The Ultimate CMMC Guide: Navigating New DoD Requirements

SECURANCE CONSULTING

the advantage of insight

www.securanceconsulting.com

NEW REQUIREMENTS FOR A NEW AGE

To help the Department of Defense (DoD) protect controlled unclassified information (CUI) within its supply chain, defense suppliers must now comply with new Cybersecurity Maturity Model Certification (CMMC) standards before being eligible to win DoD contracts. Any subcontractors will also be expected to comply with the appropriate maturity level.

As of yet, CMMC guidelines are unfinalized, so much is unknown. The final framework is projected to be published this summer (2021). In the meantime, this guide will help answer interim questions and provide clarity around CMMC and the expectations, costs, and hurdles that come with it.

CMMC STANDARDS

Understanding the foundation of CMMC is key to setting appropriate compliance goals. The framework has five maturity levels with increasingly advanced restrictions and cybersecurity protections, depicted below.

MATURITY LEVEL			
LEVEL	**PROCESSES**	**PRACTICES**	**FOCUS**
LEVEL 1	Performed	Basic	Safeguard Federal Contract Information (FCI)
LEVEL 2	Documented	Intermediate	Transition step in cybersecurity maturity
LEVEL 3	Managed	Good	Protect CUI
LEVEL 4	Reviewed	Proactive	Protect CUI and reduce risk of threats
LEVEL 5	Optimizing	Advanced	Protect CUI and reduce risk of threats

Level 1— Performed | Basic Cyber Hygiene: Organizations must follow basic safeguarding requirements and demonstrate compliance with 17 practices that protect FCI.

Level 2— Documented: Organizations have established and documented practices and policies. Includes some NIST 800-171 requirements, with a few regarding CUI protection. Includes 71 total practices.

Level 3— Managed: Organizations focus on protecting CUI and follow all NIST 800-171 security requirements, plus a few others. Includes 130 total practices.

Level 4— Reviewed: Organizations actively work to protect CUI from advanced persistent threats (APT) and comply with additional cybersecurity best practices, which enhance detection and response capabilities. Includes 156 total practices.

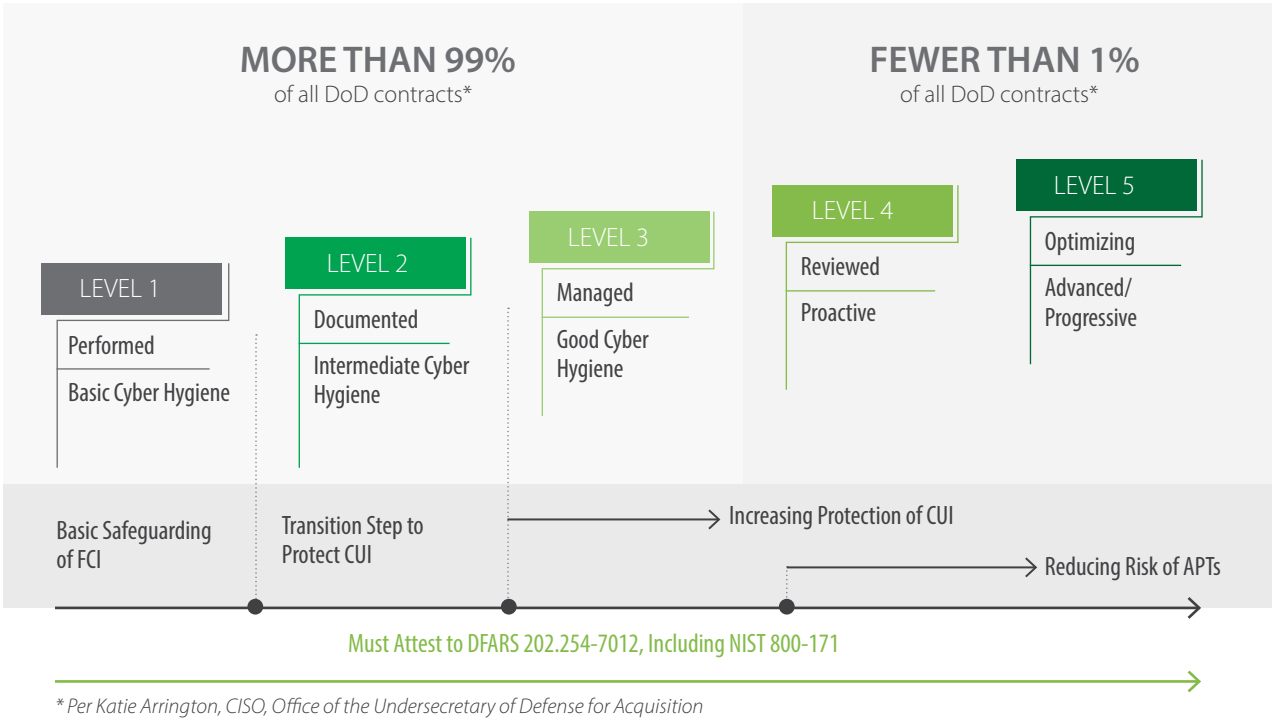
Level 5— Optimizing: Organizations standardize and optimize process implementation across the enterprise. Advanced cybersecurity capabilities protect CUI from APTs. Includes 171 total practices.

