AEROSPACE & DEFENSE

Cybersecurity Maturity Model Certification (CMMC)

Best practice guide

Contents

Executive summary

The defense industrial base faces significant challenges in meeting new DoD cybersecurity compliance mandate

Defense contractors are well aware of the Defense Federal Acquisition Regulation Supplement (DFARS), which mandates that Department of Defense (DoD) contractors adopt cybersecurity standards that follow the NIST SP 800-171 cybersecurity framework. Due to slow adoption of the standards, the DoD has released the Cybersecurity Maturity Model Certification (CMMC) to ensure that the standards are being assessed properly and are adequate for addressing security requirements throughout the defense supply chain. With five possible maturity levels, the CMMC is intended to safeguard Federal Contract Information (FCI) at Level 1, progress to protecting Controlled Unclassified Information (CUI) at Level 3 and reduce the risk of Advanced Persistent Threats (APT) to national security at Level 5.

The DoD is accelerating a proposed rule change incorporating the CMMC into DFARS 252.204-7012, to be finalized in Fall 2020. This means that CMMC will be a requirement for any company doing business with the DoD, as a prime contractor or lower-tier subcontractor.

The key difference is that while DFARS 7012 allowed contractors to self-attest to NIST SP 800-171 compliance after winning a contract, CMMC requires them to be certified before the contract is awarded.

An independent Accreditation Body is responsible for overseeing the assessors, and only certified assessors (C3PAOs) are permitted to grant certification, which will be valid for three years. The results of the assessment must indicate 100% adherence to the prescribed processes and practices. Remediation plans, or Plan of Action & Milestones (POA&M), are not permitted and will relegate an organization to a lower CMMC level. For those concerned about the cost of certification, it will be considered an allowable, reimbursable cost.

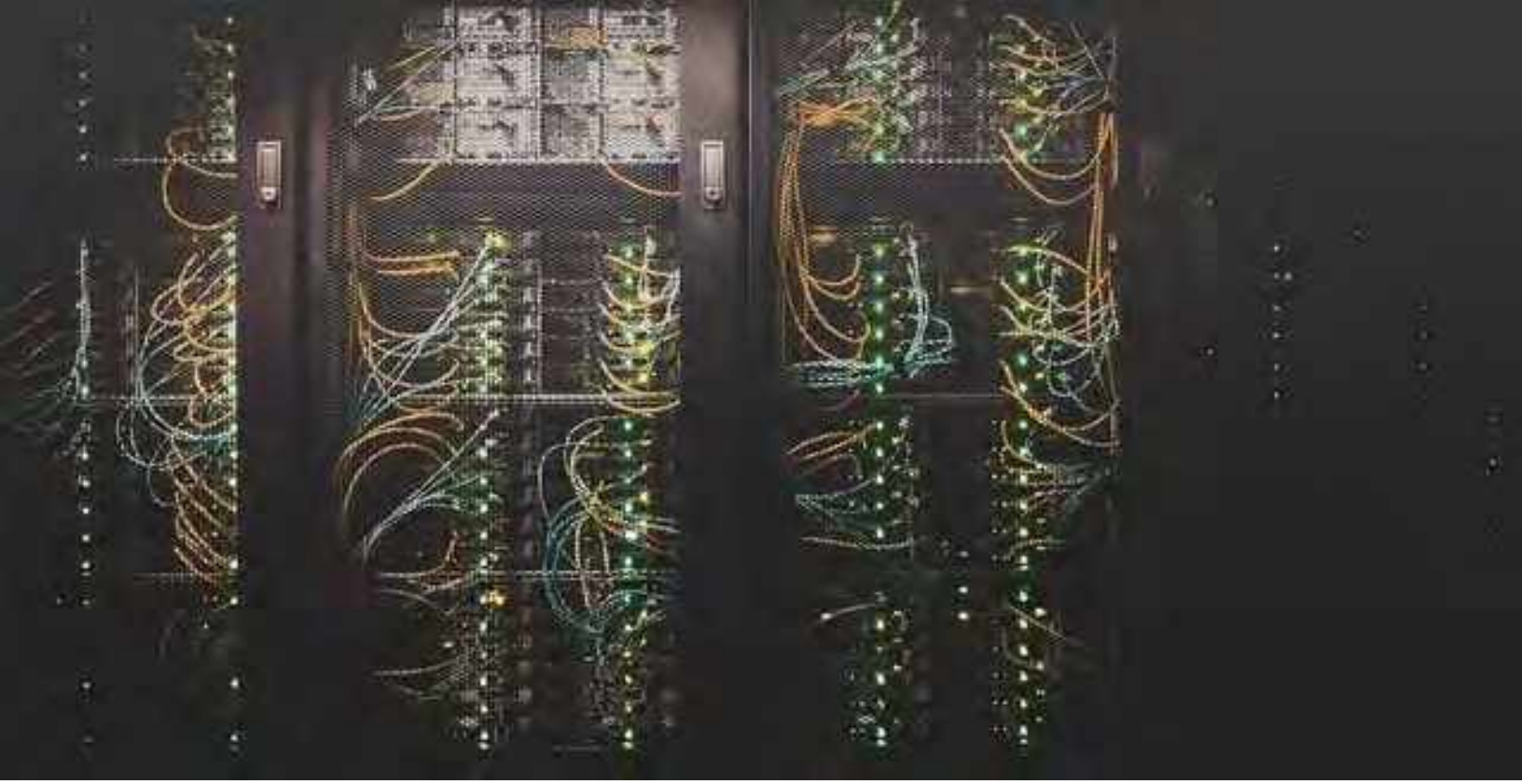
The timeline for fully rolling out CMMC is 2026. Existing contracts will not have CMMC applied retroactively, but the first RFIs and RFPs to include CMMC are expected by October 2020. CMMC will impact far more than the estimated 300,000+ companies in the

