Department of Defense Acquisition Delays Should Not Be Interpreted as CMMC Delay

By Melissa K. Ventrone, Jeffrey R. Wells / Apr 28, 2020

The Department of Defense (DoD) recently announced an expected delay of 90 days in many of its major acquisition programs. The COVID-19 pandemic is just beginning to demonstrate its effect upon, and test the resiliency of, the defense industrial base, its employees, suppliers, contractors, and the National Security of the United States. The ripple effect will influence many aspects of the Pentagon's acquisition and sustainment efforts going forward as businesses adjust to the impact of shelter in place and remote working guidelines, address supply chain issues, and wide-ranging health and enterprise-wide safety concerns. However, the impact and anticipated interruptions should not be interpreted as a delay in the implementation of the DoD's Cybersecurity Maturity Model Certification ("CMMC") requirement. The CMMC is the new security standard that will be applied to all contractors regardless of the types of products and services provided in the defense supply chain and goes into effect on July 1, 2020. While current contracts will not be impacted and companies should continue to maintain compliance with existing contract requirements and regulations, future contracts will require compliance with CMMC.

On April 24, 2020, the Chief Information Security Officer for the DoD acquisition office announced that DoD is considering a requirement that downstream suppliers to prime contractors also will need to meet the requirements. This arises as DoD reexamines its' supply chains and dependence on foreign suppliers, in response to the current pandemic.

The CMMC is an attempt to unify cybersecurity industry best practices to include all government contractors no matter the size of operations. This effort is vital to national security interests, especially as the nation addresses the short- and long-term impacts of the current dynamically changing environment. The scope and scale of increasing cybersecurity attacks on government and industry, especially by nation-states and their proxies, underscores the importance of the program and applies a heightened sense of urgency. While the DoD has strong defenses in place, attacks are now targeted at entities and individuals further down the supply chain which could have negative effects on DoD.

Existing government efforts to encourage parties in their supply chains to improve their overall cybersecurity posture, and the self-certification requirements in their contracts, have not produced the desired outcomes. Going forward, as of July 1, 2020, any entity wishing to work with DoD, regardless of size, service, or product, will be required to certify that they meet the appropriate level of cybersecurity technology and processes according to the CMMC, in order to respond to any Request for Proposals ("RFPs"). All defense contractors will be subject to the CMMC, third-party auditors will certify compliance, the certification will be verified, and no self-certification will be allowed. A searchable database will contain a record of completion by the assessed entity, and their level of certification is to be verified for each prime contractor and subcontractor. Contractors who are not certified at given or specified levels for defense contracts will not be allowed to participate in the market, so contractors must act now to prepare for and assess their readiness for the CMMC.

The CMMC measures compliance through five (5) defined levels that incorporate domains, which are broken down into cyber and compliance capabilities and achieved through specific practices and processes. At each level, the CMMC includes maturity processes for each domain, indicating the extent of institutionalization of the practices within an entity. The DoD is still finalizing the requirements to become a CMMC third-party assessment organization or individual assessor that is to be approved by the CMMC accreditation body. In the meantime, any entity anticipating business with the DoD after June 2020 should not delay in assessing their readiness for certification using the current Defense Federal Acquisition Regulation Supplement regulations and NIST 800-171 guidance. Furthermore, they should include the impact of the CMMC in their strategic planning, budgeting, operations, and partnering policies, as well as any business continuity procedures for adapting to a COVID-19 impacted future.

As we adjust to the "New Now," July might appear to be a long way away but meeting these requirements in some cases may be a time-consuming process. Companies should be looking beyond the current crisis and taking steps to ensure they are ready to meet the new requirements.

