will be instances in which a prime contractor undergoing CMMC certification will have subcontractors that are not CMMC certified. The controlled roll-out of CMMC will need to take this into consideration and it was indicated that a plan would be developed for these instances.

Common Questions (cont)

How should contractors scope CMMC environments and assessments?

- We expect this to be further defined by the DoD and/or CMMC-AB in additional publications such as the CMMC Assessment Guides, training, or others. However, we do know that CMMC focuses on the data – FCI and CUI – and the controls in place to protect and secure that data while it is being stored, transmitted, or processed. So to begin identifying what systems within your organization fall into CMMC, follow the data. The level of complexity in this exercise is dependent on the size and complexity of your organization. Start with identifying the FCI and CUI that comes into your organization and then create data flow diagrams for the data. In doing so, you will have a better understanding of the systems that should be considered when scoping your control activities and CMMC assessments.



Sources:

https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012

https://www.cmmcab.org/

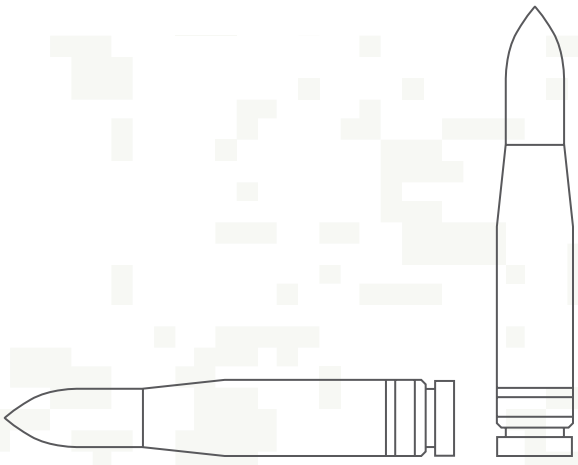
https://www.acq.osd.mil/cmmc/docs/CMMC_v1.0_Public_Briefing_20200131_v2.pdf

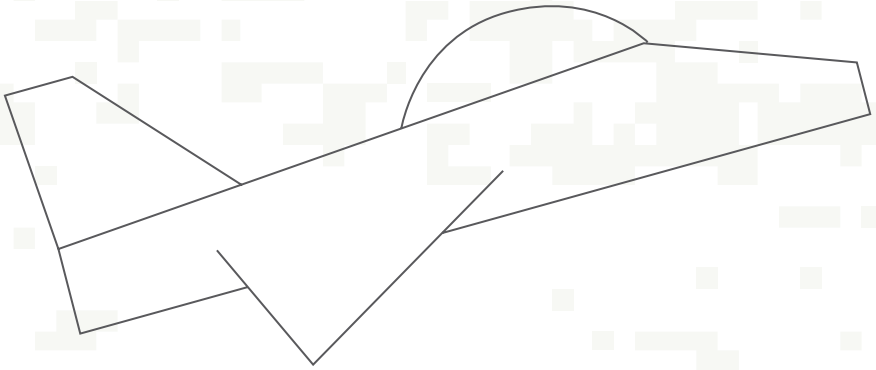
https://www.acq.osd.mil/cmmc/docs/CMMC_Model_Main_20200203.pdf

https://www.acq.osd.mil/cmmc/docs/CMMC_Model_Appendices_20200203.pdf

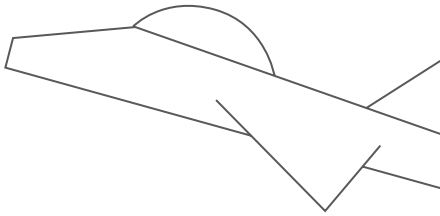
https://www.acq.osd.mil/cmmc/faq.html

Slide deck shared during the 1/28 CMMC Symposium:
https://www.hklaw.com/en/events/2020/01/cmmc-impact-on-govcon-now-and-in-2020





The Schellman team is ready to help you with your CMMC certification needs.



CLICK FOR MORE INFO

schellman
Quality, above all.

www.schellman.com

4010 W Boy Scout Blvd, Suite 600

Tampa, FL 33607

1.866.254.0000

Outside of the United States,
please dial: +1.973.854.4684