Are You Prepared for the Upcoming DoD Cybersecurity Audit Program?

DO YOU SELL PRODUCTS to any division of the U.S. Department of Defense (DoD)? Are you a subcontractor on a major defense contract? Do you want to be a DoD supplier? If you answered "yes" to one of these questions, please take note of an upcoming deadline that may affect your business. Beginning in September 2020, all vendors must show evidence of their Cybersecurity Maturity Model Certification (CMMC) when submitting a proposal for a DoD contract. Certification is achieved by passing an audit by an accredited and independent third-party commercial certification organization. The CMMC will have five levels, from Basic Cybersecurity Hygiene to Advanced. The contracting authority will request the necessary certificate level to bid on their contract.

Certification will be mandatory even if you aren't working with classified information and this includes sub-contractors for the DoD. "Please note that the landscaping contractor who cuts DoD facility grass will need at least a CMMC Level 1 Cert," wrote Eugene Jones, a Manufacturing Business Consultant with the Purdue Manufacturing Extension Partnership (MEP), in a recent newsletter.

For our readers being exposed to this information for the first time, let's review the backstory of the CMMC.

Why It's Needed

"Terrorists, criminals and foreign adversaries are using cyber to steal our technology, disrupt our economy and government processes, and threaten critical infrastructure," wrote Katie Lange in an article titled "DoD's Cyber Strategy: 5 Things to Know" published on the Department of Defense's website (www.defense.gov). Ms. Lange went on to describe the DoD's cyberstrategy that outlines their efforts to support the U.S. National Cyber Security platform, released in an Executive Order by the White House in 2019. Ms. Lange's article cited these goals of the DoD's cyberstrategy that are of particular interest to our industry:

- Preventing harmful cyber activities before they happen by strengthening the cybersecurity of systems and networks that support DoD missions, including those in the private sector
- Setting and enforcing standards for cybersecurity, resilience and reporting
- Holding DoD personnel and third-party contractors more accountable for slip-ups

In a 2016 cybersecurity summit at the U.S. military academy in West Point, Richard H. Ledgett Jr., then the deputy director of the National Security Agency, pointed out the vulnerabilities in the DoD supply chain. "More and more devices are being connected to the Internet," Ledgett said. "Some 6.4 billion things worldwide will be connected by the Internet this year, and by 2020, that number will be about 20.8 billion. The challenge is identifying emerging risks and vulnerabilities that come about with the introduction of new hardware and software. Any system is only as strong as its weakest link," he added. "Most types of devices connected to the Internet are built with differing security profiles and updated on differing timescales, and every time it's updated, that's another opportunity for a security vulnerability."[1]

While DoD prime contractors have been held to high cybersecurity standards for several years, the small- to mid-sized companies that supply DoD prime contractors often do not have robust cybersecurity defenses, making them targets for hackers. To overcome these weaknesses, DoD is launching CMMC to verify cybersecurity practices and processes are in place and to protect Controlled Unclassified Information (CUI) on the networks of DoD industry partners.

NIST 800-171, DFARS and CMMC

NIST 800-171 is a NIST Special Publication with requirements for protecting the confidentiality of Controlled Unclassified Information (CUI). Defense contractors had until December 31, 2017 to implement its requirements. NIST 800-171 has the following 14 sections that are then broken down into 110 required controls:

- Access Control
- Awareness and Training
- Auditing and Accountability
- Configuration Management
- Identification and Authentication
- Incident Response

1. "Critical Infrastructure Vulnerable to Attack, NSA Leader Says" by David Vergun at www.defense.gov.

- Maintenance
- Media Protection
- Personnel Security
- Physical Protection
- Risk Assessment
- Security Assessment
- System and Communication Protection
- System and Information Integrity

Defense contractors are also required to comply with the Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012 titled "Safeguarding Covered Defense Information and Cyber Incident Reporting." The clause specifies that all Department of Defense contractors and sub-contractors that process, store, or transmit Controlled Unclassified Information must demonstrate adequate security by, at a minimum, implementing the NIST 800-171 security requirements.

CMMC incorporates NIST 800-171 and several other cybersecurity control standards. Implementing NIST 800-171 assures compliance to the DFARS clause 252.204-7012. According to Eugene Jones, compliance to NIST 800-171 is a good approximation to achieving CMMC Level Three and Level Three will be necessary for any contractor manufacturing a product to DoD specifications.

The Benefits of CMMC to Industry

CMMC is being presented as a more realistic approach for small suppliers since a small company may not have to meet the stringent requirements of NIST 800-171. "If you are only selling nuts and bolts to a larger prime, there is no need for you to go through the effort of implementing all 110 requirements of NIST 800-171. You may only need to implement 63 of the new requirements to achieve a level 2 certification for CMMC, or even less to be level 1 certified," said Katie Arrington, Special Assistant to the Assistant Secretary of Defense, in an article at www.ComplyUp.com. The standard is meant to reduce ambiguity by clearly outlining what is expected to achieve compliance and how CMMC will be reinforced. (NIST 800-171 relies on organizations to self-assess and then report their compliance.) The consequence of non-compliance to CMMC will be very clear and immediate—a company without the appropriate level of certification will not be able to bid on DoD contracts.

