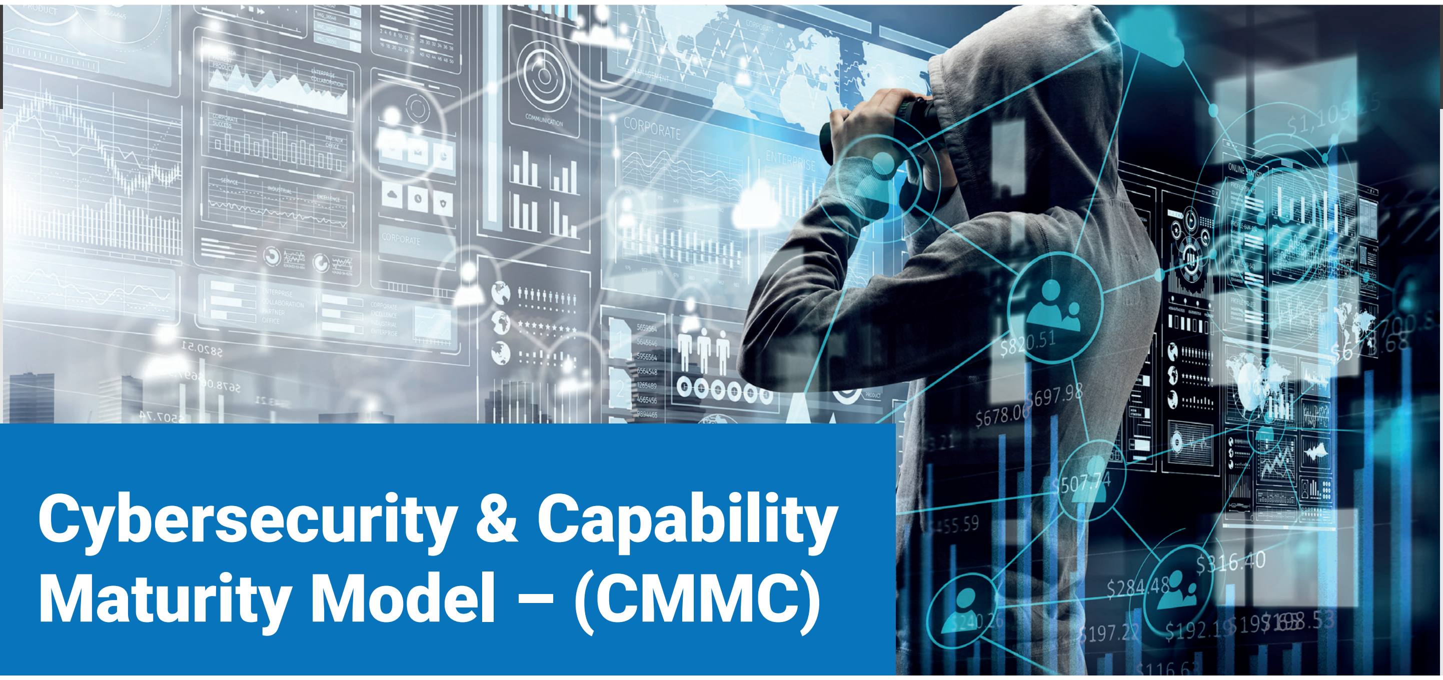
White Paper

Business Office
11000 SE CR 3280
Kerens, TX 75144

Virginia Office
11921 Freedom Dr,
Suite 550
Reston, VA 20190

Texas Office
500 West Seventh St. Suite 700
Fort Worth, TX 76102

HARMONY TECHNOLOGY SERVICES
A Clear Creek Group Company



Cybersecurity & Capability Maturity Model – (CMMC)

Introduction

Cybersecurity is a rapidly evolving field that is becoming increasingly important in today's digital age. As the world becomes more connected, the threat of cyber-attacks continues to grow. From large-scale data breaches to targeted phishing scams, businesses and individuals alike are at risk. In response, the cybersecurity industry is constantly developing new technologies and strategies to protect against these threats. However, staying ahead of cybercriminals is a constant battle, and as technology advances, so too do the methods of those looking to exploit it. Despite this, many organizations are still struggling to keep their systems secure, and it has become clear that cybersecurity is a top priority for the future.