Knowing which maturity level an organization must comply with requires understanding what type of information (i.e., CUI) it handles. Some information is more sensitive than others. Suppliers handling more confidential contracts will need to guarantee a higher level of security. Common types of CUI include:

01. Information systems vulnerability information
02. Personally identifiable information (PII) processed, transmitted, or stored on behalf of the government
03. Technical information, including:
    a. Research and engineering data
    b. Engineering reports, drawings, data sets, research, or other materials
    c. Computer software executable and source code

Most, if not all, contractors who have worked with the DoD have some type of CUI data in their infrastructure. Determining which types is the first step in understanding what level of protection is required.

It's important to note that very few suppliers will need to comply past Level 3. It is estimated that only one percent of all contracts will require Level 4 or 5 certification.



** Per Katie Arrington, CISO, Office of the Undersecretary of Defense for Acquisition*

CMMC vs. NIST 800-171

At a glance, CMMC looks very similar to NIST 800-171, but there are several key differences.

01. CMMC requires DoD contractors and suppliers to be certified by CMMC assessors. This means self-certification is not an option for the more than 350,000 vendors in the U.S. DoD supply chain. The CMMC Accreditation Body (CMMC-AB) was created in 2020 to fulfill this need and estimates that 10,000 assessors will be required for the herculean task.[1]

02. Vendors that do not comply with CMMC will not win DoD contracts. This firm rule gives credence to the CMMC certification process and authority to the CMMC-AB.

03. Defense subcontractors— not just prime contractors— must also be CMMC-certified. Compliance with NIST (but not CMMC) standards is not sufficient.

04. CMMC standards break down NIST 800-171 requirements to provide equity to smaller firms. For example, while Level 5 (larger) companies must comply with all 171 control requirements, Level 1 (smaller) suppliers only need to comply with 17.

05. CMMC isn't just NIST 800-171. It's informed by multiple best practice standards, such as Federal Acquisition Regulation (FAR) 52.204-21, Center for Internet Security (CIS), Computer Emergency Response Team Resilience Management Model (CERT-RMM), and the NIST Cybersecurity Framework (CSF). Higher-level contractors will need to comply with all NIST 800-171 controls as well as additional domains, processes, and practices within the other standards.

06. CMMC adds three control domains (asset management, recovery, and situational awareness) to NIST 800-171's 14 domains.

