SLIDES ONLY

NO SCRIPT PROVIDED

CLEARED
For Open Publication

Jan 21, 2025

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

Technical Application of CMMC Requirements

ESPs, Asset Categories, SPA/SPD, and VDI

February 2025

Agenda

- CMMC Overview
- External Service Providers (ESPs)
  - Managed Service Providers (MSPs) and Managed Security Service Providers (MSSPs)
  - Cloud Service Providers (CSPs)
- Security Protection Assets (SPAs) and Security Protection Data (SPD)
- Virtual Desktop Infrastructure (VDI)
- Asset Category Differences between Level 2 and Level 3
- Contractor Risk Managed Assets (CRMAs)

CMMC Overview (1 of 2)

- CMMC is a 3-tier model of increasing requirements to assess and protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) data
- CMMC Levels 1 & 2 validate full compliance with existing regulations
- CMMC Level 3 adds and validates additional security requirements for select DoD programs to increase protection against advanced persistent threats (APTs)
- "CMMC Status of Level 1, Level 2, or Level 3" is a condition of contract award when included in contracts that process, store, or transmit FCI or CUI
  - Primes flow requirements to subcontractors based on the data shared

CMMC Overview (2 of 2)

CMMC currently aligns to NIST SP 800-171 R2, NIST SP 800-171A Jun2018, NIST SP 800-172 Feb2021, and NIST SP 800-172A Mar2022

CMMC Level	Applicability	Security Requirements	Assessment Type	Assessment Frequency	Affirmation of Compliance
Level 1	**Federal Contract Information (FCI) [~140,000 DIB companies]**	FAR 52.204-21 (15 security requirements)	Self-assessment	Annual	Annual
Level 2	**Controlled Unclassified Information (CUI) [~75,000 DIB companies]**	DFARS 252.204-7012 requires NIST SP 800-171 R2 (110 security requirements)	Self-assessment or CMMC Third-Party Assessment Organization (C3PAO) assessment *(as specified in contract based on type of CUI)*	Every 3 years	Annual
Level 3	**CUI** deemed critical or high-value CUI by DoD program manager (PM) **[~1,500 DIB companies]**	NIST SP 800-171 R2 (C3PAO assessment) plus 24 NIST SP 800-172 Feb2021 (134 security requirements)	DIBCAC assessment *(conducted after Level 2 C3PAO assessment)*	Every 3 years	Annual

EXTERNAL SERVICE PROVIDER (ESP) SCOPING REQUIREMENTS for Level 2 and Level 3

When the ESP processes, stores, or transmits:	*When using an ESP that is:*	
	A Cloud Service Provider	Not A Cloud Service Provider
CUI (with or without Security Protection Data)	*The cloud service provider (CSP) shall meet the FedRAMP (Moderate or equivalent) requirements in 48 CFR 252.204–7012.*	*The services provided by the ESP are in the assessment scope of the organization seeking assessment (OSA) and shall be assessed as part of the OSA's assessment.*
Security Protection Data (without CUI)	*The services provided by the CSP are in the OSA's assessment scope and shall be assessed as security protection assets (SPAs).*	*The services provided by the ESP are in the OSA's assessment scope and shall be assessed as Security Protection Assets.*
Neither CUI nor Security Protection Data	*A service provider that does not process, store, or transmit CUI or security protection data (SPD) for the OSA, is not an ESP for CMMC assessment purposes.*	*A service provider that does not process CUI or SPD does not meet the CMMC definition of an ESP.*

ESPs can voluntarily undergo their own CMMC Level 2 C3PAO assessment

- Scope should cover services provided to clients
- Organizations seeking assessment (OSAs) must have a system security plan (SSP) that shows how select security requirements are performed by the ESP

ESP Services

Staff augmentation—traditional IT

- IT help desk (remote), onsite technicians, fractional CIO/CISO
- Policies and procedures

Procurement services

- Buy and install workstations, servers, and networks
- Buy and install software

Infrastructure as a Service (IaaS)

