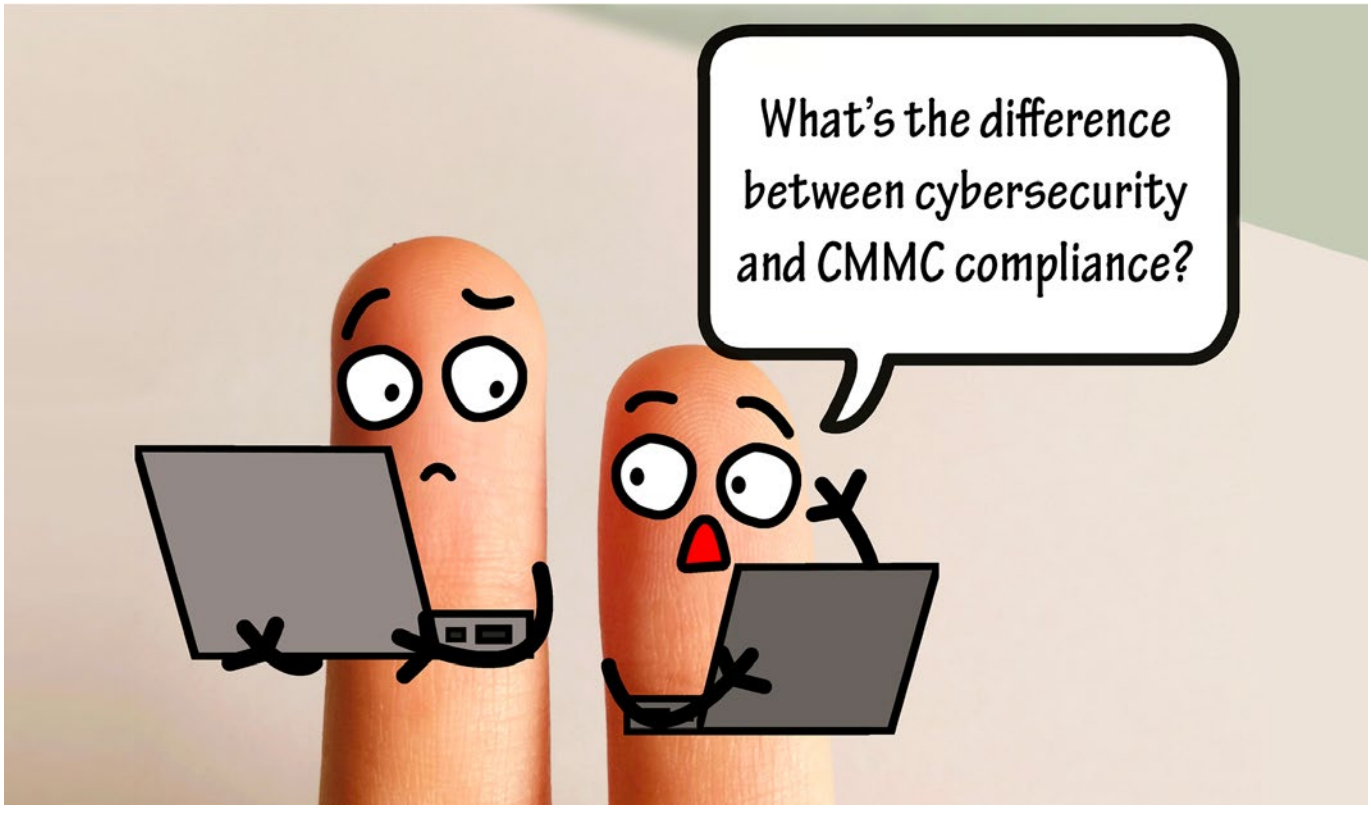

Panel Discussion: CMMC and Cybersecurity

Feature Q&A by Maribel Hernandez

The electronics manufacturing sector faces unique challenges when it comes to cybersecurity, given the highly sensitive nature of the information that it handles. With the introduction of the Cybersecurity Maturity Model Certification (CMMC) framework, businesses will soon be required to meet specific, more stringent cybersecurity standards to bid on Department of Defense contracts. This has made cybersecurity hygiene and CMMC compliance more important than ever for businesses in the sector, as non-compliance can result in lost revenue and reputational damage.