DIB, since CMMC will also likely appear in OTAs and other non-procurement contracts, which see more participation from small and mid-size businesses and non-traditional contractors. Defense contractors are found in all industries: aerospace, construction, engineering services, equipment suppliers, distributors, healthcare, higher education, manufacturing, professional services, and software development. Overall, small and mid-size businesses make up most of the DIB and face more significant challenges to meet CMMC since they typically have fewer resources to invest in cybersecurity and are less likely to be 800-171 compliant.

Rather than approach CMMC as yet another acquisition hurdle, contractors should view it as a differentiator. Contractors that obtain certification early, and are forward-thinking about the maturity level they target, will be eligible to bid on more contracts and avoid potential assessment backlogs. With Foreign Partners also interested in adopting CMMC, this mandate could also increase export opportunities. An important part of an organization's CMMC strategy will be to determine whether it can be accelerated by leveraging external services, such as compliance readiness audits, managed security services, or cloud-based IT systems and software-as-a-service (SaaS).

Adopting FedRAMP-authorized solutions that already implement the required security practices can provide an easier path to certification at a lower cost and may even enable smaller companies to target a higher CMMC maturity level.

In this guide, we look at the impact of CMMC on defense suppliers in all tiers and outline a strategy for how those organizations most impacted can turn CMMC into a competitive advantage.



Cybersecurity Maturity Model Certification

Protection of information and technology within the defense supply chain is a DoD high priority

Sensitive DoD information resides on IT systems controlled and operated by both federal agencies and government contractors. The loss of intellectual property, both unclassified and classified information, from DoD contractors is a critical threat to our national security because it weakens U.S. technological advantages and innovations. Perhaps the most cited example is the striking similarity between China's J-31 stealth fighter and the F-35 Joint Strike Fighter. Overall, global losses to our adversaries from cyberattacks are estimated at $600 billion a year, or about $4000 per individual U.S. taxpayer.[1] With increasingly sophisticated cyberattacks on contractor systems, the DoD implemented Defense Federal Acquisition Regulations Supplement (DFARS) clause 252.204-7012, Safeguarding Covered Defense Information (CDI) and Cyber Incident Reporting. Issued in 2016, this clause requires contractors to implement "adequate security" to protect "covered defense information" and to comply, contractors must establish a security posture by adhering to standards specified in NIST SP 800-171.

NIST SP 800-171 and DFARS 7012 aim to ensure vendor compliance and address any cybersecurity gaps. However, the NDIA has given the overall industry an industrial security score of 63, a D grade, the lowest among the eight dimensions they measure for health of the DIB.[2] In data compiled by Sera-Brynn from two years of assessments, they found that on average, companies implemented only 39% of the controls and zero companies were 100% compliant. [3]

CMMC is a switch from security compliance self-attestation to third party certification

Slow adoption of these standards is largely due to lack of expertise in cybersecurity controls, lack of enforcement of the contract flowdown provisions, and permitting contractors to self-attest to compliance only after contract award. To address these issues, the CMMC is a different approach in that the DoD is switching from self-attestation to independent third-party certification and will issue a proposed rule incorporating the CMMC into DFARS 7012. Expected to be finalized in Fall 2020, the DFARS rule change means that CMMC will apply to all subcontractors without regard to their supply chain tier position.

The CMMC was developed in collaboration with Johns Hopkins Applied Physics Laboratory, the Carnegie Mellon University Software Engineering Institute, academia, and defense industry trade associations, including NDIA, AIA, and PSC. In addition to NIST SP 800-171, CMMC is also based on NIST SP 800-53, AIA NAS9933, Center for Internet Security Controls, the NIST Framework for Improving Critical Infrastructure Cybersecurity, and international standards from the UK and Australia. The CMMC model framework organizes cybersecurity processes, capabilities, and practices from these sources into a set of 17 capability domains and maps them across five levels. Contractors will recognize many of these domains as having the same intent as the security control families in NIST 800-53, which is also the basis of the Federal Risk and Authorization Management Program (FedRAMP), which provides a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services.

CMMC capability domains

01. Access Control (AC)
02. Asset Management (AM)
03. Awareness and Training (AT)
04. Audit and Accountability (AU)
05. Configuration Management (CM)
06. Identification and Authentication (IA)
07. Incident Response (IR)
08. Maintenance (MA)
09. Media Protection (MP)
10. Personnel Security (PS)
11. Physical Protection (PE)
12. Recovery (RE)
13. Risk Management (RM)
14. Security Assessment (CA)
15. Situational Awareness (SA)
16. System and Communications Protection (SC)
17. System and Information Integrity (SI)

As a maturity model, CMMC captures progression in cybersecurity by introducing additional activities at each level and characterizing the extent to which the activities are embedded in the operations of an organization. The more embedded the practice, the more likely that the outcomes are consistent, repeatable and of high quality. Also, the more likely the organization will continue to perform the practice under times of stress. Level 1 focuses on "basic cyber hygiene" practices such as regularly changing passwords and using anti-virus software. Level 2 is a transition step to Level 3, which requires a significant increase from 17 to 130 practices and organizational policy in order to protect CUI. Levels 4 and 5 are intended for very critical technology companies working on the most sensitive programs, and require active cyberdefense against the tactics, techniques, and procedures used by APTs.

