DHG | views

September 2019

Department of Defense Contractors to Begin Preparing for New Cybersecurity Certification Requirement

Tom Tollerton, CISSP, CISA, QSA | Managing Director, DHG IT Advisory

Alex Imani | Associate, DHG IT Advisory

As cyberattacks against Department of Defense (DoD) contractors continue to threaten national security, the DoD is increasing oversight and enforcement of data security requirements within its supply chain. Katie Arrington, Special Assistant to the Assistant Secretary of Defense for Acquisition for Cyber, has announced a new cybersecurity maturity framework and certification process that will debut next year, building upon existing Defense Federal Acquisition Regulation (DFARS 252.204-7012) for protecting Controlled Unclassified Information (CUI). The announcement affects more than 300,000 companies comprising the Defense Industrial Base (DIB).

The Framework

The *Cybersecurity Maturity Model Certification (CMMC)* – will combine existing security frameworks, including National Institute of Standards and Technology (NIST) Special Publication 800-171 for protecting CUI, and will establish multiple cybersecurity maturity levels to enhance and unify protections around CUI. The DoD is expected to publish a final version of the CMMC framework in January 2020, and contractors should expect to see the certification requirements included as part of Requests for Information starting in June 2020. Arrington has announced that contractors will need to work with the DoD contracting officer next year to determine the level of certification required for their organization before responding to Requests for Proposals starting in September 2020.

The CMMC will be used as a unified standard for defense contractors to demonstrate cybersecurity program maturity and protection of CUI. The DoD acknowledges that contractors of varying sizes struggle to maintain an appropriate cybersecurity posture and believes this new framework will help contractors implement effective cybersecurity controls tailored to the size and nature of their business and meet the DoD's requirements.

Key elements of the framework include:

- **Maturity Model:** The CMMC will define five maturity "tiers" to distinguish maturity of cybersecurity controls. The DoD will determine the appropriate tier, based upon the nature of the contract, and will note specific CMMC requirements in sections L & M of Request for Proposals.
- **Certification:** All DoD primes and subs will be required to determine their required maturity and certification level and undergo a certification assessment performed by a third party. The nature of data required by each contract will determine the level of maturity required for certification. Self-assessments and self-certifications will not be permitted.
- **Allowable Cost:** The DoD has indicated that the cost of certification and security implementation may be an allowable cost for contractors.
- **Enforcement:** Once certification is referenced in Requests for Proposals, contractors will need to be certified in order to win a contract. The decision will be based without exception upon a contractor's achieved certification level. Development of the CMMC is a clear signal that protection of sensitive information through the supply chain remains a top priority for the DoD.

DHG's Government Contracting and IT Advisory teams provide security assessments and NIST 800-171 compliance advisory services to contractors and will advise clients as the CMMC and its specific requirements become more defined over the next several months.

DHG Contacts

Tom Tollerton, CISSP, CISA, QSA
Managing Director, DHG IT Advisory

Alex Imani
Associate, DHG IT Advisory

itadvisory@dhg.com

About DHG IT Advisory

DHG IT Advisory works with companies to manage technology risk while maintaining data integrity, protecting privacy and complying with regulations. From project management and regulatory compliance assistance to digital forensics and incident response, DHG is equipped to meet your IT advisory needs that drive your business. To learn more about DHG's IT Advisory services, visit **dhg.com/itadvisory**.

About DHG Government Contracting

DHG Government Contracting provides assurance, tax and advisory services to government contractors working with every area of civilian agencies, Department of Defense and intelligence agencies. We help strengthen compliance with applicable FAR and CAS requirements and enable companies to meet the expectations of oversight agencies such as SBA, DCMA and DCAA. To learn more about DHG's Government Contracting Practice, visit **dhg.com/industries/government-contracting**.