With the increasing use of technology while executing on both government and commercial contracts, the risk of cyber-attacks and data breaches has also increased, making it crucial for organizations to take proactive measures to secure their information systems. One of the key approaches to managing cybersecurity is by using the Capability Maturity Model - Cybersecurity (CMMC) framework.

What is CMMC? *(short history of CMMC versions)*

CMMI (Capability Maturity Model – Integration) is a model that provides a systematic approach to improving processes, practices, and tools in software engineering. The CMMC framework is a specialized version of CMMI designed specifically for cybersecurity. The CMMC is an assessment framework and assessor certification program designed to increase the trust in measures of compliance to a variety of standards published by the National Institute of Standards and Technology.

CMMC provides a structure for evaluating and improving the maturity of an organization's cybersecurity processes, practices, and tools. The CMMC framework and model was developed by Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) of the United States Department of Defense through existing contracts with Carnegie Mellon University, The Johns Hopkins University Applied, Physics Laboratory LLC, and Futures, Inc. The Cybersecurity Maturity Model Certification Accreditation Body oversees the program under a no cost contract.

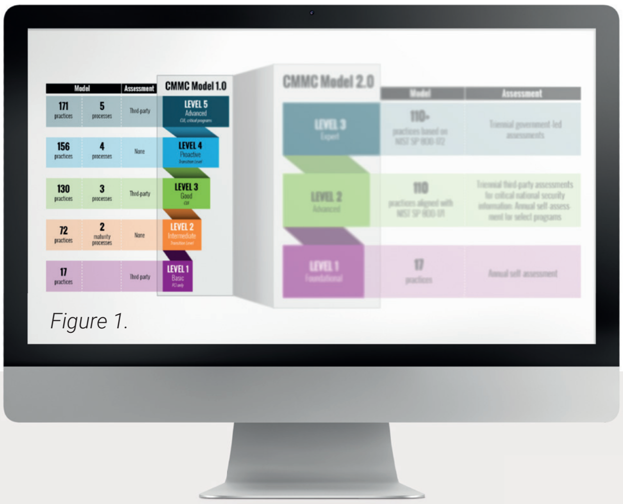
What is the Purpose of CMMC?

The purpose of CMMC is to verify that the information systems used by the contractors of the United States Department of Defense to process, transmit or store sensitive data is in compliant with the mandatory information security requirements. The goal is to ensure appropriate protection of Controlled Unclassified Information (CUI) and Federal Contract Information (FCI) that is stored and processed by the partner or vendor. **It is equally applicable to the protection of Commercial contract information.**

CMMC Model

CMMC Model 1.0

The initial version (CMMC Model 1.0) of the model was based on five maturity levels, each representing a progressively higher degree of process definition and institutionalization. Model 1.0 comprised the five maturity levels as shown in Figure 1.



Model		Assessment	CMMC Model 1.0
171 practices	5 processes	Third-party	LEVEL 5 Advanced CUI, critical programs
156 practices	4 processes	None	LEVEL 4 Proactive Transition Level
130 practices	3 processes	Third-party	LEVEL 3 Good CUI
72 practices	2 maturity processes	None	LEVEL 2 Intermediate Transition Level
17 practices		Third party	LEVEL 1 Basic FCI only

Figure 1.

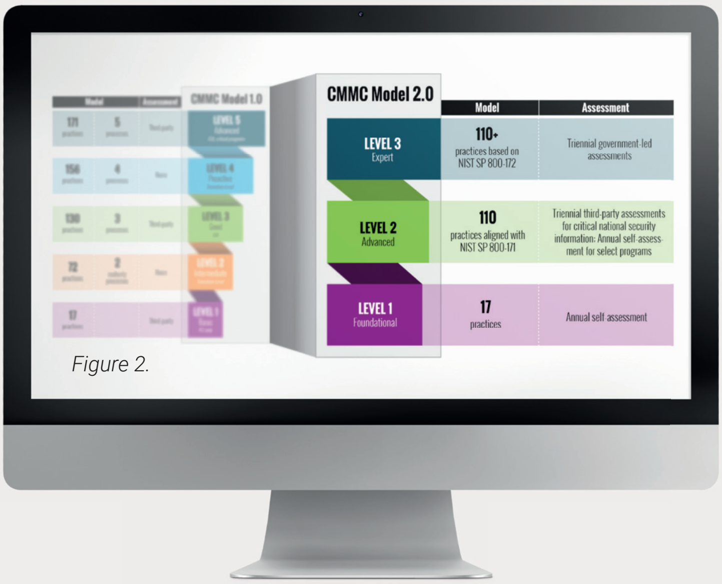
CMMC Model 2.0

CMMC 2.0 (also see Figure 1) comprises three levels, eliminating CMMC 1.0's Levels 2 and 4 in accordance with DoD's comment that these levels were only ever "developed as transition levels and never intended to be assessed requirements." A major difference is that CMMC 2.0's three levels directly correlate to other federal requirements already in place:

