



KRATOS
READY FOR WHAT'S NEXT™

Cybersecurity Maturity Model Certification (CMMC)

Ready For What's Next

December 2020

Introductions

Michael Fink
VP, Contracts
Kratos
Michael.Fink@KratosDefense.com

Justin Padilla
Director, Cybersecurity Services
Kratos | Space, Training, and Cybersecurity Division
Justin.Padilla@KratosDefense.com
Bio:
Justin Padilla leads the consulting arm of Kratos' commercial cybersecurity compliance, penetration testing, and continuous monitoring business. Drawing upon 15+ years of cybersecurity and IT experience across Cloud, Defense, Finance, Health, Transportation, and Homeland Security sectors, Mr. Padilla is expanding existing capabilities into new arenas of cybersecurity within the Kratos Space Division. Mr. Padilla participated in the CMMC-AB Training Working Group, and holds a B.S. in Computer Information Systems, Graduate certificates in counterintelligence and applied intelligence, as well as several cybersecurity industry certifications.

Cole French
Manager, CMMC Practice Lead
Kratos | Space, Training, and Cybersecurity Division
Cole.French@KratosDefense.com
Bio:
Cole French leads the CMMC capability for the consulting arm of Kratos' commercial cybersecurity compliance, penetration testing, and continuous monitoring business. Mr. French has supported clients across the health, finance, cloud, and Homeland Security sectors throughout his 10+ years of IT and cybersecurity experience. Mr. French is working to expand Kratos existing cybersecurity compliance capabilities into include CMMC assessment and advising services. Mr. French is a CMMC Provisional Assessor, Registered Practitioner, holds a Master of Science in Computer and Information Sciences, graduate certificate in cybersecurity, and several cybersecurity industry certifications.

Agenda

- What is CMMC
- CMMC Framework and Process
- Getting Ready for Certification
- An RPO Versus a C3PAO
- Questions

KRATOS
READY FOR WHAT'S NEXT™

What is CMMC

Where did it come from? How was it made? What does it mean?

What is CMMC

- A cybersecurity compliance framework established at the beginning of 2020 to provide a standard security baseline for organizations doing business with the DoD.
- The framework is sponsored by the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD (A&S)).
- The CMMC spokesperson is Katie Arrington, Chief Information Security Officer for the DoD A&S.
- The CMMC effort builds upon existing regulation DFARS 252.204-7012.

DFARS 252.204-7012

- On December 1, 2020, after a 60-day comment period, the CMMC framework officially took effect.
  - Now, the DoD can incorporate CMMC requirements into solicitations.
- This update also included a requirement that companies rate compliance against NIST's SP 800-171 using the DOD's Suppliers Performance Risk System (SPRS).
- These are closely related, because CMMC was largely derived from the NIST SP 800-171 requirements.
- In 2021, the DoD will require CMMC for 15 contracts.

CMMC Applicability

- **All DoD contractors will be required to have a CMMC certification** including:
  - Small/Large businesses
  - Subcontractors
  - Manufacturers
  - Commercial contractors
- DoD RFIs and RFPs will reflect the CMMC maturity level certification required to be awarded the contract. This will include subcontractor/supplier flow-downs.
- CMMC certification will be required at the time of contract award.
- Exceptions:
  - Classified environments
  - Organizations that solely produce Commercial-Off-The-Shelf (COTS) products, and don't make custom modifications to the COTS products

KRATOS
READY FOR WHAT'S NEXT™

CMMC Framework & Process

What's inside?

CMMC Construct

The CMMC Frameworks consists of maturity processes and security practices that are organized into a set of domains and mapped to levels.

- Domains – 17 families of security-related requirements.
  - Capabilities – Each domain has a set of processes and capabilities. There are 43 capabilities associated within the 17 domains
  - Practices – 171 specific security controls associated with a capability and aligns to the appropriate level of maturity
  - Processes – 5 maturity process associated to all domains related to documentation and management of documentation
- Levels – Five levels of cybersecurity maturity from basic to advanced.

