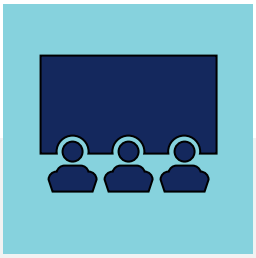
WHITEHAWK®

CMMC Overview

CYBERSECURITY MATURITY MODEL CERTIFICATION

September 2020



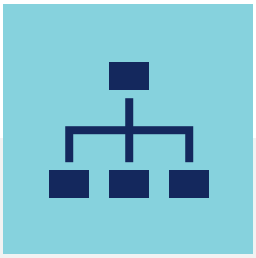



Table of Contents

CMMC Background

For over a decade, the U.S. Defense Industrial Base (DIB) and Federal Contractors have been under continuous cyber-attack from State Actors conducting industrial espionage, targeting a breadth of research and development (R&D) and intellectual property valued at tens of billions of US dollars. According to the FBI Director Wray, (Conversation Link) China in particular has many campaigns ongoing across Federal Contractors and suppliers to save their country years of R&D. These, and other State Cyber Actors and criminals, have achieved root level access across key Federal Contractors and their respective supply chains and partners. This is often a silent but costly cyber war.

As a result, since January 1, 2018, the U.S. Department of Defense (DoD) has required contractors to comply with National Institute of Standards and Technology (NIST) 800-171 to safeguard defense information. For a majority of DIB companies and suppliers who do not have sophisticated Chief Information Officer (CIO) nor Chief Information Security Officer (CISO) teams, processes, and capabilities, this requirement has been an unachievable gauntlet of cyber resilience controls and practices, resulting in a low rate of NIST 800-171 compliance across the entire DIB over the past several years. As with software development, DoD decided a maturity model approach would enable all companies to start a path to cyber resilience immediately, and over time mature, commensurate with the level of work or product they deliver. After months of development, on January 31, 2020, the 1.0 version of the Cybersecurity Maturity Model Certification (CMMC) was created as a foundational framework to certify the cybersecurity practices of contractors and suppliers, enabling a consistent approach for achieving cyber resilience across the approximately 330,000 companies in the DoD supply chain. On March 18, 2020, the DoD released version 1.02 of CMMC. CMMC will go into full effect by fall 2020.

Why was CMMC created? According to Katie Arrington (CISO for the DoD Acquisition Office), *"CMMC was created by the Department of Defense (DoD) for small businesses since in the past all defense contractors had to 'self-attest' for NIST 800-171 that they were in compliance with NIST controls before handling Federal Contract information and Controlled Unclassified Information (CUI). The DoD needed a centralized method for SMB's [small to mid-sized businesses] to get certified and provide a third-party assessment to audit companies."* The DoD is planning to use the new CMMC framework to assess and strengthen the cybersecurity posture of the DIB. Since the loss of CUI from the DIB increases the risk to our national and economic security, the Defense Sector must ensure the protection of CUI across all networks.

Who needs and does not need to achieve CMMC? Any organization that plans to conduct business with the DoD will be required to undergo an audit by an authorized CMMC C3PAO auditor before bidding, winning, and participating on a contract or subcontracting to a prime. In sections C and L of government request for proposals, it will state what CMMC level is required. All DOD contractors or

suppliers will need to achieve at a minimum CMMC Level 1, if they want to continue to do business with the DoD. Currently, Federal non-DoD contracts or companies that only produce Commercial-Off-The-Shelf (COTS) products do not require CMMC compliance.

How does an organization become certified? A non-profit, independent organization called the CMMC Accreditation Body (CMMC-AB) will accredit CMMC Third-Party Assessment Organizations (C3PAOs) and individual auditors. The CMMC-AB will establish a CMMC marketplace with a list of approved C3PAOs from which DIB companies will choose an approved auditing organization.

How does the CMMC framework function? CMMC has five different certification levels, presented below in Figure 1, that reflect the maturity and reliability of a government contractor's cybersecurity infrastructure to protect both sensitive and proprietary government information. The five levels build upon each other's technical and policy requirements, including the requirements from the previous level.