NIST 800-171 AND CMMC CONTROL | CAPABILITY DOMAINS	
Access Control	Personnel Security
Asset Management*	Physical Protection
Awareness and Training	Recovery*
Audit and Accountability	Risk Management
Configuration Management	Security Assessment
Identification and Authentication	Situational Awareness*
Incident Response	System and Communications Protection
Maintenance	System and Information Protection
Media Protection	

New CMMC Capability Domains
Asset Management
Recovery
Situational Awareness

07. NIST 800-171 is control- and practice-focused only. CMMC covers both, plus process requirements, starting at Level 2.

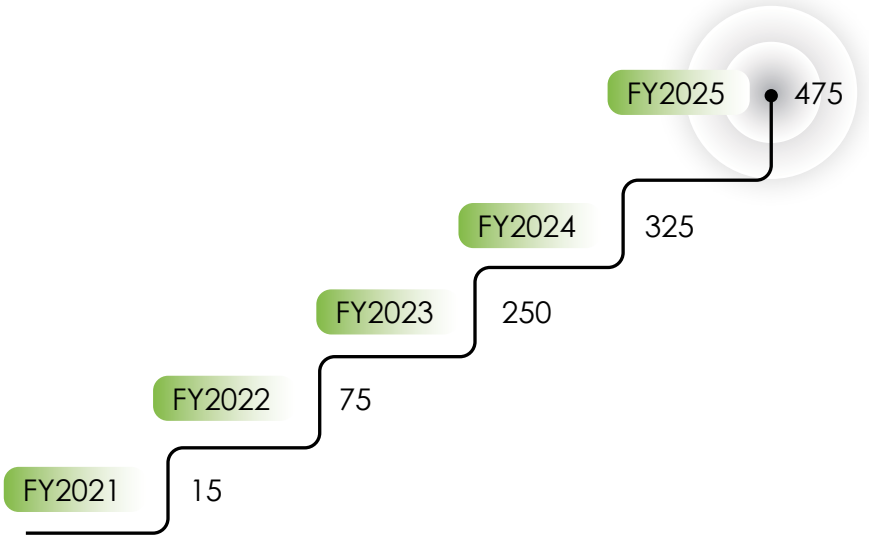
08. CMMC focuses more on cyber threat intelligence (e.g., indicators of compromise, threat hunting, and cyber threat sharing). Practices around situational awareness, cyber threat intelligence, and cyber threat alerts become exponentially more integral to compliance the higher you climb on the maturity ladder.[2]

In the end, compliance with CMMC does not inherently mean compliance with NIST 800-171. The DoD has intentionally taken guidance from multiple frameworks to add onto the standards created by NIST 800-171 and ensure a more holistic approach to national cybersecurity.

Because alignment with NIST 800-171 can be complex (and is required for CMMC compliance), it is strongly suggested that businesses who are unfamiliar with the framework enlist the help of a third-party cybersecurity expert. Working with a professional can save time, money, and human resources for other important business goals.

THE ROLLOUT PLAN

The DoD is implementing CMMC through a phased rollout plan, taking place between 2021 and 2025.



The DoD estimates 1,500 companies will be certified in 2021.[3] It has also provided seven contracts, which will serve as "experiments" for CMMC during its first fiscal year:

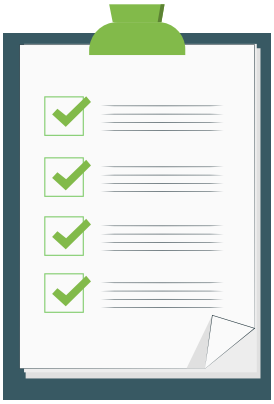
Navy
- Integrated Common Processor
- F/A-18E/F Full Mod of the SBAR and Shut-Off Valve
- Yard Services for the Arleigh Burke Class Destroyer

Air Force
- Mobility Air Force Tactical Data Links
- Consolidated Broadband Global Area Network Follow-On
- Azure Cloud Solution

Missile Defense Agency
- Technical Advisory and Assistance Contract

ACHIEVING COMPLIANCE

The road to compliance can be confusing, but it's comprised of the following steps:



01.

