SECURANCE CONSULTING

the advantage of insight

CMMC 2.0 COMPLIANCE GUIDE

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, about 300,000 defense suppliers that are part of the Defense Industrial Base (DIB) must now comply with rigorous cybersecurity standards before being eligible to win DoD contracts. Subcontractors will also be expected to comply with the appropriate maturity level. To meet this challenge, in 2020, the federal government announced Cybersecurity Maturity Model Certification (CMMC) 1.0, a framework for protecting data handled by defense contractors from cyber attack.

CMMC guidelines are still not finalized, and much remains unknown. In response to almost 1,000 public comments, in late 2021, the DoD decided to make compliance easier and less costly by introducing CMMC 2.0, which significantly streamlined the requirements of CMMC 1.0. As of this writing (June 2022), the rulemaking process is still ongoing, and CMMC 2.0 is expected to be finalized by the end of 2022.[1] In the interim, this guide will help answer some questions and provide clarity around CMMC 2.0 standards and the expectations, costs, and hurdles that come with it.

CMMC 2.0 STANDARDS

Understanding that the foundation of CMMC is NIST Special Publication (SP) 800-171 is key to setting appropriate compliance goals. The framework now has three maturity levels (CMMC 1.0 had five), with tiered assessments based on the sensitivity of information an organization handles,[2] as depicted below.

MATURITY LEVEL		
LEVEL	**PRACTICES**	**FOCUS**
LEVEL 1	Foundational	Safeguard Federal Contract Information (FCI)
LEVEL 2	Advanced	Protect CUI
LEVEL 3	Expert	Protect CUI and reduce risk of threats

Level 1— Foundational | Companies with Federal Contract Information (FCI) only: Organizations must adhere to 17 "basic cyber hygiene" controls specified in FAR 52.204-21. Level 1 certification will require annual self-assessments by the DIB company.

Level 2— Advanced | Companies with Controlled Unclassified Information (CUI): Organizations must adhere to the 110 controls specified in NIST SP 800-171. Level 2 is also separated into two categories based on the criticality of information stored by the contractor. Contractors in the first category handle CUI information that is not critical to national defense, so they can perform self-assessments similar to Level 1. Contractors in the second category handle information critical to national defense, so they will be subject to assessments by a Third Party Assessment

Organization (C3PAO). Level 2 certification will require annual third-party assessments or self-assessments based on the type of information they handle.

Level 3— Expert | Companies with Highly Sensitive CUI: Organizations must adhere to the 110 NIST SP 800-171 controls and up to 35 NIST 800-172 controls. The DoD will conduct assessments for organizations at this level every three years.

To learn more about how organizations proceed through the certification process, refer to the **Steps for Achieving CMMC Compliance** section on page 6.

Knowing which maturity level an organization must comply with requires understanding what type of information (i.e., FCI vs. CUI) it handles. CUI is highly sensitive and requires more restrictive handling than FCI. 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 DoD contractors have CUI data in their infrastructure. The type of CUI dictates the level of protection needed; the more sensitive the contract and information, the more stringent the security requirements.[3] Companies that are involved with the highest-level defense programs, approximately 1 percent of all DoD contracts, will require a Level 3 certification.

WHAT TO KNOW ABOUT CMMC 2.0

01. 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 Cyber AB (formerly CMMC-AB), the official CMMC accreditation body.

02. Subcontractors must also be CMMC-certified. Compliance with NIST, but not CMMC, standards is not sufficient.

03. CMMC is informed by multiple best practice standards, such as the Center for Internet Security (CIS) Controls, Computer Emergency Response Team Resilience Management Model (CERT-RMM), and NIST Cybersecurity Framework (CSF).