The CMMC Accreditation Body (AB) is a non-profit, independent organization that will accredit third party assessment organization (C3PAOs) and independent assessors.

The CMMC AB will establish a marketplace that includes a list of approved C3PAOs, and DIB organizations will be able to schedule an assessment for a specific level. The assessment will involve entering data into a centralized database managed by the CMMC AB, in-person visits by C3PAOs, and continuous monitoring between formal assessments. The CMMC AB is evaluating online tools that will provide a workflow and issue notifications whenever a company's security score has decreased by a certain amount. DoD staff will have access to the database to view metrics across the DIB for supply chain risk management.

	Processes (# at each level)	Practices (# at each level)	Relationship to existing regulations
LEVEL 1	Performed (0)	Basic Cyber Hygiene (17)	• Equivalent to all practices in Federal Acquisition Regulation (FAR) 48 CFR 52.204-21
LEVEL 2	Documented (2)	Intermediate Cyber Hygiene (72)	• Comply with the FAR • Includes a select subset of 48 practices from the NIST SP 800-171 r1
LEVEL 3	Managed (3)	Good Cyber Hygiene (130)	• Comply with the FAR • Encompasses all practices from NIST SP 800-171 r1
LEVEL 4	Reviewed (4)	Proactive (156)	• Comply with the FAR • Encompasses all practices from NIST SP 800-171 r1 • Includes a select subset of 11 practices from Draft NIST SP 800-171B
LEVEL 5	Optimizing (5)	Advanced / Progressive (171)	• Comply with the FAR • Encompasses all practices from NIST SP 800-171 r1 • Includes a select subset of 4 practices from Draft NIST SP 800-171B

100% adherence is required to bid on contracts

Defense contractors have become familiar with many security authorization processes, including the Risk Management Framework (RMF), FedRAMP, and obtaining an Agency Authority-to-Operate (ATO).

In addition to the requirement for third-party certification, CMMC has a few key differences from these processes that increase its rigor and impact:

- CMMC applies to an entire organization, not just to individual defense contracts, programs or systems. The security authorization processes listed above are more limited in scope, focusing on how individual program and systems are designed, implemented, and operated. Like ISO certifications in the manufacturing sector, FINRA in the financial sector, and HIPAA in the healthcare sector, CMMC evaluates the capabilities of an entire organization, which are expected to be leveraged during contract performance.

- CMMC certification is required before contract award, not after. Previously, NIST 800-171 self-attestation was required after contract award. CMMC has been described as a "go/no-go decision" and the required maturity level will be specified in RFPs for prime contractors and subcontractors. Instead of being one of many bidder qualifications that are scored as a part of source selection, security capabilities will now be one of the initial gate criteria.

- No POA&Ms are permitted. POA&Ms are key documents in a security authorization package and for continuous monitoring by tracking risk mitigation activities and the current disposition of any vulnerabilities and findings that require a corrective action. Since these actions essentially represent gaps in a security program, they are not allowed under CMMC. Failing to validate a single required practice means that the organization fails to achieve their targeted maturity level.

  A single security gap can drop an organization from Level 3 to Level 2 which means they cannot store or process CUI, leading to limited roles on defense contracts.

While CMMC is more stringent than previous requirements, these differences do present some benefits to contractors:

- The audits will be conducted by highly trained, neutral assessors rather than by individual government contractors and technical evaluators per contract. This means that the standards will be applied more consistently, and companies will not have to support multiple concurrent assessments by different agencies, or even different agency components. A CMMC certification is valid for all DoD departments, agencies, field activities, and commands.

- CMMC provides a benchmark that level sets the playing field. CMMC may actually benefit smaller businesses more in an acquisition culture that has tended to favor the Lowest Price Technically Acceptable (LPTA) model (FAR 15.101-2). As explained by Katie Arrington, CISO for OUSD A&S, a company that implements fewer security controls incurs less overhead cost and will likely have lower rates than another company that implements a greater number of and more advanced controls, even though both are technically acceptable under 800-171 self-attestation.[4] CMMC eliminates the trade-off between security and cost, schedule, or performance in proposal evaluations.

- CMMC reduces the risk of misrepresenting contractors' security posture to the federal government. Recent findings and judgments against companies in cases brought under the False Claims Act (FCA) highlight the potential liability and financial losses that can be imposed due to cybersecurity compliance failures. Industry analysts expect the number of FCA cases to increase since merely the possibility of a security breach, rather than confirmation of a successful breach, may be enough for successful enforcement of a claim.[5]

CMMC will have the greatest impact on smaller businesses and non-traditional contractors

Any DIB company that possesses Federal Contract Information must be certified at a minimum of CMMC Level 1. Level 1 essentially includes all defense suppliers, regardless of whether their IT systems actually hold DoD data, since the FAR 52.204-21 very broadly defines FCI as information provided by or generated for the Government under contract not intended for public release. Companies that solely produce Commercial-Off-The-Shelf (COTS) products do not require a CMMC certification. See the Department of Defense Guidebook for Acquiring Commercial Items to understand the difference between "commercial items" and "COTS" as defined in FAR 2.101 and DFARS 212.101. A good example is COTS components for military commercial derivative aircraft.