17 CMMC Domains

CMMC Levels, Practices, Processes

Level	Maturity - Security Practices		Maturity Processes		Total Controls
1	Basic Demonstrate basic cyber hygiene, as defined in the FAR	**17**	N/A	**0**	**17**
2	Intermediate Demonstrate intermediate cyber hygiene	17+55= **72**	Documented Standard operating procedures, policies, and plans are established for all practices	**2**	72 + 2 = **74**
3	Good Demonstrate good cyber hygiene and effective NIST 800-171 Rev 1 security requirements	72+58= **130**	Managed Activities are reviewed for adherence to policy and procedures and adequately resourced	2+1= **3**	130 + 3 = **133**
4	Proactive Demonstrate a substantial and proactive cybersecurity program	130+26= **156**	Reviewed Activities are reviewed for effectiveness and management is informed of any issues	3+1= **4**	156 + 4 = **160**
5	Advanced/Progressive Demonstrate a proven ability to optimize capabilities to repel advanced persistent threats	156+15= **171**	Optimized Activities are standardized across all applicable organizational units and identified improvements are shared	4+1= **5**	171 + 5 - **176**

CMMC Process Overview

Step	Activity	Responsible Party	Timing
1	Understand CMMC requirements and applicability	Customer with optional RPO support	Up to Customer
2	Determine you scope: Entire Enterprise, Organizational Unit, Program Enclave	Customer with optional RPO support	Up to Customer
3	Determine CMMC Level (1 – 5)	Customer with optional RPO support	Up to Customer
4	(Optional) CMMC Gap Assessment (RPO) or Readiness Assessment (C3PAO)	RPO or C3PAO	2-4 weeks
5	Close Gaps	Customer with optional RPO support	Up to Customer
6	Contract with a C3PAO	Customer	Up to Customer
7	Conduct C3PAO Assessment	C3PAO	TBD base on level est. 4-8 weeks
8	Finding Resolution (up to 90-days)	Customer with optional RPO support	0-90 days
9	CMMC-Accreditation Body reviews assessment	CMMC-AB	Est. 1 month
10	3-Year Certification is Issued	CMMC-AB	Est. 0-5 days

CMMC Process – Key Considerations

- **Applicability**: determine if CMMC applies to your organization and, more specifically, to what parts of your organization.
- **Scope**: determine if a CMMC certification is required for your entire organization or a subset.
- **Level**: determine the level of certification that is required for your organization (most organizations will require a Level 1 certification, while a smaller subset will require a Level 3 certification).
- **Gaps**: a readiness assessment can identify gaps before an assessment so that they can be closed ahead of the assessment.
- **Findings**: assessment findings must be remediated within 90 days.
- **Certification**: requires that all findings are satisfactorily closed and is valid for a period of 3 years.

KRATOS
READY FOR WHAT'S NEXT™

Getting Ready For Certification

Level 1 & Level 3

CMMC Level 1

Most organizations will naturally be meeting the 17 CMMC Level 1 requirements. These include the following capabilities:

- Establishing system access
- Controlling internal system access
- Limiting access to data
- Grant access to only authorized entities
- Sanitizing media
- Limiting physical access
- Controlling communications at system boundaries
- Identifying and managing information system flaws
- Identifying malicious content

CMMC Level 1 – Access Control (1 of 4)

Access Control

- Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
  - Users, processes, and devices are identified
  - Users, processes, and devices are authorized

An assessor will typically compare a list of users, processes, and devices against a list that shows that users, processes and devices are authorized.

CMMC Level 1 – Access Control (2 of 4)

Access Control

- Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
  - Types of transactions and functions are defined
  - System access is limited to the defined types of transactions and functions

An assessor will typically compare what is required and defined against what is actually implemented in the system.

CMMC Level 1 – Access Control (3 of 4)

Access Control

- Verify and control/limit connections to and use of external information systems.
  - External connections and use is identified
  - External connections and use is verified
  - External connections and use is controlled/limited

An assessor will typically compare the authorized intra or inter connections to actual connections.