04. While the new CMMC 2.0 is heavily influenced by NIST SP 800-171, it is important to note that this framework is control- and practice-focused only. CMMC 2.0 covers control, practice, and process requirements, starting at Level 2.[4]

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

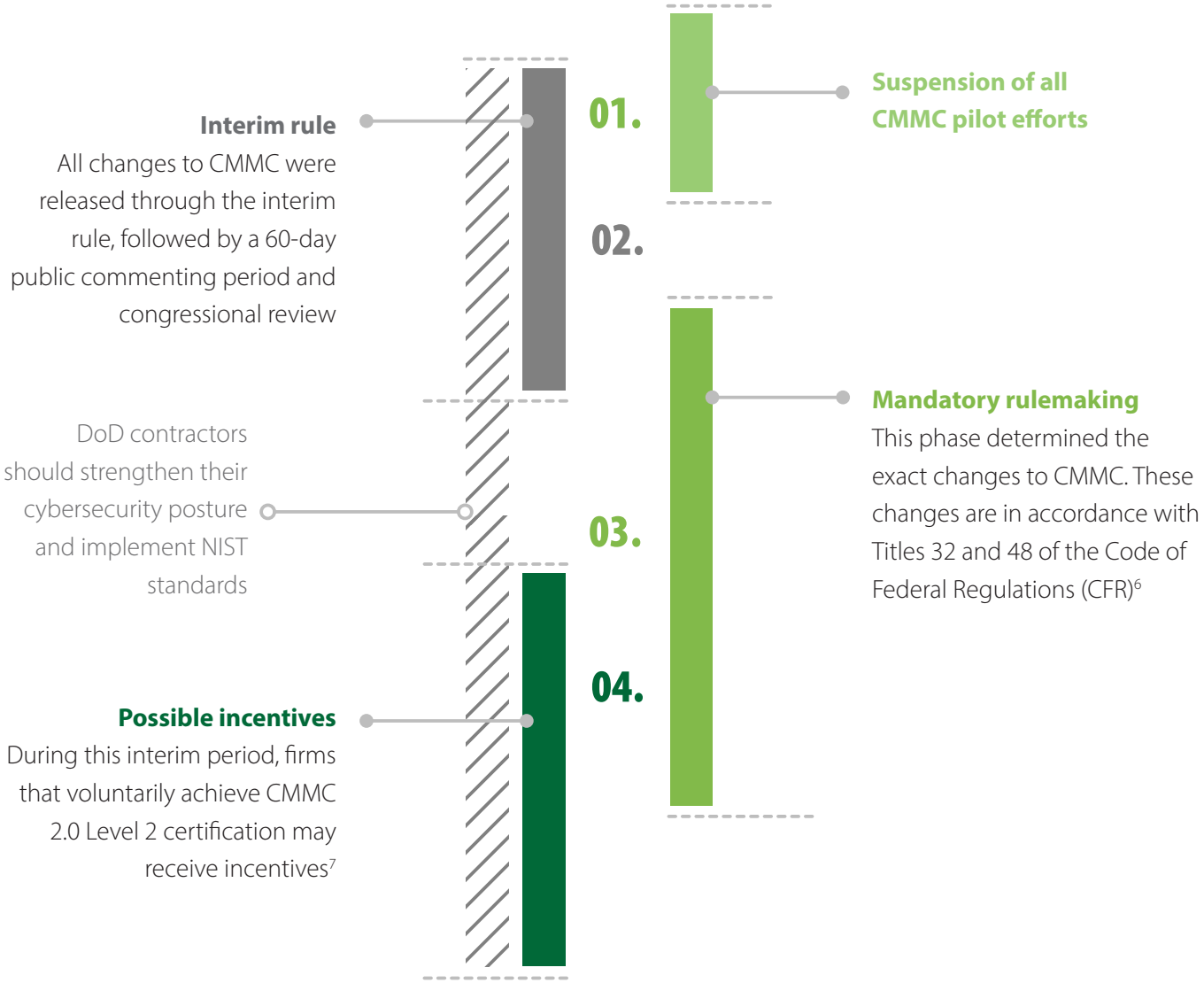
05. CMMC focuses more on cyber threat intelligence, including indicators of compromise, threat hunting, and cyber threat sharing, than NIST SP 800-171. Practices around situational awareness, cyber threat intelligence, and cyber threat alerts become exponentially more important to compliance as an organization ascends the maturity ladder.

