NORTHROP
GRUMMAN

Northrop Grumman Corporation
2980 Fairview Park Drive
Falls Church, VA 22042-4511

northropgrumman.com

April 10, 2020

To: Our Supply Chain Partners

Subject: Cybersecurity Maturity Model Certification (CMMC) Update: Are You Making Progress?

The U.S. Department of Defense (DoD) continues to make significant progress in its CMMC initiative so Northrop Grumman (NG) wants to provide updated information as your company continues to prepare your implementation strategy. As noted in our CMMC communication, dated December 16, 2019, it is critical that you become familiar with the CMMC model and start taking steps now to achieve the CMMC maturity level needed to support your business.

As planned, DoD introduced CMMC Model v1.0 at the end of January 2020 and in mid-March issued an updated CMMC Model v1.02 with some administrative changes. The five (5) CMMC maturity levels range from “Basic Cyber Hygiene (Level 1) to “Advanced/Progressive” (Level 5).

The CMMC model defines practices (i.e., requirements) that must be accomplished to achieve identified cybersecurity capabilities at specified maturity levels. The model spells out what you will need to implement at the different maturity levels. Of particular note, DoD indicates that if your company internal information systems contain Controlled Unclassified Information (CUI) , those systems will need to be Level 3 certified, at a minimum, which includes all 110 NIST 800-171 controls and 20 additional requirements. Importantly, DoD has indicated that all CMMC requirements must be implemented prior to award; no Plans of Actions and Milestones (POAMs) will be allowed. You can find out more about CMMC on the DoD CMMC website.

DoD intends to incrementally implement CMMC over the next 5 years and begin including CMMC requirements in solicitations issued in the fall of 2020. In addition, DoD has indicated it will identify 10 Pathfinder acquisitions for CMMC implementation this year. As noted above, if a company’s systems have not been assessed to meet the required level of cybersecurity maturity for a solicitation, the company will not be eligible for award. Please review the transcript from a DoD CMMC model Press Briefing to learn more about the CMMC implementation approach.

DoD also just reached agreement on a Memorandum of Understanding with the CMMC Accreditation Body (CMMC-AB). The CMMC- AB is a newly established non-profit that, among other CMMC undertakings, will select, train and certify the third party CMMC assessors. While the CMMC-AB has not selected any third party assessors at this time, certain companies are fraudulently trying to convince Suppliers that they can provide CMMC assessment services now. Please visit the CMMC-AB website for more information.

Furthermore on March 6, 2020, DoD issued DoDI 5200.48, a new instruction on CUI. While DoD will likely continue to refine this CUI instruction as cyber initiatives continue to evolve, the document provides insights with respect to DoD's current instructions regarding identifying, marking and processing CUI and delineates the internal DoD CUI-related responsibilities.

To assist suppliers in preparing for CMMC requirements, the Defense Industrial Base (DIB) Sector Coordinating Council (DIB SCC) launched a new CyberAssist website providing resources and other helpful information to aid DIB suppliers in achieving enhanced cyber maturity. The site is intended to facilitate the timely sharing of key cyber information, including information about threats, best practices, and initiatives.

NG continues to strongly encourage its Suppliers to take steps now to ensure the necessary processes and cybersecurity measures are in place to obtain third party CMMC assessment to support DoD business. Again it is recommended that you consider:

(i) verifying closed out, or tracking to timely completion of any outstanding items in your NIST 800-171 POAMs that will need to be fully implemented prior to your CMMC assessment at the level needed to support your business; and

(ii) review any new CMMC cyber requirements at that CMMC maturity level, identify any gaps, and begin implementation efforts now.

Lastly, continue to follow future key CMMC developments by regularly checking the above websites.