Level 1. **Foundational** is aligned with FAR 52.204-21: Basic Safeguarding of Covered Contractor Information Systems (for companies with Federal Contract Information (FCI) only); Level 1 focuses on the protection of FCI and consists of only practices that correspond to the basic safeguarding requirements specified in 48 CFR 52.204-21, commonly referred to as the FAR Clause [3].

Level 2. **Advanced** is aligned with NIST SP 800-171 Rev 2: Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and requires compliance with DFARS Clause 252.204-7012 (for companies with CUI); Level 2 focuses on the protection of CUI and encompasses the 110 security requirements specified in NIST SP 800-171 Rev 2 [4].

Level 3. **Expert** is aligned with NIST SP 800-172: Enhanced Security Requirements for Protecting (CUI) and requires compliance with FAR 52.204-21 and NIST SP 800-172 (for the highest priority programs with CUI); Lebel 3 will be based on a subset of NIST SP 800-172 requirements [6]. Details are to be released at a later date.



CMMC Model 2.0	Model	Assessment
LEVEL 3 Expert	110+ practices based on NIST SP 800-172	Triennial government-led assessments
LEVEL 2 Advanced	110 practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information; Annual self-assessment for select programs
LEVEL 1 Foundational	17 practices	Annual self-assessment

Figure 2.

In Summary

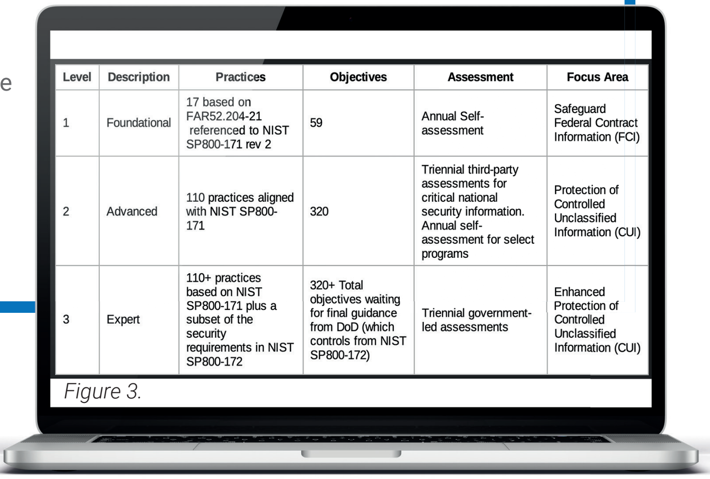
In summary, while CMMC 1.0 included requirements not found in other publications, CMMC 2.0 relies entirely on security practices prescribed in other government publications.

Level 1. Focuses on the protection of FCI and consists of only practices that correspond to the basic safeguarding requirements specified in 48 CFR 52.204-21, commonly referred to as the FAR Clause.

Level 2. Focuses on the protection of CUI and encompasses the 110 security requirements specified in NIST SP 800-171 Rev 2.

Level 3. Will be based on a subset of NIST SP 800-172 requirements. Details are to be released at a later date.

Figure 3 summarizes the three levels of CMMC 2.0:



Level	Description	Practices	Objectives	Assessment	Focus Area
1	Foundational	17 based on FAR52.204-21 referenced to NIST SP800-171 rev 2	59	Annual Self-assessment	Safeguard Federal Contract Information (FCI)
2	Advanced	110 practices aligned with NIST SP800-171	320	Triennial third-party assessments for critical national security information. Annual self-assessment for select programs	Protection of Controlled Unclassified Information (CUI)
3	Expert	110+ practices based on NIST SP800-171 plus a subset of the security requirements in NIST SP800-172	320+ Total objectives waiting for final guidance from DoD (which controls from NIST SP800-172)	Triennial government-led assessments	Enhanced Protection of Controlled Unclassified Information (CUI)

Figure 3.