In the end, compliance with NIST SP 800-171 does not mean compliance with CMMC. The DoD has intentionally taken guidance from multiple frameworks to add onto the standards created by NIST SP 800-171 to ensure a more holistic approach to national cybersecurity.[5]

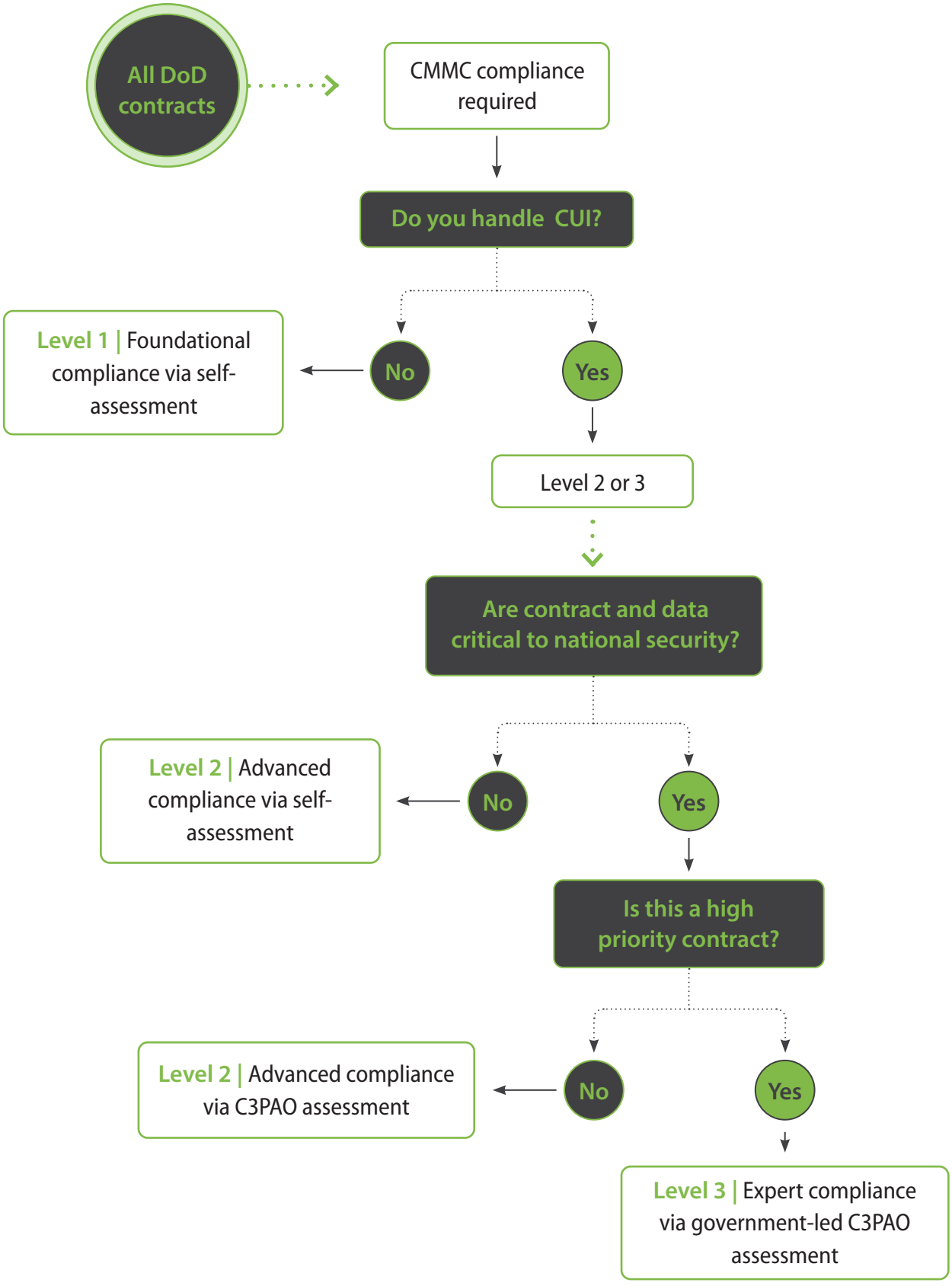
Because compliance with NIST SP 800-171 and CMMC can be complex, businesses unfamiliar with the frameworks should enlist the help of a third-party cybersecurity expert. Working with a professional can save time, money, and human resources for other important business goals.