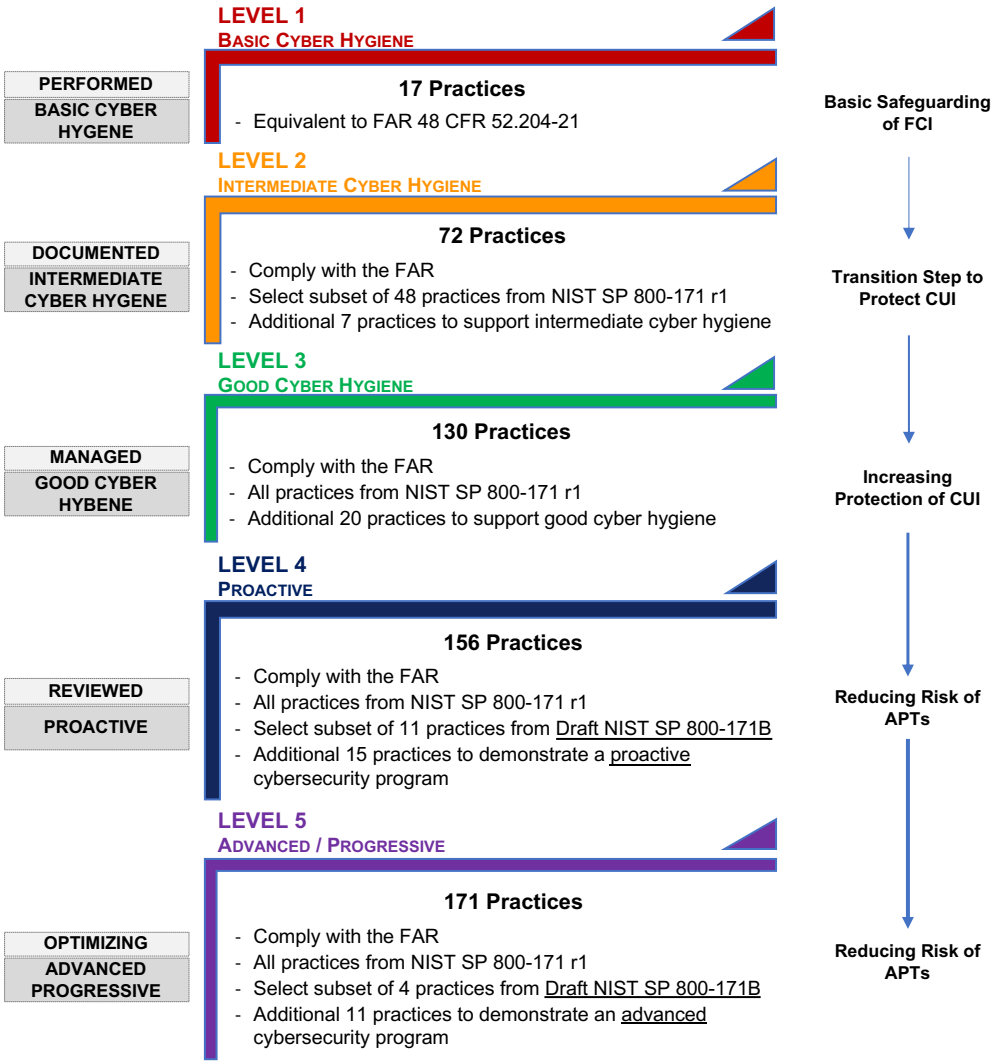


Figure 1 – CMMC Levels

Fast Track Your Path to CMMC

As with maturity level certifications, your path to CMMC certification can be daunting; especially for those DIB companies who do not have sophisticated CIO/CISO organizations internally. To support and help these companies as well as large enterprises fast-track their path to CMMC certification, WhiteHawk has developed and integrated the Cyber Risk Radar offering.

