CMMC Assessment: Preparing companies for their Cybersecurity Maturity Model Certification (CMMC)

What is CMMC compliance and why it was developed

The Department of Defence (DoD) has taken proactive measures in creating the Cybersecurity Maturity Model Certification (CMMC) to ensure basic cyber hygiene as well as to protect Controlled Unclassified Information (CUI) that resides on the DoD's industry partners' networks.

The CMMC will require companies bidding on defense contracts to meet a certain level of cybersecurity standards when responding to a Request for Proposal (RFP). The CMMC will be divided into five levels of certification in both cybersecurity practices and processes, that will be used to determine a company's cybersecurity readiness.

If you are a contractor or vendor planning to do business with the DoD, you will likely need to prepare to be audited by a certified third-party assessment organization (C3PAO) to attain your certification. AT&T can offer your company a CMMC readiness assessment and advice when it comes to preparing for your certification.

Potential benefits

- Holistic look to find the practice gaps and process maturity amongst people, process and technology and to posture against CMMC
- Extensive experience with industry standards and verticals in the DOD supply chain
- Strategic security advisors that can assess, remediate, and provide solutions to meet your desired CMMC level
- Drive faster, more efficient security response

CMMC levels and descriptions

Here is a brief description of each certification level:

- **Level 1 demonstrates "Basic Cyber Hygiene"** – DoD contractors who wish to pass an audit at this level must implement 17 controls of NIST 800 -171 rev1.
- **Level 2 demonstrates "Intermediate Cyber Hygiene"** – Here, DoD contractors must implement another 48 controls of NIST 800-171 rev1 plus seven new "other" controls.
- **Level 3 demonstrates "Good Cyber Hygiene"** – To achieve level 3 certification, the final 45 controls of NIST 800-171 Rev1 plus 13 new "other" controls must be implemented.
- **Level 4 demonstrates "Proactive" cybersecurity** – In addition to the controls in levels 1 through 3, 11 more controls of NIST 800-171 Rev2 plus 15 new "other" controls must be implemented.
- **Level 5 demonstrates "Advanced / Progressive" cybersecurity** – To achieve this highest level, DoD contractors must implement the final four controls in NIST 800800-171 Rev2 plus 11 new "other" controls.

Importance of picking a trusted registered provider organization

To achieve each certification level, contractors and vendors must meet the requirements for practices and processes associated with that level across 43 different capabilities spanning 17 capability domains. If you lack the in-house resources, outsourcing this cybersecurity work to a qualified provider can help save your organization time and money. The Cybersecurity Maturity Model Certification states that contractors can choose to "achieve a specific level for its entire enterprise network or for particular segments where the information to be protected is handled and stored." However, DoD solicitations will specify what maturity level the supplier needs to be at in order to respond to the request for proposal. Therefore, it is essential to conduct an assessment of the business and also determine what (or if) Controlled Unclassified Information (CUICUI) is part of the equation.

AT&T Cybersecurity has been providing security services and solutions in the DoD space for many years and we can provide your business with expertise and knowledge as you prepare to become CMMC certified. We will provide insights to gaps, risks, and solutions to help you work toward certification and get a head start on the competition.

If you are a contractor or vendor planning to do business with the DoD, it is imperative that you work with the right trusted advisor.

About AT&T Cybersecurity

AT&T Cybersecurity helps to reduce the complexity and cost of fighting cybercrime. Together, the power of the AT&T network, our SaaS-based solutions with advanced technologies including virtualization and actionable threat intelligence from AT&T Alien Labs and the Open Threat Exchange,™ and our relationship with more than 40 best-of-breed vendors, accelerate your response to cybersecurity threats. Our experienced consultants and SOC analysts help manage your network transformation to reduce cybersecurity risk and overcome the skills gap. Our mission is to be your trusted advisor on your journey to cybersecurity resiliency, making it safer for your business to innovate.