Perform a self-assessment (also referred to as a Basic Assessment) against NIST 800-171 requirements using the DoD assessment methodology[4] (or enlisting the help of a third-party cybersecurity firm)[5] and upload the score into the Supplier Performance Risk System (SPRS). Contractors must post their scores within 30 days of completing the assessment and supply the date they expect to be fully compliant, which should be realistic and take into consideration the available resources and budget. Scores are determined by how many of the 110 NIST 800-171 controls have been implemented.

Though it is not necessary to upload it unless the government performs a Medium or High Assessment, suppliers should also develop a Plan of Actions & Milestones (POA&M).

The confidence level for the Basic Assessment is defined as "low," because it is a self-generated score.

02.

After uploading to SPRS, contractors must remediate any security control gaps identified during the Basic Assessment by the date they provided to the DoD. If budget allows, hiring a third-party cybersecurity firm can increase the expediency and reliability of this important task.

03.

Following the Basic Assessment, the government can choose to perform a Medium Assessment, whereupon it will review the results of the contractor's self-assessment. This will include a thorough review of documentation and discussions with the contractor to clarify any details.

The confidence level will be defined as "medium" after this is performed.

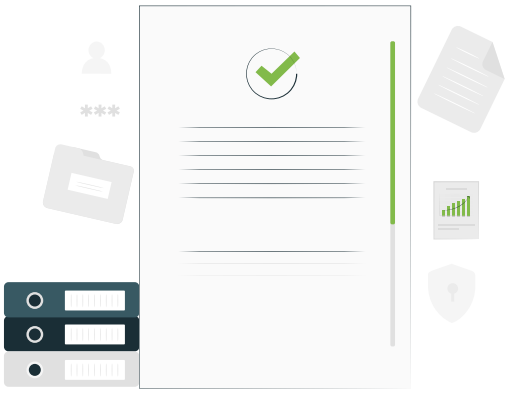
04.

The government can then also choose to perform a High Assessment, which encompasses all criteria for the Medium Assessment and adds the verification, examination, and demonstration of the contractor's system security plan (SSP) to validate that NIST 800-171 security requirements have been implemented as outlined in the SSP.

After this assessment, the confidence level is defined as "high."

05.

Once the Basic, Medium, and/or High Assessment is complete, and all shortcomings are remediated, contractors are ready to begin the process of complying with their appropriate CMMC maturity level. (See the "CMMC Standards" section for more details.) The maturity assessments must be completed by a certified CMMC Third Party Assessment Organization (C3PAO).[6]



06.

This process must be repeated every three years to maintain compliance.

POTENTIAL SPEEDBUMPS

At the time of writing, CMMC is not yet finalized, meaning multiple changes could happen between now and the official rollout. Concerns have arisen over the implementation responsibility of the CMMC-AB (a volunteer organization) and the speed of implementation, which has been grueling to meet DoD timelines.

CMMC-AB being a volunteer organization is problematic, because those lending their cybersecurity and defense expertise are doing so out of dedication to fulfill a critical national security gap— while performing their day jobs. The blazing pace set by the DoD puts additional strain on resources working for free and juggling their commitment to CMMC-AB with their actual careers. The potential for chaos is high without a focused team.

Additionally, CMMC-AB has twice published web pages about the new C3PAO program before they were approved for public release.[7] It also attempted to hold webinars last year with little success.

These types of accidents draw criticism from those already concerned about the CMMC-AB's ability to take on the massive responsibility the DoD has shouldered it with. A question of competence is the last thing an organization responsible for standardizing national security needs.

Despite the controversy, Ty Schieber, chairman of the board, is confident that the CMMC-AB will eventually be the formal organization critics expect it to be, with the staffing, finances, and expertise required to juggle both immediate needs and future strategies.[8] Time will tell if this confidence pays off.

