Update on the Cybersecurity Maturity Model Certification (CMMC) Initiative

Update provided by Professional Services Council Cybersecurity Policy Working Group

Overview

- The U.S. Department of Defense (DOD) has recently announced the creation of a new Cybersecurity Maturity Model Certification (CMMC) program
- The idea behind this new initiative is to provide a single unified standard under control by a neutral third party that all DoD Contractors will be required to meet in order to submit proposals for future new business
- The CMMC framework arose in response to a series of high profile breaches of DoD information. This caused DoD to reevaluate its reliance on security controls in National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-171
- Presenting the overall goals and design of this new program is Katie Arrington, Special Assistant to the Assistant Secretary of Defense for Acquisition for Cyber, Office of the Under Secretary of Acquisition and Sustainment

Contract Security Level Assessment

- The CMMC will have maturity levels, currently proposed as 1 - 5 that range from "Basic Cybersecurity Hygiene" to "Advanced", with CMMC Level 1 being the easiest to obtain.
- Availability of the Scoring Methodology: The scoring methodology should be available for public comment soon.
- Receiving Updates and Feedback: Government provides continual updates and Q&A through process. When complete there will be a preliminary assessment score provided, followed by a formal assessment report that may provide POAM follow up items.
- The intent is to identify the required CMMC level in RFP sections L and M and use as a "go /no go decision."
- Based on the NIST 800-171 controls, the FAR 32 CFR Part 2002, CMMI, and ISO9001
- To be included in RFPs (June 2020) and new Solicitations (Late 2020)
- All DoD Contractors will be required to pass an assessment/audit to officially obtain their required CMMC Level acknowledgement. There will be no self-assessments allowed
- Authorizes a non-profit organization to oversee the program and accredit private-sector auditors

Rules for Small DIB Contractors

- Security levels will flow down to subs.
- 70% of companies DCMA deals with have less than 100 employees, and limited IT resources available
- Provisions may be made for smaller contractors with no deep IT/CIO/Technology competence that provide critical product or services

Assessment Costs

- The DoD has announced that the costs to prepare for CMMC certification will be considered an "allowable cost." Allowable costs are expenses specified in a contract that can be billed to the DoD.
- Katie Arrington, at a recent acquisition conference sponsored by the Professional Services Council in Arlington, Virginia."I need you all now to get out your pens and you better write this down and tell your teams: Hear it from Katie Arrington, who got permission to say it from Mr. [Kevin] Fahey [the assistant secretary of Defense for Acquisition in the Office of the Under Secretary of Acquisition and Sustainment]: 'security is an allowable cost. Amen. Right?"
- This should be considered great news for government contractors, many of whom have struggled to navigate the hurdles of complying with DoD cybersecurity mandates over the last few years

Yet to be Determined

- What about contracts already awarded? Can the contracts office request it?
- Commercial companies: Discussion on commercial item pricing, impacts on higher levels, do these costs open up audits?
- NIST 800-171-B: Not finalized, still in draft. 800-171-B build on 800-171, and may include some of the elements of level 4 and 5 cyber requirements. Where 800-171 is a general requirement; 800-171B is intended to eventually be a direct requirement specified on a contract-by-contract or program basis.

JAMIS will continue to keep you posted as updates come in. The next PSC Cybersecurity Policy Working Group meeting with occur this December 2019.

JAMIS®
www.jamis.com

1-800-65-JAMIS (655-2647) email **info@JAMIS.com**
or visit us on the web at **www.JAMIS.com**