Cybersecurity Resiliency for Defense Contractors Webinar Series:

CMMC Breakdown

November 5, 2020
Jana White

ALPINE SECURITY IMEC

1

Today's Topics

- What is Cybersecurity Maturity Model Certification (CMMC)?
- Levels of CMMC framework and how to determine required level of compliance

ALPINE SECURITY IMEC

2

ALPINE SECURITY

Service-Disabled Veteran Owned Small Business (SDVOSB)

Areas of Focus:

Cybersecurity Training

Penetration Testing

Vulnerability Assessments

CISO-as-a-Service

Cybersecurity Strategy

DFARS 252.204-7012 & CMMC

Based in Greater St. Louis Area

IMEC

3

What is Cybersecurity Maturity Model Certification (CMMC)?

The CMMC is a **maturity model** which measures an organization's cybersecurity maturity with five levels and aligns a set of **processes** (based on security domains) and **practices** (based on current capabilities) with the type and sensitivity of information to be protected (**CUI**) and the associated range of threats to that information and the organization as a whole (**risks**).

CYBERSECURITY MATURITY MODEL CERTIFICATION

ALPINE SECURITY

IMEC

4

What is a maturity model?

A maturity model is a set of characteristics, attributes, indicators, or patterns that represent capability and progression in a particular discipline (best practices and standards)

A maturity model provides a benchmark for an organization to evaluate the current level of capability of its processes, practices, and methods and set goals and priorities for improvement

ALPINE SECURITY

IMEC

5

CMMC: Securing the supply chain

Malicious cyber actors have targeted and continue to target the Defense Industrial Base (DIB) sector and the supply chain of the Department of Defense (DoD).

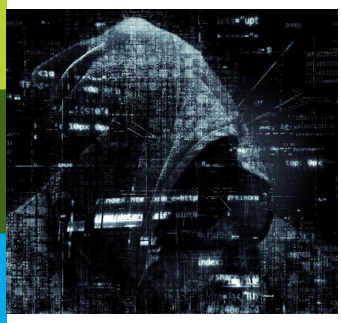
The DIB sector consists of over 300,000 companies that support the United States military efforts and contribute towards the research, engineering, development, acquisition, production, delivery, sustainment, and operations of DoD systems, networks, installations, capabilities, and services.

ALPINE SECURITY

IMEC

6

Supply chain cybersecurity risks you need to watch out for



- Third party suppliers (contracted to larger companies and often targeted because they are more vulnerable)
- Tier 2 suppliers (your suppliers' suppliers)
- Software solutions providers
- Social engineering – lack of security awareness training

ALPINE SECURITY

IMEC

7

Why is the DoD mandating CMMC certification?

CMMC is designed to provide increased assurance to the DoD that a Defense Industrial Base contractor can adequately protect Controlled Unclassified Information (CUI) at a level commensurate with the risk, accounting for information flow down to its subcontractors in a multi-tier supply chain.

ALPINE SECURITY

IMEC

8

The Cybersecurity Maturity Model Certification (CMMC) Framework

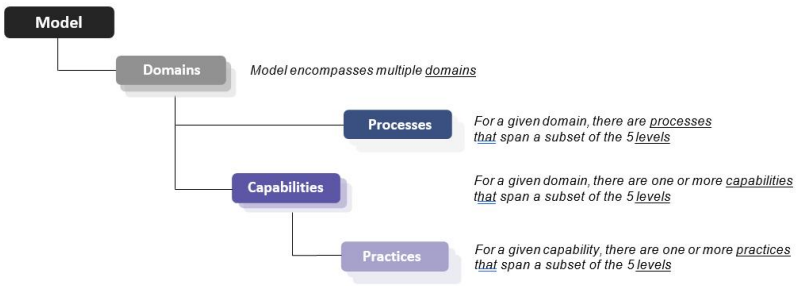


Figure 1. CMMC Model Framework (Simplified Hierarchical View)