At the recent EMS Leadership Summit, held during IPC APEX EXPO 2023 in January, summit organizers arranged a panel discussion with three industry experts. The panel, moderated by Maribel Hernandez, followed a question and answer format. Panelists included Joaquin Hernandez, Allen Anderson, Vijay Takanti. They discussed the details and intricacies of CMMC compliance, and how it can affect a business. The experts shared their insights into the challenges that businesses in the sector are likely to face, the specific requirements tied to CMMC compliance, and the steps that businesses can take to ensure that they are adequately protected and able to achieve compliance within the framework. This article, compiled by the participants, summarizes portions of the discussion from the summit event.

What's the difference between cybersecurity and CMMC compliance?

Joaquin Hernandez: Cybersecurity is the practice of protecting computer systems, networks, and data from unauthorized

asc-i.com

WE ARE READY TO BRING YOU THE FUTURE

Our new Ultra HDI technology allows us to produce PCBs with parameters never seen before in our industry. With lines down to 1 mil with a line aspect ratio of 1:1 at production volumes, the future is here!

Check out our UHDI capabilities

American Standard Circuits

Creative Innovations In Flex, Digital & Microwave Circuits

access, theft, and damage. It's a broad concept that encompasses many different tactics, techniques, and procedures. The CMMC compliance, on the other hand, refers to the requirements set forth by the DoD to ensure that contractors are meeting a minimum level of cybersecurity readiness before being awarded contracts.


Joaquin Hernandez

In other words, cybersecurity is the foundation upon which compliance is built. A company must have a solid cybersecurity posture that extends to cover compliance safeguards in order to achieve compliance. While CMMC compliance is a specific set of requirements that a company must meet to do business with the DoD, cybersecurity is a broader and ongoing practice that should be applied to all aspects of a company's operations to protect against cyber threats.

What are the current DoD cybersecurity requirements?

Allen Anderson: Effective Dec. 31, 2017, the Defense Federal Acquisition Regulation Supplement (DFARS), and specifically DFARS clause 252.204-7012, mandates security controls defined in National Institute of Standards and Technology Special Publication 800-171 (NIST 800-171) be followed by all defense contractors, relying on the contractor's self-attestation of compliance through DFARS clause 252.204-7019 and the Supplier Performance Risk System or SPRS.

NIST 800-171 recommends certain cybersecurity standards. It consists of 110 controls to protect unclassified, but sensitive, information, and to govern timely reporting of cyber incidents.

CMMC—or DFARS clause 252.204-7021—will move the level of proof of compliance from mere self-attestation to third-party audit and verification. In short, CMMC is designed to ensure defense contractors are acting as they have been attesting with respect to the NIST 800-171 controls.

What is CMMC?

Vijay Takanti: The DoD created CMMC in response to the ongoing compromise of sensitive unclassified information that threatens our national security. The existing security requirements imposed on members of the Defense Industrial Base (DIB), those companies that directly or indirectly serve the DoD, have proven ineffective.

While CMMC remains a work in progress ahead of its official implementation, the current version of the framework, CMMC 2.0, consists of three Maturity Levels. Maturity Level 1 comprises 17 requirements, known as practices, designed to protect Federal Contract Information (FCI). Maturity Level 2 contains 110 practices, including the 17 from Level 1, which will protect Controlled Unclassified Information (CUI). These 110 practices directly align with the 110 controls defined in NIST 800-171, the standard to which companies that handle, process, or store CUI are held today. Maturity Level 3 has not yet been fully defined because it will apply only to a small number of contracts and contractors, but it will encompass the 110 practices of Level 2 and additional practices drawn from other standards like NIST 800-172.

There's an important difference between CMMC and its predecessors. In the current environment, companies can self-attest their compliance with NIST 800-171. Most companies seeking CMMC Maturity Level 2 accreditation, and all pursuing Maturity Level 3, will have to pass an assessment conducted by a CMMC Third Party Assessment Organization (C3PAO) or the Defense Contract Management Agency's (DCMA) Defense Industrial Base

Cybersecurity Assessment Center (DIBCAC).


