CMMC CONTRACTOR COMPLIANCE CHECKLIST

SCA®
SECURITY COMPLIANCE ASSOCIATES

CMMC is the latest cybersecurity standard making a considerable impact on the DIB and our National security posture. Version one of CMMC was introduced as part of the DFARS Interim Rule that went into effect on November 30, 2020, specifically, DFARS clause 52.204-7021, Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement. Since then, revisions have been made, v1.2 was suspended in 2021, and CMMC v2.0 is now in the Rulemaking Phase to be entered into the C.F.R and DFARS.

A new Interim Rule may require compliance with CMMC v2.0 for new contracts as soon as May 2023, but it has yet to be confirmed as of this writing. In the meantime, the following is a brief checklist to begin your CMMC v2.0 journey:

1. Understand FCI and CUI

Federal Contract Information (FCI) is defined as information provided by or generated for the Government under a contract to develop or deliver a product or service for the US Government. Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls. There are similarities and a distinction. Learn more about CUI through the free online course here.

The CUI Registry provides a catalog of information types under the CUI program and can be accessed at CUI Categories | National Archives

2. Identify What System(s) Contain FCI or CUI

This is the step where your project (assessment) scope is defined. The Assessment scope defines which assets within your environment will be assessed and the assessment details. Assets include people, technology facilities, and external service providers that will process, store or transmit CUI.

3. Perform the Respective Assessment or Readiness Assessment

CMMC Level 1 provides for self-assessment and attestation to satisfy CMMC requirements annually. Levels 2 and 3 may prepare by assessing against NIST 800-171 and NIST 800-172 controls using the respective assessment methodology. Doing so is also part of satisfying DFARS clauses 252.204-7019 and 252.204-7020, the performance of a NIST 800-171 DoD Assessment.

Contractors requiring Level 2 certification must have a CMMC Level 2 assessment performed by a CMMC Third-Party Assessment Organization (C3PAO) every three years. The Level 2 Assessment Guide is now available and can be used as a guide for readiness before the certification assessment. The Level 3 Assessment Guide has not been released.

Registered Practitioner Organizations (RPOs) can provide assistance and consulting to help complete the NIST 800-171 DoD Assessment and/or CMMC Readiness Assessment.

4. Draft a System Security Plan (SSP)

The SSP describes how the security requirements are met or how you plan to meet the requirements and address known and anticipated threats. Per the NIST 800-171 DoD assessment methodology, the SSP is technically reviewed first, and the assessment is performed against the Plan.

5. Create a Plan of Action and Milestones (POA&M)

Your POA&M describes how unimplemented security requirements will be met and how any planned mitigations will be implemented.

6. Upload to Supplier Performance Risk System (SPRS)

The results of the above self-assessments should be uploaded to SPRS. This is very important for those suppliers who handle CUI and are likely to comply with Level 2. Current NIST 800-171 DoD Assessment requirements are in effect, and SPRS is used to aggregate supplier results. Contracting officers will also be referencing SPRS to determine supplier eligibility for projects.

7. Remediate and Monitor

Using your POA&M as your guide, take corrective action to implement needed controls. Update your POA&M as well as your SSP. Your goal is to complete remediation before engaging a C3PAO for the certification assessment.

Tackling CMMC can be daunting, as many organizations do not have adequate cybersecurity resources in place. Recognizing this, the CYBER-AB created the Registered Practitioner Organization (RPO) role. These companies have demonstrated expertise in cybersecurity and have been vetted by the CYBER-AB to provide consulting services to those organizations seeking certification (OSC). Security Compliance Associates is a CYBER-AB-recognized RPO with over 17 years of industry experience to help your organization conquer CMMC!

For more information on CMMC compliance to make sure your company meets the requirements to successfully bid on DoD contracts, please click here.