ALPINE SECURITY

IMEC

9

The 17 domains of the CMMC

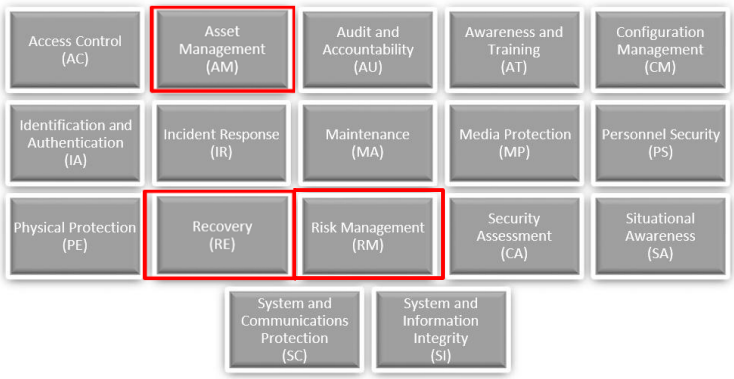


Figure 4. CMMC Domains

ALPINE SECURITY

IMEC

10

Capabilities

Domain	Capability
Access Control (AC)	• Establish system access requirements • Control internal system access • Control remote system access • Limit data access to authorized users and processes
Asset Management (AM)	• Identify and document assets • Manage asset inventory
Audit and Accountability (AU)	• Define audit requirements • Perform auditing • Identify and protect audit information • Review and manage audit logs
Awareness and Training (AT)	• Conduct security awareness activities • Conduct training

Each domain consists of a set of processes and capabilities (and in turn, practices) across the five levels. Table 1 in the CMMC v 1.02 document itemizes the 43 capabilities associated with the 17 domains in the CMMC model.

ALPINE SECURITY

IMEC

11

Processes

Maturity Level	Maturity Level Description	Processes
ML 1	Performed	*There are no maturity processes assessed at Maturity Level 1.* *An organization performs Level 1 practices but does not have process institutionalization requirements.*
ML 2	Documented	Establish a policy that includes [DOMAIN NAME].
		Document the CMMC practices to implement the [DOMAIN NAME] policy.
ML 3	Managed	Establish, maintain, and resource a plan that includes [DOMAIN NAME].
ML 4	Reviewed	Review and measure [DOMAIN NAME] activities for effectiveness.
ML 5	Optimizing	Standardize and optimize a documented approach for [DOMAIN NAME] across all applicable organization units.

Within the context of the CMMC model, process institutionalization provides additional assurances that the practices associated with each level are implemented effectively.

- *organizations perform practices at Level 1, but process maturity is not assessed for ML 1*

ALPINE SECURITY

IMEC

12

Practices

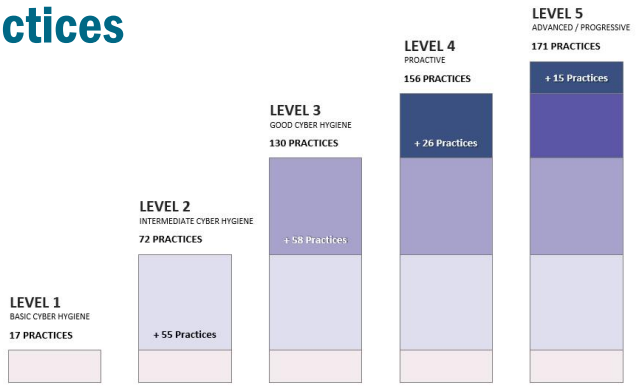


Figure 5. CMMC Practices Per Level

The CMMC model measures not only process maturity but also the implementation of practices. The model consists of 171 practices that are mapped across the five levels for all capabilities and domains.

ALPINE SECURITY

IMEC

13

Levels of CMMC framework

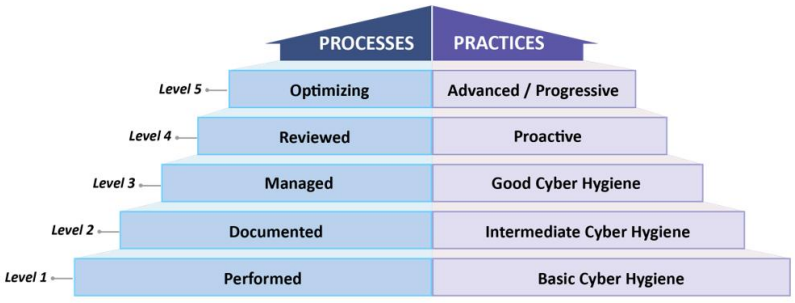


Figure 2. CMMC Levels and Descriptions

In order for an organization to achieve a specific CMMC level it must also demonstrate achievement of the preceding lower levels.