- Provide a portion of a cloud infrastructure that the ESP manages
- Provide infrastructure on ESP-owned hardware (private datacenter)

IT security services (MSSP)

- Security Operations Center (SOC)
  - An enterprise might provide this service to divisions within the same corporation
- Incident response and forensics

What you call them isn't important—it's what they do and provide that matters

CMMC Implications – Staff Augmentation

- Outsourced staff are essentially the same as OSA staff
- If there are offsite technicians or the managed service provider (MSP) has passwords to OSA equipment
  - Likely holding security protection data (SPD) in the form of admin passwords

CMMC Implications – IaaS

- What separates this from a CSP
  - End users cannot make changes and rapidly stand up and spin down hosts
- Examples
  - Physical servers in a rack in a data center
  - Small remote desktop server (RDS) environment in which the servers are owned and managed by the MSP
  - Virtual desktop infrastructure (VDI) environment tailored to DIB companies by the MSP
- Include within assessment scope if processes, stores, or transmits CUI
  - If not a CSP, then CUI is stored in ESP systems
  - How to draw the scoping boundary depends on the degree of isolation between the OSA's enclave and the rest of the MSP's infrastructure

CMMC Level 2 Assessment Implications – Managed Security Service Provider (MSSP)

Typically operates an SOC on behalf of the OSA

- Security protection assets (SPAs) (Table 3 to § 170.19(c)(1)—CMMC Level 2 Asset Categories and Associated Requirements)
  - Document in the asset inventory
  - Document asset treatment in SSP
  - Document in the network diagram of the CMMC Assessment Scope
  - Prepare to be assessed against CMMC Level 2
  - Assess against Level 2 requirements that are relevant to the capabilities produced
- Security protection data (SPD)
  - Assess against Level 2 requirements that are relevant to the capabilities produced

CMMC Level 3 Assessment Implications – Managed Security Service Provider (MSSP)

Typically operates an SOC on behalf of the OSA

- Security protection assets (SPAs) (Table 5 to § 170.19(d)(1)—CMMC Level 3 Asset Categories and Associated Requirements)
  - Document in the asset inventory
  - Document asset treatment in SSP
  - Document in the network diagram of the CMMC Assessment Scope
  - Prepare to be assessed against CMMC Level 2
  - Limited check against Level 2 requirements and assess against all Level 3 requirements that are relevant to the capabilities produced
- Security protection data (SPD)
  - Limited check against Level 2 requirements and assess against all Level 3 requirements that are relevant to the capabilities produced

What Is a Cloud Service Provider?

Cloud Service Provider (CSP) means an external company that provides cloud services based on cloud computing. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This definition is based on the definition for cloud computing in NIST SP 800-145 Sept2011. (CMMC-custom term, 32 CFR Part 170 Glossary)

Cloud Service Providers

- If CUI is processed, stored, or transmitted in a cloud offering, it must be FedRAMP-authorized at the Moderate level or higher or meet FedRAMP Moderate equivalency requirements
  - This is the same as current requirements under DFARS 252.204-7012
  - FedRAMP Moderate equivalency is described in a DoD policy memo
  - There is no registry of offerings that meet equivalency requirements
  - The OSA must evaluate the CSP's body of evidence (BOE)
  - CMMC Third-Party Assessment Organizations (C3PAOs) and Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) assessors will review the CSP's BOE as part of an OSA's assessment
- If CUI is not processed, stored, or transmitted in the cloud, FedRAMP authorization is not required
  - The services provided by the CSP are in the OSA's assessment scope and shall be assessed as SPAs.

Is my ESP a CSP?

- There are clear cases of an offering being a cloud offering
  - The company markets itself as a cloud offering – something as a Service (__aaS)
  - You acquire this service from the company, usually as a subscription service, and can rapidly provision and change services covered by the subscription
  - An MSP which configures an OSA's subscribed cloud service is not a CSP
- There are clear cases of not being a cloud offering
  - Host **your** hardware (leased or owned) in a colo or datacenter
  - Your ESP hosts your data on their system similar to shared drives on a local network
- There is a gray area where either case could be made depending on the service offered and what is covered in the customer responsibility matrix (CRM)
  - It depends on the relationships between the CSP, MSP, and OSA
  - Document and describe in the SSP

Is my MSP a CSP?