The critical threshold will be suppliers that store, process, or transmit Controlled Unclassified Information. Handling CUI requires CMMC Level 3 and compliance with the NIST 800-171, an effort that is still ongoing for many since the release of DFARS 7012 in 2016. All export-controlled data is considered CUI, so all companies that are currently required to be compliant with International Traffic in Arms Regulations (ITAR) will also need to become CMMC Level 3 certified. Suppliers will need to be certified regardless of their location. For Five Eyes and other alliance partners, the CMMC AB will build relationships with local accreditation bodies or certify allied foreign nationals to assess local companies. International certification procedures are not yet fully developed.

CMMC will likely have the greatest impact on smaller businesses, which make up the majority of the DIB and are recognized as a significant source of strategic defense innovation. However, they also typically have fewer resources to dedicate to cybersecurity and foreign adversaries know it. Increasing security does mean real costs associated with additional IT tools, IT implementation services, outsourced security services, and time required to conduct additional procedures. This cost and effort will need to be considered as companies choose what CMMC maturity level to target. However, the cost of certification will be considered an allowable, reimbursable cost with a statement already appearing in a DoD 2020.1 SBIR solicitation.

CMMC will also apply to non-procurement contracts and vehicles such as Other Transaction Authorities (OTAs) that are not subject to the FAR but will likely include CMMC as a technical requirement. Since OTAs have frequently been used by the DoD as a vehicle to rapidly evaluate technology from startups, small businesses, and commercially focused companies, the reach of CMMC may be far greater than the estimated 300,000 vendors in the DIB. These companies may have never worked with the government before or been assessed against NIST SP 800-171.

> "We know that the adversary looks at our most vulnerable link, which is usually six, seven, eight levels down in the supply chain.

Ellen Lord
Under Secretary of Defense for Acquisition and Sustainment (A&S)

Organizations should begin preparing now to be ready for CMMC

CMMC requirements will first appear in ten "pathfinder" solicitations in Fall 2020. Current active contracts will not have CMMC applied retroactively, but contractors can expect it when contracts face renewal, re-negotiation, or re-competition. The full CMMC rollout is planned to complete in 2026 because the typical duration of many contracts, as well as the Pentagon's budget process, is five years. Officials are beginning with high priority contracts, which include nuclear, missile defense, and major weapons programs. Critical strategic programs can have hundreds to thousands of subcontractors, who will receive contract flowdown requirements. Each RFP will state the CMMC levels required for specific roles, which will be found in Sections L and M as well as the Statement of Work. Many subcontractors will likely require a lower maturity level than prime contractors. However, since certification is required by the time of award, subcontractors could be asked to provide verification much earlier as part of teaming agreements.

Organizations should begin preparing now to be ready for self-assessment and third party certification. Closing security control gaps could require major decisions such as procuring additional IT, migrating IT infrastructure, and adopting different back office business systems or user devices, not to mention extensive documentation of organizational standards, policies, and procedures to provide evidence of compliance. CMMC also includes controls beyond what contractors are used to in NIST 800-171, including cybersecurity governance, asset management, and situational awareness. This is a time of uncertainty for defense suppliers since the CMMC rulemaking process is not complete, and there are no firm timelines for when assessors will be ready to begin scheduling assessments. Meanwhile, the following section provides a guide for how organizations can position themselves for greater success.

While the timeline for CMMC is evolving, here are some estimated dates to track (as of May 2020):

May 2020
CMMC AB Marketplace

June 2020
Initial RFIs with CMMC Requirement

July 2020
Initiate CMMC AB training for assessors and Defense Acquisition University training for acquisition officials for Levels 1-3

Sept 2020
Complete DFARS Rulemaking Process

September 2020
Initiate CMMC AB training for assessors and Defense Acquisition University training for acquisition officials for Levels 4-5

October 2020
Initial RFPs with CMMC Requirement (dependent on final Rulemaking)