ALPINE SECURITY

IMEC

14

You must have both the processes and the practices in place!

An organization must demonstrate **both** the requisite institutionalization of processes and the implementation of practices for a specific CMMC level and the preceding lower levels in order to achieve that level.

If an organization demonstrates different achievements with respect to process institutionalization and practice implementation, the organization **will be certified at the lower of the two levels.**

ALPINE SECURITY

IMEC

15

CMMC Level Focus

- **Level 1**: Safeguard Federal Contract Information (FCI)
- **Level 2**: Serve as transition step in cybersecurity maturity progression to protect CUI
- **Level 3**: Protect Controlled Unclassified Information (CUI)
- **Levels 4-5**: Protect CUI and reduce risk of Advanced Persistent Threats (APTs)

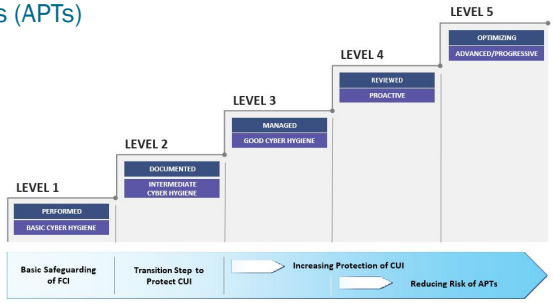


Figure 3. CMMC Levels and Associated Focus

ALPINE SECURITY

IMEC

16

Level 1 – Basic Cyber Hygiene (17 practices)

Processes: Performed

- Level 1 requires that an organization performs the specified practices. Because the organization may only be able to perform these practices in an ad-hoc manner and may or may not rely on documentation, process maturity is not assessed for Level 1.

Practices: Basic Cyber Hygiene

- Level 1 focuses on the protection of FCI and consists only of practices that correspond to the basic safeguarding requirements specified in 48 CFR 52.204-21 ("Basic Safeguarding of Covered Contractor Information Systems")

ALPINE SECURITY IMEC

17

Level 2- Intermediate Cyber Hygiene (72 practices)

Processes: Documented

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

Practices: Intermediate Cyber Hygiene

- Level 2 serves as a progression from Level 1 to Level 3 and consists of a subset of the security requirements specified in NIST SP 800-171 as well as practices from other standards and references. Because this level represents a transitional stage, a subset of the practices reference the protection of CUI.

ALPINE SECURITY IMEC

18

Level 3 – Good Cyber Hygiene (130 practices)

Processes: Managed

- Level 3 requires that an organization 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. **(SSP, POAM)**

Practices: Good Cyber Hygiene

- Level 3 focuses on the protection of CUI and encompasses all of the security requirements specified in NIST SP 800-171 as well as additional practices from other standards and references to mitigate threats.
  - *It is noted that DFARS clause 252.204-7012 ("Safeguarding of Covered Defense Information and Cyber Incident Reporting") [5] specifies additional requirements beyond the NIST SP 800-171 security requirements such as incident reporting.* ***(IRP)***

ALPINE SECURITY IMEC

19

Level 4 – Proactive Practices (156 Practices)

Processes: Reviewed

- Level 4 requires that an organization review and measure practices for effectiveness. In addition to measuring practices for effectiveness, organizations at this level are able to take corrective action when necessary and inform higher level management of status or issues on a recurring basis.

Practices: Proactive

- Level 4 focuses on the protection of CUI from APTs and encompasses a subset of the enhanced security requirements from Draft NIST SP 800-171B as well as other cybersecurity best practices. These practices enhance the detection and response capabilities of an organization to address and adapt to the changing tactics, techniques, and procedures (TTPs) used by APTs.