Vijay Takanti

Who must comply with CMMC?

Hernandez: Any company that wants to do business with the DoD must comply with the CMMC requirements. This includes both prime contractors and subcontractors at all tiers of the supply chain.

The CMMC requirements apply to all DoD contracts, including those for goods and services. It's important to note that compliance is mandatory and that companies must undergo a CMMC assessment to verify their compliance level before being awarded a contract. The CMMC framework is designed to ensure that contractors are meeting a minimum level of cybersecurity readiness, so it's crucial for companies to take these requirements seriously and invest in cybersecurity measures to protect themselves and their clients.

When will CMMC come into effect?

Anderson: Frankly, the CMMC rollout continues to be a moving target, and, in fact, it now appears there may be further delays in CMMC 2.0 reaching final ruling as the Pentagon considers additional revisions to the proposed rule. As might be expected, much of the delay can be attributed to internal politics and concerns related to business impact. Notwithstanding these delays, which could push the CMMC rollout into 2024, it is important to remember that the underlying NIST 800-171 requirements—excepting the third-party audit requirements—have been in place for defense contractors since Dec. 31, 2017, and those remain.

What happens if a company fails to comply?

Takanti: In the near future, as existing DoD contracts come up for renewal and the DoD seeks partners for new programs, solicitations will include DFARS clause 252.204-7021, which links to CMMC. Solicitations also will include the Maturity Level accreditation which must be possessed by the prime contractor and subcontractors at all tiers.

Failure to possess the proper CMMC Maturity Level accreditation affects all members of the DIB. Prime contractors lacking accreditation may be unable to bid, costing them anticipated renewal revenue or new business opportunities. Subcontractors at any tier will face being left off the bid team by the prime contractor and replaced by one of their competitors.

DIB companies that received CMMC Maturity Level 1 or 2 accreditation as the result of a self-assessment may be subject to audit by DIBCAC. Consequences for an inaccurate assessment can be steep, possibly including termination of contract, corporate prosecution under the False Claims Act, and personal liability for executives who must sign a document verifying the accuracy of the self-assessment.

How long will it take a business to prepare for CMMC compliance?

Hernandez: The time it takes to prepare a business for CMMC compliance will depend on several factors, including the company's current level of cybersecurity readiness, the size and complexity of its IT infrastructure, and the level of CMMC certification it is seeking.

Each of the three CMMC Maturity Levels comes with its own set of requirements, and the higher the level, the more rigorous the requirements. For a small business with a basic IT infrastructure, achieving a Maturity Level 1 certification may only take a few months, while a larger enterprise with more complex systems

and processes may take years to achieve a Maturity Level 2 or 3 certification.

It's important for businesses to conduct a thorough self-assessment to identify any gaps in their cybersecurity measures and work with experienced cybersecurity professionals to develop and implement a plan to achieve compliance.

Allen Anderson

How much will the certification cost businesses?

Takanti: Companies should plan on substantial costs to acquire their CMMC accreditations. Several factors serve as cost drivers.

First, regardless of the Maturity Level they pursue, members of the DIB should perform a self-assessment against the relevant CMMC practices. The self-assessment will either be sufficient for accreditation or help prepare for a third-party assessment. Many organizations, particularly small- and medium-sized businesses (SMBs), lack the expertise, resources, and time to conduct an assessment properly. Instead, they must rely on outside consultants or tools, and each comes with a price tag.

Second, audits already conducted by DIBCAC have shown that most companies, even large enterprises, find themselves much further from meeting the relevant requirements than they think. Achieving the necessary full compliance takes significant remediation and implementation activities, which means incurring overhead costs and possibly capital expenditures.

Finally, most organizations at Maturity Level 2, and all at Maturity Level 3, will need to be assessed by an approved outside party to receive their accreditation. The size of the organization and the depth and breadth of CUI throughout its infrastructure impact the scope of a C3PAO's audit, which can span days or weeks and thus become expensive.

Add it all up, and the numbers can become quite large. Expect a minimum of five figures, and perhaps six, of hard and soft costs to successfully acquire CMMC accreditation.