The WhiteHawk Cyber Risk Radar provides a rapid identification, prioritization and assessment of both cyber and business risk areas of focus to enable to development of an actionable mitigation plan. This is done for both the organization itself as well as for its supplier/vendors to cover the entire service ecosystem. Because WhiteHawk leverages risk related data sources that are publicly available and Artificial Intelligence (AI) and risk tradecraft-based analytics, we are able to provide these deliverables within a matter of days. By identifying gaps and mitigating risks prior the CMMC audit phase, organizations are able to remove the potential review cycles, thereby reducing the level of audit labor. Through the Whitehawk Cyber Risk Radar, we help group an organization's suppliers/vendors into multiple Tiers, mapping our capabilities efficiently to those tiers. Refer to Figure 1 below. In most cases, there is no need to invest the same level of effort across the entire supplier/vendor set. Through this approach, we are able to provide reference points that highlight areas of risk and options for remediations in a matter of days and provide actionable recommendations. For more information on how we can fast track your organizations path to CMMC, contact us at consultingservices@whitehawk.com.

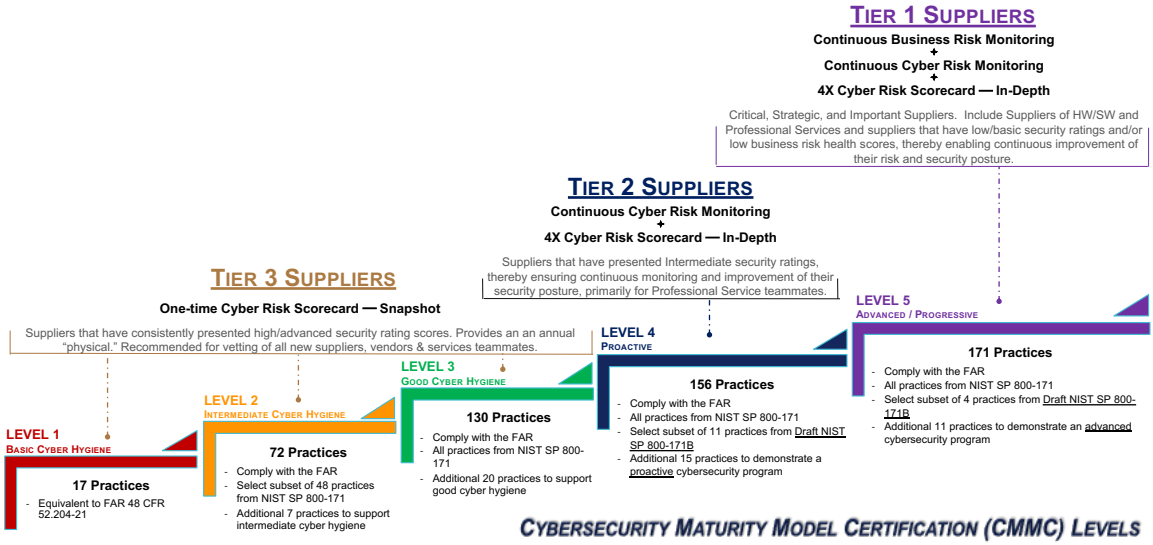


Figure 2 – Fast-Track to CMMC with WhiteHawk

Subsequent sections of this whitepaper provide a summarized reference of Security Domains and potential paths to each CMMC Level certification.

Cybersecurity Domains and Controls

The five CMMC levels are comprised of 17 cybersecurity domains, as depicted in Figure 3 below. Each CMMC control is categorized into one of these 17 domains.