Getting ready for CMMC

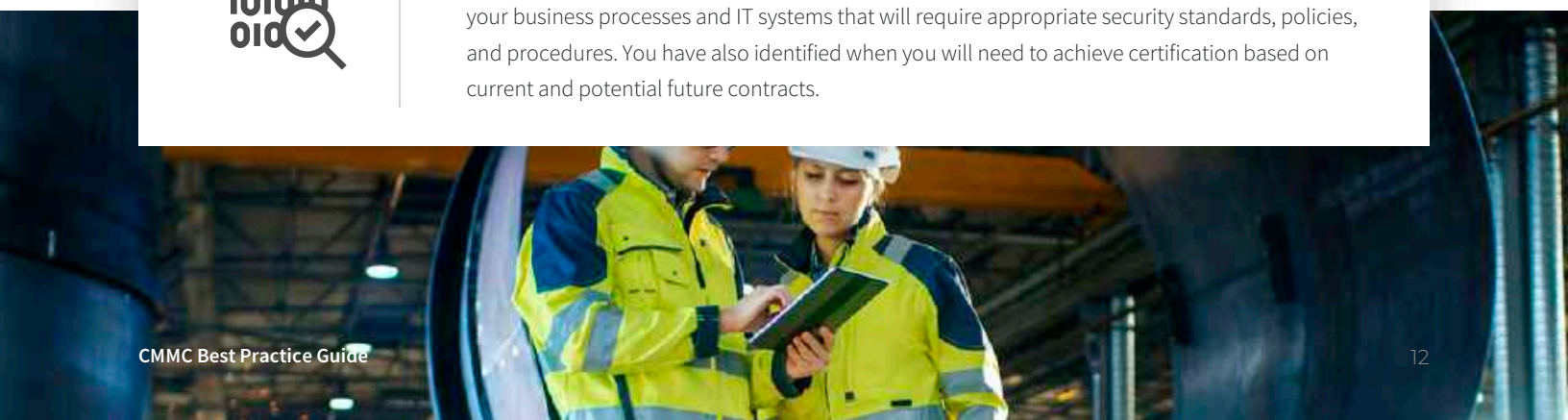
Step 1:
Identify target maturity level

An organization's target maturity level depends on the contracts they are currently performing on and programs they are interested in bidding on in the future. One shortcut is that if ITAR regulations apply, then at a minimum, CMMC Level 3 certification is required. Both current contractors and those new to DoD programs should review the RFIs and RFPs expected in Fall 2020 to understand what maturity levels are being required for typical program roles.

For organizations that do both commercial and defense work, current guidance recommends that all documentation delineate processes and procedures by division, department, physical location, etc. as necessary. While a wider scope may mean that it takes longer to remediate any security gaps to obtain an initial certification, it is less likely that a re-certification will be necessary if the business expands or re-organizes and more systems come within scope of CMMC. CMMC applies only to a contractor's unclassified networks that handle, process, and/or store FCI or CUI. Work with your current business partners to identify all your possible options. The DoD, defense industry trade associations, and prime contractors are looking at ways to assist smaller businesses, such as providing and maintaining secure infrastructure and facilities that could lower the maturity level required of subcontractors. Prime contractors should identify their sole-source suppliers and evaluate the impact on delivering products and services if the supplier cannot or will not get certified.

To identify the target maturity level, current contractors should:

- Confirm the DFARS CDI/CUI clauses that currently apply to your organization.
- Identify the dates when current contracts will expire as well as expected solicitation dates for contracts you are interested in bidding on.
- Perform a data discovery to confirm what CDI/CUI is currently stored, processed, or transmitted by your organization.
- Identify all IT systems that require security controls, especially those that store, process or transmit CUI, and the personnel that need access to those systems.
- Examine your business processes to determine whether identified CDI/CUI can be limited to the least number of IT systems, networks, and personnel to minimize the scope.
- Identify any existing System Security Plan (SSP) or other security policies and procedures used by your organization.



Exit criteria: Your organization has identified a target CMMC maturity level, the security controls that are needed to achieve that level based on the CMMC Model Framework, and the scope of your business processes and IT systems that will require appropriate security standards, policies, and procedures. You have also identified when you will need to achieve certification based on current and potential future contracts.

Step 2:
Determine whether external security or compliance services are needed

Based on an organization's target maturity level and experience implementing security controls like those in NIST 800-171, the quickest way to achieving CMMC certification may be to outsource some security and compliance activities to consultants or third-party IT solution vendors. For some use cases, this can be as simple as choosing to migrate from an on-premises IT solution to a cloud-based software-as-a-service (SaaS). The tools and skills required to achieve CMMC certification can mean a significant change in operating expenses, personnel, and administrative overhead. The overall impact, as well as whether these are temporary or permanent costs, should be considered when choosing whether to pursue CMMC certification entirely in house or to engage external expertise and services.

Organizations that require Level 2 or above and are facing NIST 800-171 for the first time through CMMC or have no dedicated security personnel should work with qualified third-party advisors to perform the remaining steps. For Level 3 and above, contractors will need standard operating procedures for handling of CUI, either in physical or digital form, such as manufacturing technical data.

Contractors should:

- Review any existing System Security Plan (SSP) or other security policies and standard operating procedures that were identified in Step 1.
- Identify who "owns" the security controls you identified in Step 1. Responsibility for security extends beyond just a security team. You may also have business process owners and IT asset managers. Also identify security controls that currently have no clear owner.
- Identify any tools in your IT portfolio that are currently providing security capabilities.
- Evaluate whether you currently have the necessary security expertise and personnel.
- Evaluate whether you will hire additional staff or use external services to perform the remaining steps to obtain certification. This may include a cost-benefit analysis based on your timeline for needing certification and your expertise in IT security solutions.

Exit criteria: Your organization has outlined a CMMC certification strategy based on NIST 800-171 compliance with clear roles and responsibilities, either internal or external. You have identified the scope of entities and IT systems within your organization to which CMMC will apply. You have gathered all existing business process, IT systems, and security-related documentation that require updating for submission to C3PAOs.

Step 3:
Conduct self-assessment and update supporting documentation

The self-assessment is a preliminary walkthrough of how an organization implements security controls and evaluates whether they are sufficiently documented, captured in policy, managed, or reviewed as required by a given CMMC maturity level. The quality of documentation is a significant factor in how long a third-party audit takes. The CMMC Model Framework provides crosswalks to other security standards, which will assist contractors that already reference these frameworks in their security programs.