THE ROLLOUT PLAN

Since CMMC 1.0 was suspended, and to ensure that CMMC 2.0 is implemented with enough input from all stakeholders, the DoD has yet to formally announce the launch of CMMC 2.0 or a firm timeline. In the meantime, the DoD has encouraged firms to strengthen their cybersecurity posture and comply with NIST standards in anticipation of a formal rule by the end of 2022. The initial phases for launch include:



Steps for Achieving CMMC Compliance



POTENTIAL SPEEDBUMPS

Until the DoD's rulemaking process is complete, vendors can expect further changes to the CMMC standards. In fact, given Cyber AB's status as a nonprofit with a volunteer board of directors, the industry has raised concerns over its ability to support the rapid implementation that the DoD requires. The volunteers lending their cybersecurity and defense expertise do so out of dedication to national security. Yet, they must balance their commitment to Cyber AB with full-time jobs, which means that the DoD's short timeframe for implementing CMMC may be unrealistic. Without a dedicated team, the potential for chaos is high.

For example, Cyber AB twice published web pages about the new C3PAO program before they were approved for public release.[7] It also tried to hold webinars last year with little success. These types of missteps attract criticism from government officials, industry groups, and cybersecurity companies, who worry that Cyber AB is under-funded, under-staffed, and poorly organized.

Finally, the accreditation body had to overcome internal challenges after dismissing key executives over conflicts of interest, tax exemption status, and pay-to-play accusations.[8] The body has been reorganized, but this upheaval has hurt the organization's reputation and impacted the implementation timeline.

> CMMC 2.0 should alleviate many of the compliance hurdles contractors face, but implementation issues persist.

COST

As the final version of CMMC is still being determined, the cost to vendors remains uncertain. Estimates for Level 2 compliance approach $20,000, while Level 3 compliance will likely cost hundreds of thousands.[9] The DoD is attempting to keep costs low by allowing contractors to self-certify against Levels 1 and 2 (in some cases). When the rulemaking process is complete, the DoD will release a cost analysis for compliance with each level.[10]

STAYING AHEAD OF THE CURVE

Navigating the new CMMC 2.0 requirements will require a focused effort from organizations that want to work with the DoD, and the sooner they begin, the better. Contractors should determine the scope of CUI they handle and complete a basic assessment against NIST SP 800-171 requirements. Prime contractors that use subcontractors must recognize that doing so adds an additional layer of complexity to the certification process. Subcontractors not privy to CUI must meet CMMC Level 1 requirements. Subcontractors working with CUI must meet the level of certification required by the contract. It is the responsibility of the prime contractor to ensure all subcontractors meet the appropriate certification requirements.

> Full CMMC compliance is more than a simple checklist. It requires active discovery, planning, assessment, and reassessment. Once the new CMMC 2.0 guidelines are in place, initial and one-off hiccups aside, CMMC will be poised to strengthen national cybersecurity and protect critical supply chains in lasting ways.

Contact Securance to learn more about how your organization can protect sensitive information, determine its CMMC maturity level, and better position itself to win DoD contracts.

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://www.rimstorm.com/cmmc-2-0-is-here-are-you-ready-for-the-changes/
2. https://www.acq.osd.mil/cmmc/assessments.html
3. https://www.acq.osd.mil/cmmc/faq.html
4. https://cmmc-eu.com/cmmc-domains/
5. https://www.bakertilly.com/insights/cmmc-2.0-five-key-changes-for-government-contractors
6. https://blog.charlesit.com/the-timeline-for-cmmc-2.0-rollout-what-you-should-know
7. https://cmmcab.org/c3pao-lp/
8. https://www.oxebridge.com/emma/katie-arrington-loses-congressional-bid/
9. https://etactics.com/blog/cmmc-certification-cost
10. https://www.acq.osd.mil/cmmc/faq.html

CMMC 2.0: Compliance Guide

SECURANCE CONSULTING
the advantage of insight

13916 Monroes Business Park, Suite 102 • Tampa FL 33635 • 877.578.0215
www.securanceconsulting.com