An additional benefit of CMMC certification is that it's an asset to your entire customer base, not just the DoD. It shows your commitment to protecting their confidential information and it is an accomplishment similar to achieving ISO certification. A strong cybersecurity policy will also protect your company from threats like Ransomware and cyber theft from inside and outside your organization.

Timeframe for Compliance

According to the DoD, CMMC Version 1.0 (an assessment and accreditation tool) will be available in January 2020. In June 2020, industry should begin to see the required CMMC level in Requests for Information (RFIs). The standard's requirements will be included in Request for Proposals (RFPs) starting in September 2020.

Questions With Answers

If you think you will be affected by CMMC, you may have the following questions.

How Will CMMC Impact My Business?

Every contractor's existing work will be up for grabs depending upon which CMMC level is required by the contracting authority. You could lose or gain business, depending on if you obtain CMMC certification.

How Much Will Compliance Cost in Time and Money?

This depends on your level of cybersecurity hygiene now. The first step to obtaining CMMC certification will be an analysis of your current practices by an outside resource. (More on these resources later in this article.) After an analysis, you can determine if DoD business is worth the time and money needed to keep it. Ms. Arrington, at a Professional Services Council event in July 2019, said contractors could write off a portion of their cybersecurity spending for government contracts, including implementing NIST guidance. As of November 2019, no further information was available on this.

Questions With No Answers

Despite the hours of research I conducted for this article, I couldn't find a good answer to several questions.

- What is the appropriate CMMC Level for the contract? The only information I could find was "The government will determine the appropriate tier for the contracts they administer and the CMMC requirements will be part of Requests for Information."[2] (This could make it difficult to achieve the appropriate level in time to bid on the contract.)
- If a company sells an off-the-shelf product to a prime or subcontractor, will that company need CMMC certification?
- Since a supplier needs to be certified by a third-party certification vendor, is it realistic that every supplier can be certified by September 2020?
- What happens if a large number of DoD suppliers can't be certified in time? Will the deadline be extended? Or will many small companies drop out of the supply chain?

I'm not the only one with questions. CMMC is getting pushback from industry. Three of the largest defense industry associations—the Professional Services Council, the National Defense Industrial Association and the Aerospace Industries Association—are raising questions about CMMC,

2. The Office of the Under Secretary of Defense for Acquisition & Sustainment Cybersecurity Maturity Model Certification at www.acq.osd.mil/cmmc/faq.html.

including concerns about the implementation time line and the lack of clarity on how it will be applied across different programs and suppliers. "This would have severe unintended consequences on small businesses that do not have the resources and sophistication to obtain a high CMMC level, producing market entry barriers and limiting competition," the Professional Services Council wrote in a Sept. 25, 2019 letter to the DoD after a draft release of the plan.[3]

Next Steps

If you are unsure if you need to achieve CMMC, check with your prime contractor or subcontractor. They are already preparing for accreditation and they may know if you need to attain CMMC, and at which level, to keep their business.

If you do need to achieve compliance, a good place to seek information is the National Institute of Standards and Technology Manufacturing Extension Partnership (NIST MEP) program in your state. There are MEP Centers in all 50 states and Puerto Rico. (Visit www.nist.gov/mep/mep-national-network to find the program in your state.) Your MEP center may have already launched CMMC compliance assistance seminars. If you have IT staff, it is possible to achieve the appropriate CMMC level in-house, following the NIST Handbook 162 (see Resources below).

There are also numerous CMMC Consultants online that can help companies through the process, from assessment to audit.

In Conclusion: It's Only the Beginning

When I wrote this article in the fall of 2019, the launch of CMMC seemed very fluid to me. And I recognize that I lightly touched on critical components of CMMC, in particular NIST 800-171 and DFARS. To this end, I provided a few resources below to help you learn more about CMMC. ●

3. "Should Contractors be Fined for Their Subprimes' Cybersecurity?" by Andrew Eversden at www.federaltimes.com.

Resources

NIST Handbook 162 "NIST MEP Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements." Download at www.nist.gov/publications/nist-mep-cybersecurity-self-assessment-handbook-assessing-nist-sp-800-171-security.

The National Institute of Standards and Technology Manufacturing Extension Partnership at www.nist.gov/mep/mep-national-network.

Frequently Asked Questions on many aspects of CMMC are at the Office of the Under Secretary of Defense for Acquisition & Sustainment Cybersecurity Maturity Model Certification. (www.acq.osd.mil/cmmc/faq.html)

Seven Reasons You Need Strong Cybersecurity

1. Ransomware

According to Cybersecurity Ventures, Ransomware will have cost businesses and organizations around the world $11.5 billion in 2019 in ransom money, downtime and lost data.

2. Email

Email accounts are hacked because they are often a weak link in an organization's security pipeline.

3. Data breaches

A data breach can be caused by:

- Human error
- System glitches
- Malicious or criminal attacks

4. Laptops

Lost or stolen company laptops are a common cause for security incidents.

5. Employee theft

IBM's 2016 Cyber Security Intelligence Index found that 60 percent of all breaches are carried out by insiders, including current and former employees who—intentionally or unintentionally—take classified or proprietary information with them when they depart.

6. Lack of employee training

Do your employees know what to do when a data breach occurs?

7. Your customers

Your customers entrust you with their financial and business information. It's your responsibility to protect it. A strong cybersecurity policy should be part of your marketing materials—it demonstrates your commitment to good business practices. ●