Contractors should pay particular attention to these controls, if required, when completing the following activities:

- Create or update your System Security Plan. The plan describes how the security requirements are implemented, the system boundary, the operational environment, and relationships between IT systems. You may want to consider software solutions designed to guide organizations through how to document security controls and their implementation.
- Review your SSP and your organizational policies, standards and procedures for consistency.
- Capture all gaps and a preliminary remediation plan for each in a Plan of Action & Milestones (POA&M).

Both industry and government surveys generally report the same set of security controls as being not consistently implemented by defense contractors [3,6]:

3.1.3	Control the flow of CUI
3.1.11	Terminate a user session
3.3.4	Alert for audit logging process failure
3.4.2	Enforce security configuration settings
3.4.8	Black-/white-listing
3.5.3	Multifactor authentication
3.6.3	Test incident response
3.7.5	Multifactor authentication
3.8.4	CUI marking
3.8.5	Control CUI access
3.8.7	Control removable media
3.8.8	Prohibit portable storage
3.13.11	FIPS-validated cryptography
3.13.13	Control mobile code
3.14.1	Timely flaw remediation
3.14.7	Identify unauthorized use

Exit criteria: Your organization has updated all documentation typically required for a third-party security assessment: the System Security Plan, Plan of Action & Milestones, and organizational standards, policies, and procedures. These documents clearly describe how security controls are implemented, plans for closing any gaps, and a timeline for when the gaps will be closed.

Step 4:
Remediate gaps

The POA&M created in Step 3 serves as a to-do list to better organize, prioritize, and track the completion of all gap closure activities. Actions in the POA&M may require development of new organizational standards, policies, and procedures. Larger gaps may mean modifying the architecture of an organization's IT infrastructure and procurement of new software and IT security solutions. While decisions of this scale can be costly and time-consuming to implement, it can be an opportunity for organizations to consolidate on enterprise-wide solutions and standards. This not only streamlines the scope of security controls and documentation that need to be completed, but can also have other benefits in optimizing business operations and total cost of IT ownership.

Organizations that use SaaS IT solutions can leverage security capabilities and documentation provided by those cloud service providers (CSP), especially if they are FedRAMP-authorized.

DFARS 7012 states that security requirements equivalent to the FedRAMP Moderate baseline apply when a contractor intends to use an external CSP to store, process or transmit any CDI for the contract.

- Prioritize your POA&M based on an approach such as the NIST Risk Management Framework or based on the estimated timeline to complete. Take into account the time it takes to train personnel on new tools, processes, and procedures.
- Assign ownership of remediation actions based on the identifications you made in Step 1. Owners may be your security team, business process owners, IT asset managers, etc.
- Continuously update the POA&M as you finalize preliminary remediation plans.
- Continuously update the SSP as remediation actions are completed.
- Train all personnel as appropriate on updates to your organizational security standards, policies, and procedures.
- Train specific personnel with additional detailed information so they are ready to support the third-party assessors during the audit.

Exit criteria: Your organization has updated all documents typically required for a third-party security assessment: the System Security Plan and organizational standards, policies, and procedures. These documents were updated in accordance with your POA&M, which has been completed with no outstanding actions. All personnel have received security awareness training based on your updated documents. Appropriate personnel are ready to support C3PAOs with additional supporting information as needed during an audit.

Step 5:
Conduct CMMC readiness assessment

After completing the previous steps, organizations are ready to repeat their CMMC self-assessment as a final readiness check before the actual C3PAO audit. Organizations that have not used external services yet may consider doing so now to raise their level of confidence. This can also serve as a practice run for the actual audit.

- Repeat Step 3 by walking through all the security controls that are required for your target CMMC maturity level.
- Confirm that your System Security Plan and all organizational standards, policies, and procedures are consistent.
- Confirm that appropriate personnel have reviewed all documentation and are ready to support the assessor.
- Continuously maintain your security program, security awareness training, and update all documentation as necessary.

Organizations should take a continuous monitoring approach to protect their investment in a cybersecurity program and ensure ongoing capability that will make renewal of the certification easier.

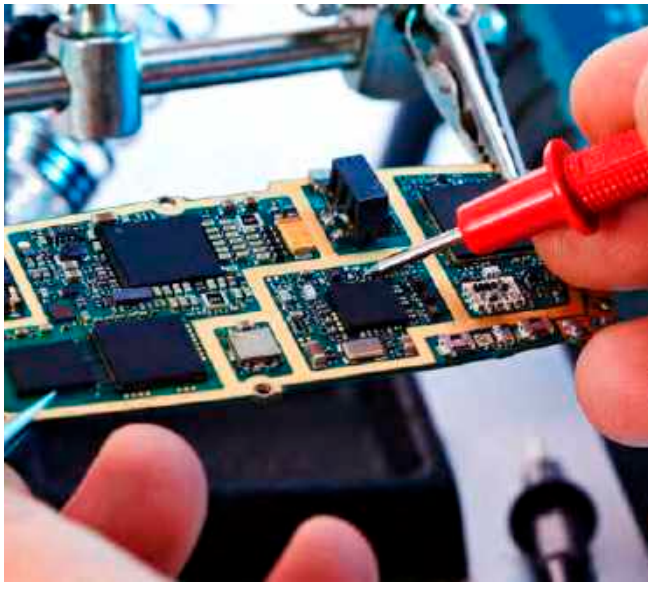
Exit criteria: Your organization is ready to identify a C3PAO from the CMMC Accreditation Body's website and schedule an assessment. All remediation actions are completed (no POA&M), and all documentation is ready for independent review. Personnel are prepared to support the assessment with additional information or demonstration as needed, based on their role on your security team or their ownership of IT systems or business processes. Organizations should take a continuous monitoring approach to protect their investment in a cybersecurity program and ensure ongoing capability that will make renewal of the certification easier.