Benefits of CMMC

The use of CMMC provides several benefits to organizations in terms of cybersecurity, including:

Improved Processes: CMMC provides a structure for evaluating and improving the maturity of an organization's cybersecurity processes, practices, and tools. This can lead to more effective and efficient processes, and reduced risk of cyber-attacks and data breaches.

Increased Awareness: The use of CMMC helps raise awareness of the importance of cybersecurity within an organization. This can lead to greater involvement and commitment from employees, and a stronger overall culture of security.

Better Resource Allocation: By evaluating the maturity of their cybersecurity processes, practices, and tools, organizations can better allocate resources to areas that need improvement. This can help ensure that resources are used effectively and efficiently, and that the organization's information systems are better protected.

Improved Compliance: CMMC can help organizations meet regulatory and industry standards for cybersecurity. This can be especially important for organizations in regulated industries, such as finance, healthcare, and government.

Harmony Technology Services

Harmony Technology Services works with clients in several ways to optimize performance of people, processes and technology while also helping to identify and mitigate dangers in the following ways:

- **Risk Assessment** – working with you to determine your specific data risks .
- **Policy Development** – helping you define guiding principles to protect your company including network access policies and specific software protection requirements.
- **Architectural Definition and Deployment** – determining your policy and needs to technical support (hardware and software) needed.
- **Monitoring and Compliance** – to ensure that your policies are being applied and respond effectively to changing technical environments and threats.

Harmony Technology Services has high level expertise in the Department of Defense (DoD) space and components of the NIST framework for cybersecurity. They provide their clients with guidance in translating the NIST cyber framework into a business context without it becoming overwhelming. In addition, they deliver continuing analysis and ongoing threat mitigation.

Harmony Technology Services partners with clients for long-term cybersecurity partnerships from A to Z, with a phased approach that includes:

- **Risk Assessment**
- **System Engineering/Design**
- **Implementation**
- **Ongoing Oversight & Reassessment**

Conclusion

Cybersecurity is a critical issue that affects organizations of all sizes and industries. The use of CMMC provides a structured approach to improving the maturity of an organization's cybersecurity processes, practices, and tools, and can help organizations reduce the risk of cyber-attacks and data breaches. By using CMMC, organizations can better protect their Federal and Corporate information, and be in compliance with Federal requirements.

Your level of cybersecurity protection depends on the risks you are willing to take, the robustness of the system in place and your compliance footprint. By partnering with Harmony Technology Services, we will help you mitigate the risk of threats to your company's data while protecting your business continuity, customer confidence, business investments and opportunities.

Everyone now needs cybersecurity as sensitive data is stored globally and your network boundaries become less clear. You need peace of mind to know your information systems used for government and commercial contracts are verified to process, transmit and store sensitive data, and are in compliance with the recommended security requirements. Partnering with Harmony Technology Services will help you answer your cybersecurity needs.

RESOURCES

Harmony Technology is dedicated to Improving Healthcare data security by evaluating people, process, & technology.

References

48 CFR 52.204-21
SP 800-171 Rev 2
SP 800-172

Author

Dan Seely

Dan provides world-class technical and program management expertise and advice to our executive leadership team in areas as diverse as cyber security, health care systems, system and software development, information and data acquisition, and information processing systems. Dan has 45+ years of experience delivering information technology systems, intelligence information systems, data acquisition systems and signal and data processing systems and is experienced in the full life-cycle of system engineering, development and program management activities, including pre-proposal marketing, proposal development, team building, system requirements specification, enterprise and system architecture.

✉ *dan.seely@harmonytechnologyservices.com*

Contact

Josh Shelman

Director of Business Development

✉ *josh.shelman@harmonytechnologyservices.com*
☎ *817-879-3787*
in *www.linkedin.com/in/josh-shelman-b79039a*

Contact Us

Business Office
11000 SE CR 3280
Kerens, TX 75144

Virginia Office
11921 Freedom Dr,
Suite 550
Reston, VA 20190

Texas Office
500 West Seventh St. Suite 700
Fort Worth, TX 76102

www.harmonytechnologyservices.com

www.linkedin.com/company/harmony-technology-services-inc/

VISIT OUR
WEBSITE