COSMOS
Navigate the Compliance Universe

CEP Magazine - May 2024

**Janet Himmelreich** (janet.himmelreich@3comply.com, linkedin.com/in/janethimmelreichgrcexpert/) is a Managing Director of 3Comply LLC in King of Prussia, Pennsylvania, USA.

# What's all the fuss about CMMC?

By Janet Himmelreich, CIPP/E/US, CMMC RA, RPA, formerly CCEP

If you are a compliance professional for a company with federal contracts, you've likely heard the term "CMMC," or Cybersecurity Maturity Model Certification.[1] It is one of those terms that seems to trigger almost immediate high anxiety with executives and IT leaders no matter the organization's size. It does not have to be this way. Understanding what it is, what it means to your organization, and what you can do about it is essential to protecting the company—now and well into the future. It is not just a "thing to fuss about"; it is essential business practice today.

## CMMC is not new

Primarily associated with the U.S. Department of Defense (DoD), CMMC has been discussed as a requirement for almost every contractor to the DoD, at least since the National Institute of Standards and Technology (NIST) SP 800-171 became a requirement in December 2017. The NIST special publication (SP) is now on its second revision (NIST SP 800-171 Rev. 2).[2] CMMC is simply a validation that provides an independent confirmation that the controls are implemented correctly and operating as intended and the required outcome can be evidenced. Other federal government agencies are planning to adopt the same or similar requirements as well. While originally designed as a maturation model, today's iteration of CMMC is now 2.11 and focuses on the status of implementation of the controls. It is important to recognize that validating the controls put in place is specifically designed to protect controlled unclassified information (CUI). Thus, if you are in the supply chain for the DoD, even if you do something as seemingly minor as manufacturing a special screw or something similarly small, the DoD requires that your company have appropriate controls in place to protect DoD CUI. Rapidly reporting cybersecurity incidents is another key mandate. These requirements stem from the Defense Federal Acquisition Regulations Supplement procurement clause 252.204-7012.[3]

Regrettably, many members of the Defense Industrial Base (DIB) have not even attempted to figure out how the controls prescribed in NIST SP 800-171 Rev. 2—the controls that CMMC must validate—apply to their business. This is unfortunate because if that procurement clause has been in your contract—perhaps directly or as a flow down from the contractor you deal with—you have technically been responsible for implementing the 110 controls of NIST SP 800-171 Rev. 2 since December 2017. There is not only substantial risk of breach of contract but also of having submitted false claims to the federal government.

As a fundamental starting point, the most vital thing for any company is to establish whether your organization operates within the federal government supply chain. (Hint: Make double sure you know that answer.) There could be that sneaky contract that is flying under the radar for the DoD or a member of its supply chain, and it is a major concern for cybersecurity compliance. As noted, CMMC currently only applies to the DoD. However, many

executive branch agencies have now established their own cybersecurity frameworks. For example, if your company is publicly traded, you must ensure you meet Securities and Exchange Commission cyber reporting requirements already going into effect. The Departments of Homeland Security and Energy also established their own requirements.

Even as a private company that does not have a DoD contract, the controls required under CMMC are the basic ones that every company should have in place. This is not "special" anymore; it is fundamental. The vulnerabilities and threats that are being controlled and protecting the company from cyberattacks may also reside with your outsourced providers, such as managed service providers, managed security service providers—known as external service providers (ESPs) under CMMC—and software-as a-service providers, commonly known as SaaS. These ESPs are in a company's supply chain. If a CMMC requirement has flowed through a contract to you, then you must flow it to your supply chain members, including ESPs.