Additional recommendations

Of the 300,000 companies in the DIB, it is believed that 290,000 currently have no cybersecurity requirements at all, and industry analysts think it is possible that CMMC could discourage smaller companies, start-ups and commercial companies from pursuing DoD contracts.[4] Companies that view CMMC as a differentiator, however, could see even greater opportunity. Here are three final recommendations for how CMMC certification can be turned into a competitive advantage:

1. Aim to achieve CMMC certification on the first attempt.

At this time, it is not clear how many C3PAOs and assessors will be trained and licensed by the CMMC Accreditation Body. Since CMMC will be a go/no-go decision and is required before contract award, companies that delay certification could get caught in a backlog of audits that cause additional RFP opportunities to pass them by, especially as many companies may not pass on the first attempt. Both industry and government reports surveying NIST 800-171 compliance indicate that contractors have struggled to satisfactorily implement the required security controls. Rigorous self-assessments and meticulous documentation may initially feel slow, but it will shorten the time it takes to complete an audit. Passing on the first try will also eliminate the fees associated with re-assessment and reduce the risk of becoming ineligible to bid on RFPs in your pipeline.



2. Use a high-water mark when choosing a CMMC level to target.

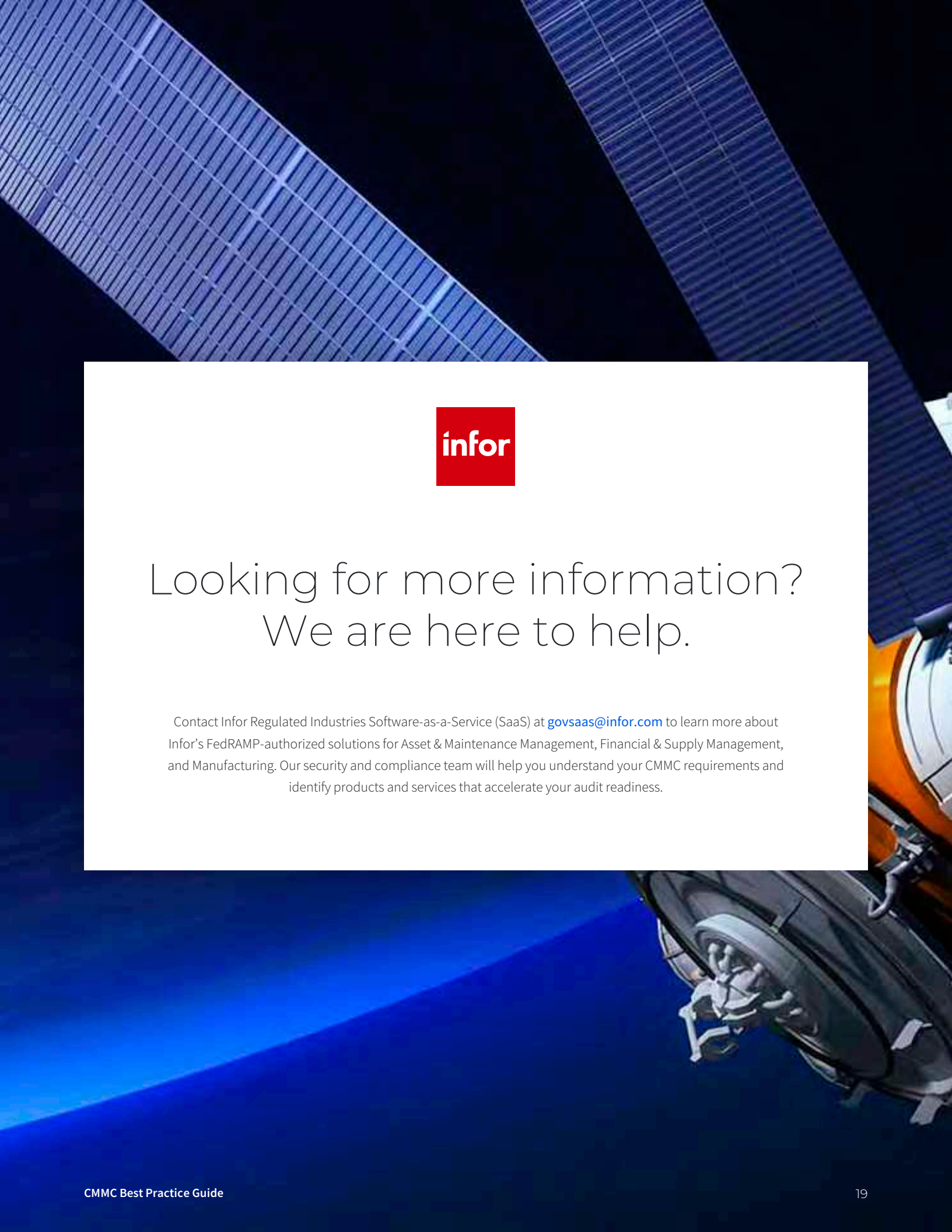
Since CMMC is a capabilities audit, it is possible for organizations to be certified at a maturity level that is higher than their current contract requirements. Contractors should consider targeting a higher level, especially if they are looking to move to Level 3 and have specific potential future contracts in mind. Level 3 requires significantly more security practices, but it allows a company to store, process, or transmit CUI. Depending on your timeline, it could be beneficial to only go through the certification once, rather than attempt to repeat the process in less than 3 years in order to be a qualified bidder. Defense suppliers could also see their business expand overseas, if they achieve the right maturity level. The DoD's CMMC team has been working with Foreign Partners and the EU Cybersecurity Body, and it is possible that other countries will also adopt CMMC.[7]