CMMC Level 1 – Access Control (4 of 4)

Access Control

- Control information posted or processed on publicly accessible information systems.
  - Identified individuals authorized to post on publicly accessible systems
  - Procedures for reviewing posts prior and after being made publicly accessible
  - Mechanisms for removing and addressing improper postings

An assessor will typically review public postings and validate that they were approved for public release.

CMMC Level 1 – Identification & Authentication

Identification & Authentication

- Identify information system users, processes acting on behalf of users, or devices.
- Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
  - Users, processes, and devices are uniquely identifiable
  - The identity of a user, device, or process is authenticated as a prerequisite to system access

An assessor will typically review unique devices identifiers, and unique attributes of users or processes acting on behalf of users to validate that there is individual accountability and traceability. An assessor will validate that there is some authentication mechanism for users, devices, and processes acting on behalf of users.

CMMC Level 1 – Media Protection (1 of 1)

Media Protection

- Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.
  - System media containing FCI or CUI is sanitized or destroyed prior to disposal or reuse

An assessor will review the process to validate that sanitization practices are in place and consistent. NIST SP 800-88 provides specific guidance on media sanitization.

CMMC Level 1 – Physical Protection (1 of 4)

Physical Protection

- Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
  - Authorized individuals are identified
  - Physical access to systems, equipment and the operating environment is limited to authorized individuals

An assessor will review physical access processes, validate that authorized individuals are identifiable, and determine if access is controlled.

CMMC Level 1 – Physical Protection (2 of 4)

Physical Protection

- Escort visitors and monitor visitor activity.
  - Visitors are escorted
  - Visitor activity is monitored

An assessor will review visitor processes and look for evidence that visitors are escorted and monitored.

CMMC Level 1 – Physical Protection (3 of 4)

Physical Protection

- Maintain audit logs of physical access.
  - Physical access logs are maintained

An assessor will review paper or digital logs to validate that physical access logs are maintained.

CMMC Level 1 – Physical Protection (4 of 4)

Physical Protection

- Control and manage physical access devices.
  - Physical access devices are identified, controlled, and managed

An assessor will validate that physical access devices are identifiable, controlled and managed.

CMMC Level 1 – System & Communications Protection (1 of 2)

System and Communications Protection

- Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
  - External and key internal system boundaries are identified
  - Communications in and out of the boundaries are monitored, controlled, and protected

An assessor will review at the network design and protection mechanisms (e.g., firewalls) at boundary edges.

CMMC Level 1 – System & Communications Protection (2 of 2)

System and Communications Protection

- Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
  - Publicly accessible systems are identified
  - Subnetworks for publicly accessible systems are physically or logically separated from internal networks.

An assessor will typically review publicly facing assets and validate that they are contained within DMZ.

CMMC Level 1 – System & Information Integrity (1 of 4)

System and Information Integrity

- Identify, report, and correct information and information system flaws in a timely manner.
  - The timing of when system flaws are identified is specified, occurs, and is reported
  - The timing of when system flaws are corrected is specified, and occurs

An assessor will typically review the system patching cycle, system updates, and signature updates to validate that they are timely and consistent.

CMMC Level 1 – System & Information Integrity (2/3 of 4)

System and Information Integrity

- Provide protection from malicious code at appropriate locations within organizational information systems.
- Update malicious code protection mechanisms when new releases are available.
  - Designated locations for malicious code protection are identified
  - Protection from malicious code at designated locations is provided
  - Malicious code protection mechanisms are updated when new releases are available

An assessor will typically determine is anti-virus and anti-malware mechanisms are in place within the environment and validate that signature updates are occurring and up to date.

CMMC Level 1 – System & Information Integrity (4 of 4)

System and Information Integrity

- Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.
  - Define the frequency of malicious code scans
  - Scans are conducted within the defined frequency
  - Real-time code scans of files from external source

An assessor will validate that email attachments, downloads, and external media is scanned during download.

CMMC Level 3

Working with various organization we have identified a few of the top challenges that can be showstoppers.

