SYNC21

Protect Your Reputation . . . Secure Your Business!

We help DoD Contractors achieve CMMC 2.0 Certification to Win Contracts, and Protect the USA from our adversaries. As your virtual Chief Information Security Officer our Managed Compliance, Cybersecurity and IT services allow us to be in the watchtower over your business.

Always in the Watchtower.

We start every morning excited to be in the "watchtower" for our clients as they face the difficult world of cybersecurity and government compliance in their businesses.

Are you unsure how CMMC 2.0 is going to affect your business?

Are you concerned about losing contracts because you are not CMMC compliant? We understand how you feel. We have put together an affordable service based on Microsoft 365, Azure and Microsoft Security. With our CMMC 2.0 Compliance Services, you get a virtual Chief Information Security Officer to lead you toward success in your quest to keep your existing contracts and win more in the future.

Achieving CMMC Compliance Takes Time.
Please don't wait; Get Started Today!

CMMC 2.0 Will Be Here Sooner Than You May Think!

Understanding the current FAR and DFARS regulations and enforcement mechanisms, as well as what is coming very soon with CMMC 2.0 is critical for helping your business keep its existing DoD contracts and win more in the future!

Current Regulations

If you have Federal or Department of Defense (DoD) contracts now, then there are current Federal Acquisition Regulations related to Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) that you must adhere to by law.

FAR 52.204-21

✓ Defines Federal Contract Information (FCI)

✓ Defines (15) Safeguarding requirements and procedures

✓ Applies to all Federal contracts, not just DoD

✓ Includes Primes and Subcontractors (flows down)

✓ Mentions CUI, and will likely be expanded in the future

DFARS 252.204-7012

✓ Defines Controlled Unclassified Information (CUI)

✓ Seeks to protect both FCI and CUI

✓ Aimed at DoD contractors
   – FAR clause impacting Federal contracts with CUI is in the works

✓ Points to NIST 800-171 Self-Assessment

✓ Includes Primes and Subcontractors (flows down)

CMMC 2.0 Executive Briefing

Current Enforcement

Until CMMC rulemaking is complete, only the clauses above are in play, but they are enforced by the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC). **DIBCAC can audit you and find you in Breach of Contract through the False Claims Act if you are not adhering to the regulations. The following items are required for all DoD contracts containing the DFARS 252.201-7012 clause**:

✓ **NIST 800-171 Self-Assessment**

✓ **Enter Self-Assessment Score in SPRS**

✓ **System Security Plan (SSP)**

✓ **Plan of Action & Milestones (POA&M)**

✓ **Must report any data breach within 72 hours**

CMMC 2.0

CMMC 2.0 is all about future enforcement. All current regulations will still be in force after CMMC 2.0 is final. In early February 2024 the DoD's CIO released an update video, and stated that the objective timeline for implementing contractor compliance with CMMC 2.0 requirements has been, and remains, FY2025. Look for CMMC 2.0 to become finalized within Q1 2025, including immediate self-assessment requirements and certification requirements starting 6 months later.

You may not be awarded contracts if you are not ready to be CMMC compliant, and those that are ready may step in and win contracts instead of you. It is worth noting that DoD contracts without CUI are still considered to contain Federal Contract Information (FCI), which requires CMMC Level 1 certification...this is not a trivial set of requirements for contractors with little or no cybersecurity infrastructure.

✓ Certification required for contract award, including meeting all assessment objectives

✓ Level 1 for FCI – Self Assessment (Annually)
   – 17 Practices
   – 59 Assessment Objectives

✓ Level 2 for FCI/CUI – 3rd Party Assessment (Every 3 Years)
   – 110 Practices
   – 320 Assessment Objectives

Putting it ALL Together for You...

Now that you have some sense of the basics of the current FAR and DFARS regulations and enforcement mechanisms, let's take a quick look at what you can do now if you haven't already started.

I have Federal contract(s) what should my company do now?

1. Recognize you have FCI

2. Determine whether you have CUI or not

3. Perform a FAR 52.204-21 Gap Assessment

4. Remediate any gaps found in the Gap Assessment

5. If you have CUI, additional FAR clauses are coming requiring you to protect CUI

I have DoD contract(s) what should my company do now?

1. Recognize you have FCI

2. Determine whether you have CUI or not

3. Perform a CMMC 2.0 Gap Assessment

   a. If you do not have CUI, then commensurate with CMMC Level 1

   b. If you do have CUI, then commensurate with CMMC Level 2

4. Calculate Score & enter into Supplier Performance Risk System (SPRS)

5. Create & Maintain a System Security Plan (SSP)

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

7. Remediate any gaps found in the Gap Assessment

8. If you have CUI, then you will need to be ready for a 3rd party assessment

Remember that CMMC 2.0 Certification takes time, even at a Level 1, so getting started now is a good idea to keep your existing contracts in place and win new contracts in the future. We have already seen examples of DoD contractors being put on hold due to not implementing NIST 800-171.

Please don't wait; Get Started Today.

Our Service Offering

Sync21 can help!

We help DoD contractors achieve CMMC 2.0 compliance by providing gap analysis, remediation planning and implementation, and ongoing compliance monitoring.

CMMC 2.0 Compliance

- ✓ **Review of DFARS Contract Clauses**
- ✓ **FCI & CUI Scoping**
- ✓ **NIST 800-171 Gap Assessments & Remediation**
  - – Scoring for Supplier Performance Risk System (SPRS)
  - – System Security Plan (SSP)
  - – Plan of Action & Milestones (POA&M)
- ✓ **CMMC Gap Assessments & Remediation**
- ✓ **Ongoing CMMC Compliance Maintenance**

Cybersecurity Compliance

- ✓ **CMMC 2.0 Compliance**
- ✓ **HIPAA Compliance**
- ✓ **PCI DSS Compliance**
- ✓ **Risk Assessment & Remediation**
- ✓ **Cybersecurity Policies & Procedures**
- ✓ **Cybersecurity Insurance Consulting**
- ✓ **Apptega Continuous Compliance Platform – Shared Access**

Microsoft Cloud Solutions Provider (CSP)

- ✓ **365 Cloud Migration Services**
- ✓ **365 Configuration & Management**
  - – Entra ID
  - – Exchange Online, Rooms, SharePoint, Teams, Etc
  - – Azure Virtual Desktop
  - – Azure Virtual Machines

- ✓ **Microsoft Licensing**
  - – Microsoft 365 Government Community Cloud (GCC)
    - – Microsoft 365 GCC High
    - – Microsoft 365 GCC
  - – Microsoft 365 Enterprise
  - – Microsoft 365 Business

Managed Security Services Provider (MSSP)

- ✓ **Apptega Continuous Compliance Management**
- ✓ **Microsoft 365 & Azure Security**
  - – Microsoft Sentinel
  - – Microsoft Purview
  - – Desired State Configuration & Monitoring
- ✓ **Managed Security Operations Center (SOC)**

- ✓ **Email Security**
- ✓ **Endpoint Security**
- ✓ **DNS Protection**
- ✓ **Security Awareness Training**
- ✓ **Remote Worker Security**

Managed Services Provider (MSP)

- ✓ **Business Continuity & Disaster Recovery (BCDR)**
- ✓ **Remote Monitoring & Management (RMM)**
- ✓ **Hardware & Operating System Support**

- ✓ **Smart IT Documentation**
- ✓ **Professional Service Automation**

Apptega PARTNER | PREVEIL | Microsoft Cloud Solution Provider | paloalto NETWORKS | CISCO Partner | HP Business Partner