3. Accelerate your CMMC strategy with a partner that can provide security advisory services, managed information security services, and even software-as-a-service solutions.

Based on an organization's target maturity level and experience implementing security controls like those in NIST 800-171, the quickest way to achieving CMMC certification may be to outsource some security and compliance activities or outsource their IT systems entirely. Similar to independent security consultants, many cloud service providers also have extensive government cybersecurity expertise due to the assessment processes that are part of the FedRAMP program. Organizations that use SaaS IT solutions can leverage security capabilities and documentation provided by CSPs, especially if they are FedRAMP-authorized. Companies that have FedRAMP authorization already surpass the majority of the CMMC's control requirements, certainly at Levels 1-3, since FedRAMP requires continuous monitoring and improvement. The DoD is considering granting at least partial reciprocity between CMMC and FedRAMP because DFARS 7012 already allows the use of a cloud-based system certified at a minimum security level of FedRAMP Moderate.[8]

> If you are a vendor providing FedRAMP services, you are actually doing more than CMMC requires because, FedRAMP requires continuous monitoring.

Gordon Bitko
Senior Vice President of Policy for the Information Technology Industry Council and former FBI CIO[9]



Looking for more information? We are here to help.

Contact Infor Regulated Industries Software-as-a-Service (SaaS) at govsaas@infor.com to learn more about Infor's FedRAMP-authorized solutions for Asset & Maintenance Management, Financial & Supply Management, and Manufacturing. Our security and compliance team will help you understand your CMMC requirements and identify products and services that accelerate your audit readiness.

Citations

1. Department of Defense, "Press Briefing by Under Secretary of Defense for Acquisition & Sustainment Ellen M. Lord, Assistant Secretary of Defense for Acquisition Kevin Fahey, and Chief Information Security Officer for Acquisition Katie Arrington," January 31, 2020.
2. NDIA, Vital Signs 2020: The Health and Readiness of the Defense Industrial Base. February 2020. https://www.ndia.org/policy/vital-signs-2020
3. Sera-Brynn, Reality check: Defense industry's implementation of NIST SP 800-171, May 2019.
4. Exostar, "New DoD Cybersecurity Requirements Will Affect You in 2020," webinar, October 24, 2019.
5. Tina Reynolds and Rachael Plymale, "A watershed moment in cybersecurity for government contractors – anticipated impacts of the Department of Defense's Cybersecurity Maturity Model Certification Program," Government Contracts Insights (https://govcon.mofo.com/), January 7, 2020.
6. Department of Defense Office of Inspector General, "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems," DODIG-2019-105, July 2019.
7. Jon Harper, "U.S. Allies Considering Adopting Pentagon's CMMC Cybersecurity Standards," National Defense Magazine (https://www.nationaldefensemagazine.org/), March 4, 2020.
8. Lauren C. Williams, "FedRAMP may satisfy some security requirements for DOD contractors, security chief says," GCN (https://gcn.com/), November 18, 2019.
9. Government Matters, "New CMMC standards issued," February 3, 2020.

Other sources

- Office of the Under Secretary of Defense for Acquisition & Sustainment. Cybersecurity Maturity Model Certification. https://www.acq.osd.mil/cmmc/index.html
- CMMC Accreditation Body. https://www.cmmcab.org/
- Federal Acquisition Regulation (FAR) 52.204-21, Basic Safeguarding of Covered Contractor Information Systems. https://www.acquisition.gov/content/52204-21-basic-safeguarding-covered-contractor-information-systems
- Defense Federal Acquisition Regulations Supplement (DFARS) clause 252.204-7012, Safeguarding Covered Defense Information (CDI) and Cyber Incident Reporting. https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm
- Federal Risk and Authorization Management Program (FedRAMP). https://www.fedramp.gov/
- NIST SP 800-171 Rev. 1. Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final
- NIST SP 800-171B DRAFT. Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Enhanced Security Requirements for Critical Programs and High Value Assets. https://csrc.nist.gov/publications/detail/sp/800-171b/draft

Infor builds business software for specific industries in the cloud. With 16,500 employees and over 90,000 customers in more than 170 countries, Infor software is designed for progress. To learn more, please visit www.infor.com.

641 Avenue of the Americas, New York, NY 10011

INFDTP2323216-en-US-0520-1