You might be ready for CMMC. Are your Sub-Contractors?

The Cybersecurity Maturity Model Certification (CMMC) is the Department of Defense (DoD) solution to stem the malicious cyber activity targeting the Defense Industrial Base (DIB). These malicious cyberattacks have been undercutting US technical advantages and innovations in defense and significantly increase risks to national security.

Prime contractors should be communicating with their sub-contractors about CMMC certifications. If you are a sub-contractor and have not discussed this with your prime contractor, now is the time to begin that conversation. The larger contractors working on highly sensitive material may need to be Maturity Level three to continue handling sensitive information.

CMMC 2.0 Maturity Level Descriptions

CMMC Level 1 (Foundational):

Processes Performed: Level 1 requires an organization to perform 17 specified practices and conduct annual self-assessments. Level 1 does not assess process maturity because the organization may only be able to perform these practices in an ad-hoc manner and may or may not rely on documentation.

Foundational Cyber Hygiene Practices: Foundational focuses on the protection of Federal Contract Information (FCI) and consists only of controls that correspond to the basic safeguarding requirements specified in 48 CFR 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems).

CMMC Level 2 (Advanced):

Processes Documented: Level 2 requires that an organization establish and document practices and policies to guide the implementation of their CMMC efforts. The documentation enables individuals to perform them in a repeatable manner. Organizations develop mature capabilities by documenting their processes and practicing them as written.

Advanced Cyber Hygiene Practices: Level 2 requires companies that process Controlled Unclassified Information (CUI) to meet the 110 practices aligned with the National Institute for Standards and Technology (NIST) Special Publication (SP) 800-171.

CMMC Level 3 (Expert):

Processes Managed: Level 3 requires an organization to establish, maintain, and resource a plan demonstrating the management of activities for practice implementation. The plan may include information on missions, goals, project plans, resourcing, required training, and involvement of relevant stakeholders.

Expert Cyber Hygiene Practices: Level 3 protects the highest priority programs with CUI and encompasses all the security requirements specified in NIST SP 800-171 and a subset of controls from NIST SP 800-172.

Defense contractors must determine where they and their sub-contractors are on the DoD's three-tier maturity level certification process and where they need to be to bid on DoD contracts. The intent is to

identify the required CMMC level in each RFP (sections L and M), and the maturity level to be used as a "go / no go decision" by the Contracting Officer.

The premise of CMMC is simple: The Department of Defense (DoD) will hold information security as foundational to acquisition — on par with cost, schedule, and performance — when awarding contracts. The new requirement builds upon existing Defense Federal Acquisition Regulation Supplement (DFARS) regulations by adding a verification factor to contractor cybersecurity controls and enhancing the protection of controlled unclassified information (CUI) within the supply chain.

All Defense contractors recognize that Cybersecurity is a business imperative. Prime contractors should be asking their sub-contractors the following:

- *Where do you stand regarding CMMC?*
- *Where do you need to be regarding CMMC?*
- *Do you anticipate being able to meet CMMC requirements?*
- *When will you be ready for Certification?*

If your Sub-Contractor has not completed a CMMC assessment, the time is now.

Prime contractors must determine where their sub-contractors fall on the DoD's CMMC Maturity Level and where they need to be included in proposals. Prime contractors and sub-contractors should have contingency plans if a contractor does not meet CMMC requirements or loses their CMMC certification.

Alluvionic's certified expert staff can help you achieve compliance with standards like the Cybersecurity Maturity Model Certification (CMMC), NIST Cybersecurity Framework (CSF), Risk Management Framework (RMF), ISO/IEC 27001, Health Insurance Portability and Accountability Act (HIPAA), and the EU General Data Protection Regulation (GDPR).

Alluvionic can analyze the current state of their CMMC cyber hygiene by applying our full-scope gap assessment scorecard.

Alluvionic utilizes collaborative tools to develop a comprehensive picture of organizational cybersecurity resiliency. Your starting point is the same, whether assessing your cybersecurity posture for the first time or as part of your routine operations. The need for actionable information drives risk-based decisions and an effective management program to address any critical deficiency.

CMMC persistence is not a matter of organizational compliance, it is a matter of organizational change, and Alluvionic® is a leader in organizational change management. Techniques rooted in an understanding of organizational behavior facilitate communication, learning, and adoption of Cybersecurity changes. Utilizing a proven, disciplined process and proven team management, our CMMC advisors will:

- Provide a complimentary workshop outlining the objectives of CMMC and how we will reach your desired certification level.
- Analyze the current state of your cyber hygiene by applying our full-scope gap assessment scorecard.
- Develop remediation roadmaps for the most relevant risks to your program.
- Customize efficient and effective cybersecurity improvement plans.

- Provide tactical risk granularity for your technical staff, comprehensive, actionable data for operational managers, and consistent strategic reporting to keep your C-Suite informed.
- Quickly mitigate your documentation gaps with pre-built policies & procedures, rapid change management application, and required service documentation.
- Cultivate growth toward a culture of cyber resilience.
- Instill confidence in your CMMC readiness at the board level.