ALPINE SECURITY IMEC

20

Level 5- Advanced/Progressive Practices (171 Practices)

Processes: Optimizing

- Level 5 requires an organization to standardize and optimize process implementation across the organization.

Practices: Advanced/Proactive

- Level 5 focuses on the protection of CUI from APTs. The additional practices increase the depth and sophistication of cybersecurity capabilities.

ALPINE SECURITY

IMEC

21

Where do I have to implement CMMC within my network?

When implementing CMMC, a DIB contractor can achieve a specific CMMC level for its entire enterprise network or for particular segment(s) or enclave(s), depending upon where the information to be protected is handled and stored.

Reducing your CUI Information System (IS) is a fantastic way to better control and secure your CUI and reduce resources needed for the implementation of DFARS and CMMC controls!

ALPINE SECURITY

IMEC

22

How to determine your required level of compliance

For now, look at your contracts/analyze your data

- vendors that only have contracts (FCI) with the DoD or a vendor in the supply chain but do not build components, have or use diagrams/schematics/drawings (or pieces of these documents) may only need level 1 (examples – lawn care service for Boeing building, payment processor for supply chain vendor)
- If you have anything else (CUI), work towards level 3!

ALPINE SECURITY

IMEC

23

How to leverage my existing SSP and POAM to determine my compliance level

- Review your SSP and POAM and look at the NIST SP 800-171 controls you believe you have fully implemented
  - *Use the NIST SP 800-171A to dive deeper*
- Check off the 110 NIST SP 800-171 controls from your CMMC spreadsheet
- Identify your gaps, add the missing CMMC controls to your existing POAM
- Implement the missing controls

ALPINE SECURITY

IMEC

24

C3PAOs – These are the assessors you are looking for

- CMMC 3rd Party Assessor Organizations
- https://www.cmmcab.org/marketplace
- This process is still under development, check back often!!!

ALPINE SECURITY

IMEC

25

How long will my certification be valid?

The certification must be in place prior to contract award (rather than at the time of proposal submission or after award), and will be valid for three years

ALPINE SECURITY

IMEC

26

CMMC dos and don'ts

Do get ready for certification now and get your assessment as soon as you can (220,000 vendors in line!)

Don't tell anyone your certification level unless it is needed for a contract/DoD

ALPINE SECURITY

IMEC

27

When will I have to be CMMC compliant?

- DFARS interim rule clauses 252.204-7019-7021 go into effect November 30, 2020
- Office of the Under Secretary of Defense for Acquisition & Sustainment (OUSD [A&S]) must approve use of the clause on new acquisitions until October 2025
- After October 2025 CMMC is required for all contracts (above micro-purchase threshold [$10K]), excluding COTS
- Primes will have to ensure subs are certified prior to awarding subcontracts

ALPINE SECURITY

IMEC

28

What should I do to begin my CMMC journey?

1. Conduct your DoD required basic assessment of the NIST SP 800-171 controls (submit your score to SPRS by Nov. 30, 2020)
2. Make sure your organization has an SSP, POAM, and IRP
3. Begin implementing any NIST SP 800-171 controls not implemented (POAM)
4. Review the CMMC Level 3 control requirements, include gaps or missing controls on current POAM (20 controls)
5. Use NIST SP 800-171A to ensure you are implementing both processes and practices for the 800-171 controls

ALPINE SECURITY

IMEC

29

Other Helpful Resources (Freebies!)

- OUSD A&S page for CMMC - https://www.acq.osd.mil/cmmc/draft.html
- CMMC Model version 1.02 - https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf
- CMMC Version 1.02 Audit Spreadsheet

ALPINE SECURITY

IMEC

30

What We Covered Today…

- What is Cybersecurity Maturity Model Certification (CMMC)?
- Levels of CMMC framework and how to determine required level of compliance

ALPINE SECURITY

IMEC

31

Jana White
jana.white@alpinesecurity.com
www.alpinesecurity.com
info@alpinesecurity.com
(844) 925-7463

ALPINE SECURITY

IMEC

32