- Documentation
- Inventory
- Multi-factor authentication
- Centralized auditing
- Application Approved/Deny Lists
- CUI Handling and Marking

CMMC Level 3 - Documentation

Documentation

- System Security Plan
- Policy for each of the CMMC domain families
- Practices for each of the CMMC domain families
- Resource Plan for each of the CMMC domain families
- Configuration Management Plan
- Incident Response Plan
- Contingency Plan
- Risk Mitigation Plan
- Vulnerability Management Plan
- Separation of Duties / Privileged Functions Matrix
- Business Impact Analysis
- Continuous Monitoring Plan

CMMC Level 3 - Inventory

Inventory

- The ability to generate inventories, specific to the CMMC environment that would include:
  - User and elevated privilege user Inventory
  - Asset inventory
  - Application/Software Inventory
  - Site inventory

CMMC Level 3 - Multi-Factor Authentication

Multi-Factor Authentication

- Multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
  - MFA for Network Access of non-privileged accounts
  - MFA for Network Access of privileged accounts
  - MFA for Privileged accounts

CMMC Level 3 – Centralized Auditing

Centralized Auditing

- Centralized audit log capture through the use of a Security Information and Event Management (SIEM) tool.
  - Standardized Network Time Protocols for log correlation
  - Defined auditable events for capture
  - Notification of logging failures
  - Reporting and correlation capability
  - Audit log reviews and analysis
  - Audit record protection

CMMC Level 3 – Application Approved/Deny Lists

Application Approved/Deny Lists

- Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software.

OR

- Apply deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.
  - Requires policy specifying which option is deployed within the environment
  - Requires approved OR denied software to be defined/documented
  - Requires the prevention of unauthorized software

CMMC Level 3 – CUI Handling and Marking

CUI Handling and Marking

- Proper and consistent CUI markings with distribution limitation in accordance with CUI requirements.
  - Required for paper and electronic media
  - Identification of where CUI is stored
  - Physical and digital protection of CUI
  - Consistency of CUI handling and marking procedures

KRATOS
READY FOR WHAT'S NEXT™

An RPO Versus a C3PAO

A Trusted Advisor versus an Assessor

What is an RPO

- A Registered Practitioner Organization (RPO) is an organization that provides CMMC services, such as gap assessments and strategic and technical consulting.
- RPO is an official designation by the CMMC.
- RPOs have Registered Practitioners (RP), which is also an official designation by the CMMC.
- An RP must receive and successfully complete CMMC training.
- An RP must undergo a commercial background check.
- RPs are intended to provide advisory/consulting support services but can also be involved in an assessment.

RPO Cautionary Advice

Not all advisors are created equally. Knowing what you are buying is important. Some red flags include:

- Companies that say they can provide advisory and assessment services for you.
- Flat fee documentation – unless they are providing you with templates only, an advisor that says they will write everything for you with minimal involvement from you side.
- Gap Assessments that are conducted too early can often result in a massive amount of findings with minimal direction on how to fix.
- One stop shop managed services for everything rarely exists.

What is a C3PAO

- A CMMC Third Party Assessment Organization (C3PAO) is the only business authorized to deliver CMMC assessments.
- C3PAOs provide services such as scoping analysis, readiness assessments and penetration testing/red teaming.
- A C3PAO must have a certified assessor (or provisional assessor) certified at the level that the organization seeking assessment is attempting to achieve (e.g., an organization seeking a Level 3 certification must leverage a certified assessor that is certified at a Level 3).
- C3PAOs and certified assessors must undergo background investigations and successfully pass an assessment themselves.

C3PAO Cautionary Advice

Selecting a qualified C3PAO is important, companies should be cautious about who they are signing with.

- Currently, there are no C3PAOs. However, the CMMC-AB has trained “Provisional Assessors”, which are different than being a C3PAO.
- Assessors that want upfront payment to get in a queue – the CMMC-AB has advised heavily against this practice.
- Assessors that say they can consult and assess your environment.
- Assessors that say they can assess your level 4/5 environment.

KRATOS
READY FOR WHAT'S NEXT™

Questions