What if my company doesn't contract directly with the DoD, or even with a prime contractor? Does CMMC still apply?

Anderson: While CMMC may not directly apply to a sub-contractor or supplier not contracting with the DoD or even a prime contractor, it will eventually be the cost of doing business in the defense sector and reach the subcontractor or supplier through mandated contractual flowdowns.

Moreover, one can absolutely expect similar or identical requirements for those in the government contracting chain, as similar standards are now being mandated by GSA, NASA, and other civilian agencies.

Where can a business find the resources to get started?

Takanti: CMMC can be daunting, in terms of compliance and cost. Fortunately, members of the DIB have access to a variety of resources to help on both fronts.

The DoD Office of Small Business Programs initiated Project Spectrum to provide companies with a comprehensive platform that includes the tools and training needed to increase cybersecurity awareness and maintain compliance in accordance with DoD contracting requirements. The federal Small Business Administration, along with locally based Manufacturing Extension Partnerships and Procurement Technical Assistance Centers, offer training, counseling, and even grants to improve cybersecurity readiness and maturity in preparation for CMMC and similar mandates.

Easy-to-use, cost-effective tools also exist that do everything from explaining the CMMC practices in plain English and guiding the self-assessment process and progress to creating the policies, plans, and other documentation necessary for accreditation. Look to managed service providers (MSPs) and managed security service providers (MSSPs) as partners with proven capabilities who can efficiently offload much of the compliance burden by reducing the assessment footprint and thus the overall time and cost to CMMC accreditation.

How can a business reduce its burden?

Hernandez: There are several steps a business can take. One important step is to conduct a thorough self-assessment to identify any gaps in its cybersecurity measures, develop a plan to address them, and prioritize its efforts and resources effectively.

Another important step is to work with experienced cybersecurity professionals who can provide guidance on the CMMC requirements and help the business develop and implement a compliance plan. This otherwise might be difficult for SMBs with limited IT staff.

MSSPs possess the knowledge, tools, and credentials to assist with CMMC compliance. They can provide cost-effective solutions and services by leveraging their existing technical controls and expertise.

By outsourcing the self-assessment and preparation to an MSSP, businesses can access the experienced resources needed to achieve compliance without having to invest in building their own cybersecurity programs with dedicated cybersecurity staff. The MSSP will pre-assess the level of compliance, identify the gaps, and help implement the required controls in preparation for the actual assessment.

It's important to remember that CMMC compliance is not a one-time thing but rather continuous maintenance of the certified status, which can be delegated to the MSSP. Businesses need to continually monitor their cybersecurity posture, conduct regular security assessments, and update their security controls to ensure ongoing compliance with the CMMC framework. **SMT007**

Allen Anderson represents local, national, and international businesses, as well as public and governmental entities, on a variety of legal matters, ranging from drafting and negotiation of both commercial and governments contracts; to formation of entity-wide compliance programs in response to an ever-changing political landscape; to disputes arising in both state and federal courts and before various arbitration or governmental panels. Allen is part of F&B Law Firm, P.C., a global practice, providing focused and timely legal advice on issues affecting a spectrum of industries including electronics manufacturing service providers.

Joaquin Hernandez is an electronics and telecommunications engineer with over 15 years of experience helping small- and mid-sized businesses as an information security professional. Currently a cybersecurity and CMMC consultant, Joaquin is the founder and president of Empowered IT Solutions, a security service provider serving companies in the United States and México, offering innovative IT technologies and cutting-edge cybersecurity solutions to implement, maintain, and comply with mandated CMMC and NIST requirements.

Vijay Takanti is SVP of Innovation and Informatics at Exostar, a provider of secure, cloud-based, compliant B2B collaboration capabilities and communities for highly regulated industries worldwide. He is responsible for the strategy and product roadmap, design, development, and customer delivery of The Exostar Platform. Takanti has more than 35 years of experience in electronic data processing, application design and development, and information security solutions for government and commercial customers globally. He facilitates the development of industry best practices and standards by bringing together CISOs and CSCOs from leading companies to focus on improving supply chain cybersecurity and risk management.