CISQ Cyber Resilience Summit

Supporting Industry; Achieving Cybersecurity Maturity Model Certification

Dr. Phyllis Schneck
Vice President and Chief Information Security Officer
13 October 2020
Northrop Grumman and the Defense Industrial Base (DIB) have partnered closely with the government to support CMMC development.

Founding member of DIB Sector Coordinating Council (SCC) Supply Chain Cyber Task Force

Task Force working group dedicated to CMMC

- Best practices from leading companies
- Ensuring all practices can be implemented in real-world environments
Benefits of Moving to the CMMC Standard

• Increased data confidence from assessment by a third party
• Roadmap (CMMC Levels) for companies striving to enhance cyber protections
• Improved security consistency, as the CMMC is a unifying standard containing best practices from several sources
• Continuous security improvement as CMMC maturity drives companies to keep enhancing their practices and adapting to the threat
• Reduced data management and reporting for suppliers
• Support for small suppliers
CMMC Resources

CyberAssist website
• Developed by DIB SCC Supply Chain Cyber Task Force
• CMMC Practice implementation guides, videos, example policies, applicable tools, lessons learned

https://ndisac.org/dibscc/cyberassist/

DoD CMMC Model website
• Official site, model PDF downloads, FAQ
https://www.acq.osd.mil/cmmc/

CMMC Accreditation Body website
• Assessment information
• Marketplace of authorized providers
https://www.cmmcab.org/marketplace
CyberAssist Demo

DIB SCC CyberAssist

Our Mission: Provide trusted resources to assist DIB companies and suppliers of varying sizes with the implementation of cyber protections, and awareness of cyber risk, regulations and accountability for their supply chain.

To assist suppliers in enhancing their cyber security protections, the DIB SCC Industry Task Force is identifying and posting links to helpful publicly available cybersecurity resources. The resources were selected both to help companies (i) meet DoD and other U.S. cybersecurity standards applicable to U.S. federal contractors (e.g., FAR Basic Safeguarding clause, DFARS Safeguarding Covered Defense Information (CDI) clause, DoD Cybersecurity Maturity Model Certification (CMMC)); and (ii) otherwise improve their current cybersecurity protections. We will continue to add links to other available resources over the coming months.
Data protection, or data confidentiality, is defined by NIST as protecting against the disclosure of information by ensuring that the data is limited to those authorized or by representing the data in such a way that its semantics remain accessible only to those who possess some critical information. The following provides resources for enterprise-wide data protection. (Source)
CMMC Success – Next Steps

Continue to prepare for CMMC assessments and support your suppliers

• Many CMMC practices take several months to implement correctly

Watch items / What’s next

• Availability of third-party assessors
• How to find out about completed supplier CMMC certifications
• Reciprocity if a company has already been certified to a different cyber standard
  – Defense Industrial Base Cybersecurity Assessment Capability - DIB CAC