If you store CUI in the cloud and an MSP administers the environment, there needs to be an understanding if the MSP is a CSP.

It is determined by the relationships between the CSP, the MSP, and the OSA. If the cloud tenant is subscribed/licensed to the OSA (even if the MSP resells the service), **then the MSP is NOT a CSP.**

If the MSP contracts with the CSP and further modifies the basic cloud service, **then the MSP is a CSP** and must meet applicable FedRAMP or equivalency requirements. Further modifications to the service goes beyond simply configuring and maintaining the service on behalf of clients

- If the MSP owns the cloud tenant and further sub-divides it for customer use, they have probably crossed the line and are offering it as a cloud service
    - The MSP could choose to describe the service as storing CUI in their own system, in which case CMMC assessment requirements apply

Notable SPA and SPD Updates

ESPs that only store SPD or provide an SPA and **do not** process, store, or transmit CUI do **NOT** require a separate CMMC assessment, nor do they require FedRAMP authorization or equivalency.

The SPD definition also defines configuration data as data required to operate a security protection asset.

TABLE 3 TO § 170.19(c)(1)—CMMC LEVEL 2 ASSET CATEGORIES AND ASSOCIATED REQUIREMENTS

Asset category	Asset Description	OSA requirements	CMMC Assessment Requirements
Security Protection Assets	*Assets that provide security functions or capabilities to the OSA's CMMC Assessment Scope*	• *Document in the asset inventory* • *Document asset treatment in SSP* • *Document in the network diagram of the CMMC Assessment Scope* • *Prepare to be assessed against CMMC Level 2 security requirements*	*Assess against Level 2 security requirements that are relevant to the capabilities provided*

TABLE 5 TO § 170.19(d)(1)—CMMC LEVEL 3 ASSET CATEGORIES AND ASSOCIATED REQUIREMENTS

Asset category	Asset Description	OSA requirements	CMMC Assessment Requirements
Security Protection Assets	*Assets that provide security functions or capabilities to the OSA's CMMC Assessment Scope, irrespective of whether or not these assets process, store, or transmit CUI*	*• Document in the asset inventory* *• Document asset treatment in SSP* *• Document in the network diagram of the CMMC Assessment Scope* *• Prepare to be assessed against CMMC Level 2 and Level 3 security requirements*	*Limited check against Level 2 and assess against all Level 3 CMMC security requirements that are relevant to the capabilities provided*

Virtual Desktop Infrastructure (VDI)

An endpoint hosting a virtual desktop infrastructure (VDI) client configured to prevent any processing, storage, or transmission of CUI beyond the Keyboard/Video/Mouse sent to the VDI client is considered an Out-of-Scope Asset

- Use of tokens/certificates to authenticate to and within the portal is acceptable
- Assessors will check the configuration of the VDI system
- If not properly configured to prevent the processing, storage, or transmission of CUI, the endpoint will be treated as a CUI asset

Asset Category Differences Between Level 2 and Level 3 – Specialized Assets

Specialized Assets Assets that can process, store, or transmit CUI but are unable to be fully secured, including Internet of Things (IoT) devices, Industrial Internet of Things (IIoT) devices, Operational Technology (OT), Government Furnished Equipment (GFE), Restricted Information Systems, and Test Equipment		
	Level 2	Level 3
OSA Requirements	• Document in the asset inventory • Document asset treatment in the SSP ▪ Show these assets are managed using the contractor's risk-based security policies, procedures, and practices • Document in the network diagram of the CMMC Assessment Scope	• Document in the asset inventory • Document asset treatment in the SSP • Document in the network diagram of the CMMC Assessment Scope • Prepare to be assessed against CMMC Level 2 and Level 3 security requirements
CMMC Assessment Requirements	• Review the SSP • Do not assess against other CMMC security requirements	• Limited check against Level 2 and assess against all Level 3 CMMC security requirements • Intermediary devices are permitted to provide the capability for the specialized asset to meet one or more CMMC security requirements

Contractor Risk Managed Assets (CRMAs)

In the CMMC Assessment Requirements column for contractor risk managed assets (CRMA), it states, "If sufficiently documented, do not assess against other CMMC security requirements, except as noted."

