TOP CONTRACTOR QUESTIONS EMERGING FROM THE U.S. DEPARTMENT OF DEFENSE CYBERSECURITY MATURITY MODEL CERTIFICATION

BDO

The U.S. Department of Defense (DOD) has recently announced the creation of a new Cybersecurity Maturity Model Certification (CMMC) program. The DOD has stated the new CMMC program will provide a cybersecurity framework for enforcement of their Defense Federal Acquisition Regulation Supplement (DFARS) requirements to protect controlled unclassified information (CUI). The current DFARS requirements for cybersecurity invokes the National Institute of Standards and Technology (NIST) Special Procedure (SP) 800-171, which contains 110 information security control requirements. The DFARS requirements for cybersecurity was officially implemented effective December 31, 2017.

However, during the past 18 months the DOD contractor self-assessment approach to compliance with NIST SP-800-171 has not achieved the desired level of enhanced information security for sensitive unclassified information. Clearly, DOD has recognized the need to implement a formal cybersecurity audit program to ensure adequate information security measures are being implemented by defense contractors.

A STEP IN THE RIGHT DIRECTION

The new DOD CMMC program is still in the development phase and is widely expected to be patterned after the well-established Carnegie Mellon University Software Engineering Institute (CMU/SEI) Capability Maturity Model Integration for software development. The new DOD CMMC is anticipated to be a five-level Cybersecurity Maturity Model, using the new revised version of NIST SP-800-171, released on June 19, 2019, as the information security control requirements.

Further, the DOD has announced their plans to require all defense contractors to become complaint with the CMMC program, via passing a formal CMMC audit, which DOD plans to contractually require on all new contracts effective as of June 2020. According to a DOD spokesperson, outside/private sector information security auditors will be used to perform the CMMC audits starting in late 2020 or 2021.

In addition, DOD plans to use a non-profit organization to oversee the new CMMC program and accredit the outside/private sector information security auditors. Presently, DOD is working with both The John Hopkins University Applied Physics Laboratory and CMU/SEI to support the planning of this new program.

TOP TEN CONTRACTOR QUESTIONS

Based upon our recent discussions with government contractors, there are numerous industry concerns about the DOD's new Cybersecurity Maturity Model Certification (CMMC) program, including the following frequently asked questions:

When will the DOD CMMC program be initially completed and available for industry review/comments?

When will the non-profit organization responsible for managing the outside/private sector information security auditors be selected and begin accrediting the auditors?

Will the DOD CMMC auditors only evaluate information security plans and policies?

Will the DOD CMMC require a defense contractor to have a Chief Information Security Officer (CISO)?

Will the DOD CMMC outside/private sector auditors be certified/accredited on an individual basis, company/firm basis, or both, and how much will all of this accreditation cost?

Is it the intent of the DOD CMMC to require defense contractors to have periodic Vulnerability Assessments and Penetration Testing conducted by independent firms?

Will the new DOD CMMC require defense contractors to conduct, either internally or via Managed Security Service Providers (MSSPs), 24 X 7 X 365 information security monitoring, detection, and incident response?

Is it expected that the DOD CMMC will require defense contractors to develop and periodically test their contractor cyber data breach Incident Response (IR) plan, Disaster Recovery (DR) plan, and/or Business Continuity Plan (BCP)?

How much will it cost a company to have an outside/private sector firm conduct a CMMC audit?

After a defense contractor passes the initial DOD CMMC audit, will there be an annual or bi-annual compliance review requirement?

SUMMARY

Cybersecurity is a critical risk factor for all organizations, especially for U.S. defense contractors tasked with protecting sensitive unclassified information. For over a decade, the U.S. Department of Defense has struggled with how best to ensure defense contractors effectively implement cybersecurity in order to protect our national security interests. It appears the new program is a positive step in implementing enhanced contractor information security. The new DOD CMMC will be contractually enacted by the DFARS to ensure contractors compliance with the revised NIST SP-800-171 security controls, with a real enforcement mechanism via the use of outside/private sector information security auditors. Of course, the devil is always in the details, and there are a lot of important questions and details to be addressed. The clock is ticking on the new DOD CMMC program. The number and level of cyber-attacks are continuously increasing, and the risk of the loss of valuable intellectual property and national security information is both real and significant to our country.

CONTACT

GREGORY GARRETT
U.S. & International Head of
Cybersecurity Advisory Services
703-770-1019
ggarrett@bdo.com

ED AMOROSSO
Office Managing Partner, Government
Contracting Industry National Co-Leader
757-640-7295
eamorosso@bdo.com

AARON RADDOCK
Managing Director, Government
Contracting Industry National Co-Leader
703-336-1693
araddock@bdo.com