COST

In addition to the potential hurdles described above, many experts have also questioned the inherent costs of CMMC compliance, for which there is no official structure.

Katie Arrington, Chief Information Security Officer (CISO) at the Office of the Under Secretary of Defense Acquisition & Sustainment, provided a cost estimate of between $3,000-$4,000 for Level 1 CMMC certification, during a DoD conference in 2020.[9] At this point, with CMMC guidelines unfinalized and consulting costs varying across the cybersecurity industry, it's impossible to provide a flat cost for compliance with any level of certainty.

One industrial group mentioned an unnamed defense company has spent approximately $250,000 to reach Level 3 certification, not inclusive of auditing or certification costs.[10] The reason behind such high costs is investment in cybersecurity technologies and resources required to comply with mandatory security controls.

Less often discussed are recurring engineering costs, which can become prohibitive for defense contractors (some estimates have reached the millions). The table below provides a summary of the total estimated annual costs for a small business to achieve each CMMC certification level. Nonrecurring engineering costs have been spread out over a 20-year period to determine the average annual cost. Similarly, assessment costs have been spread over a three-year period to represent reassessment occurring every three years.

CMMC Level	Average Nonrecurring Engineering Cost	Recurring Engineering Cost	Average Assessment Cost	Total Annual Assessment Cost
LEVEL 1	$0	$0	$1,000	$1,000
LEVEL 2	$407	$20,154	$7,489	$28,050
LEVEL 3	$1,311	$41,666	$17,032	$60,009
LEVEL 4	$46,917	$301,514	$23,355	$371,786
LEVEL 5	$61,511	$384,666	$36,697	$482,874

"The Pitfalls of Factoring in Security and CMMC Costs." National Defense, 8 June 2021.

STAYING AHEAD OF THE CURVE

Navigating new CMMC requirements will require a focused effort from organizations seeking to do business with the DoD. Contractors must determine the scope of CUI handled, complete a Basic Assessment (at a minimum), meet the level of maturity required to comply with DoD contracts, and ensure all subcontractors meet Level 1 requirements as well— permitting contractors do not share covered defense information (CDI) with them, which would require a higher level of certification.

Full CMMC compliance is more than a simple checklist. It requires active discovery, planning, assessment, and reassessment. With these new guidelines in place, initial and one-off hiccups aside, CMMC is poised to strengthen national cybersecurity and protect critical supply chains in lasting ways.

ABOUT SECURANCE

Securance has two decades of experience helping organizations combat evolved cyber threats, build effective risk management programs, align with compliance standards, and increase operational efficiency. Our comprehensive approach integrates proven methodologies, dependable expertise, and each customer's unique requirements to maximize the benefits and long-term value of each assessment.

SOURCES

1. https://cmmcab.org/
2. https://breakingdefense.com/2020/02/cmmc-1-0-vs-nist-800-171-eight-essential-differences/
3. https://www.insaonline.org/katie-arrington-dod-discusses-cmmc-rollout/
4. https://www.acq.osd.mil/cmmc/faq.html
5. https://www.securanceconsulting.com/cmmc-compliance/
6. https://cmmcab.org/marketplace/?search_category=headline&q=&search_method=contains&cat=1
7. https://cmmcab.org/c3pao-lp/
8. https://www.fedscoop.com/cmmc-dod-cybersecurity-requirments-contractors-timeline/
9. https://dreamport.tech/events/event-defense-industrial-base-cybersecurity-maturity-model-conference.php
10. https://about.bgov.com/news/defense-contractors-to-face-added-costs-with-cybersecurity-audit/
11. https://www.nationaldefensemagazine.org/articles/2021/6/8/the-pitfalls-of-factoring-in-security-and-cmmc-costs

The Ultimate CMMC Guide: Navigating New DoD Requirements

SECURANCE CONSULTING
the advantage of insight

13904 Monroes Business Park • Tampa, FL 33635 • 877.578.0215
www.securanceconsulting.com