“Prepare to be assessed against CMMC Level 2 security requirements” must be taken in context with the associated actions specified in the CMMC assessment column. **If the CRMAs are sufficiently documented in the SSP, then they will not be assessed against the other Level 2 security requirements.**

If the assessor determines that a limited check is needed due to lack of sufficient documentation or assessment findings that raise questions about how the asset is managed, then preparation can help support a successful assessment result. To reduce the likelihood of a limited check, clearly document in the SSP how the CRMA is effectively managed using the contractor’s risk-based security policies, procedures, and practices, to include the prevention of CUI being processed, stored or transmitted on that asset or a comprehensive approach to protect any CUI that might be accessed from that asset.

If an asset cannot be fully secured for any of the NIST SP 800-171 R2 requirements, it is considered a Specialized Asset, not a CRMA.

Asset Category Differences Between Level 2 and Level 3 – CRMA

CRMAs are described as assets that can, but are not intended to, process, store, or transmit CUI because of security policy, procedures, and practices in place.

These assets are not required to be physically or logically separated from CUI assets.

CRMAs in CMMC Level 2 become CUI Assets in Level 3 if in the same assessment scope

- OSC may choose to establish a Level 3 scope as a subset of the Level 2 scope.
- If an OSC intends to pursue a CMMC Level 3 assessment following the Level 2 assessment (for the same assessment scope), then the OSC may consider having the CRMAs assessed, or spot checked, as CRMAs are considered CUI Assets for Level 3 assessments.

Point of Contact

Cybersecurity Maturity Model Certification Program Management Office

For inquiries regarding Technical Application of CMMC Requirements

osd.pentagon.dod-cio.mbx.cmmc-inquiries@mail.mil

Questions?

What are SPAs and SPDs?

- **Security Protection Assets (SPAs)** are assets providing security functions or capabilities for the OSA's CMMC Assessment Scope.
  - SPAs might include SIEM, vulnerability scanners, and EDR solution
- **Security Protection Data (SPD)** means data stored or processed by Security Protection Assets (SPAs) that are used to protect an OSC's assessed environment. SPD is security-relevant information and includes but is not limited to configuration data required to operate an SPA, log files generated by or ingested by an SPA, data related to the configuration or vulnerability status of in-scope assets, and **passwords that grant access to the in-scope environment**.

(CMMC custom terms, 32 CFR Part 170 Glossary)

Acronyms (1 of 3)

Acronym	Definition
APT	Advanced Persistent Threat
BOE	Body of Evidence
C3PAO	CMMC Third-Party Assessment Organization
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMMC	Cybersecurity Maturity Model Certification
CRM	Customer Responsibility Matrix
CRMA	Contractor Risk Managed Asset
CSP	Cloud Service Provider
CUI	Controlled Unclassified Information
DFARS	Defense Federal Acquisition Regulation Supplement

Acronyms (2 of 3)

Acronym	Definition
DIBCAC	Defense Industrial Base Cybersecurity Assessment Center
DoD	Department of Defense
ESP	External Service Provider
FAR	Federal Acquisition Regulation
FCI	Federal Contract Information
IaaS	Infrastructure-as-a-Service
MSP	Managed Service Provider
MSSP	Managed Security Service Provider
NIST	National Institute of Standards and Technology
OSA	Organization Seeking Assessment
PM	Program Manager

Acronyms (3 of 3)

Acronym	Definition
RDS	Remote Desktop Server
SOC	Security Operations Center
SP	Special Publication
SPA	Security Protection Asset
SPD	Security Protection Data
SSP	System Security Plan
VDI	Virtual Desktop Infrastructure