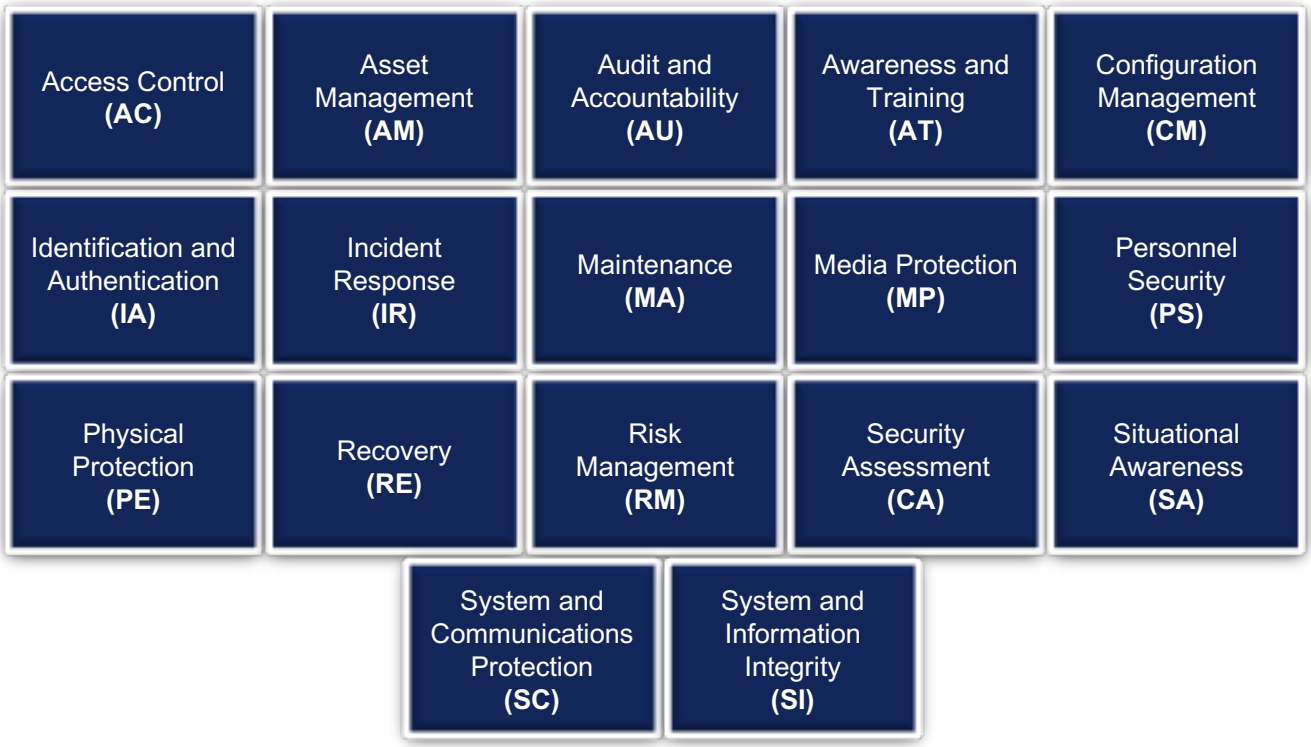


Figure 3 – Cybersecurity Domains

Fourteen of the 17 domains originate from the security-related areas in Federal Information Processing Standards (FIPS) publication 200, and the related security requirement families from NIST 800-171. The remaining three (3) security domains (AM, RE, and SA) come from other security frameworks. CMMC controls originate from the following frameworks: FAR 52.204-21, NIST 800-53 rev 4, NIST 800-171 rev2, NIST 800-171B, NIST Cybersecurity Framework, CERT Resiliency Management Model (RMM), International Organization for Standardization (ISO) 27002:2013, and Center for Internet Security (CIS) Critical Security Controls (CSC) 7.1.

It's important to understand that completing a CMMC audit does not equate to your organization being compliant with NIST 800-171. While NIST 800-171 focuses on the 110 CUI controls, note that it also requires compliance to an additional 63 Non-Federal Organization (NFO) controls. Therefore, to comply with NIST SP 800-171, your organization still needs to comply with both CUI and NFO controls.

A brief description of each security domain and its requirements are presented below. Remember these Controls primarily apply to your Information Technology systems, platforms, applications, devices and all data that they hold:

- **Access Control (AC) —** Technology and processes that provide each company employee with tailored access to certain information or features based upon their responsibilities. Access Control requires the following:
  - Establish system access requirements
  - Control internal and remote system access
  - Limit data access to only authorized users and processes
- **Asset Management (AM) —** The control over one's hardware and software inventory. It should identify, document, and manage the hardware and software your organization owns. This should include all computers (desktops and laptops), cell phones, tablets, servers, network equipment, and software licenses purchased for use on those devices.
- **Audit and Accountability (AU) —** A system to protect information during audit processing that holds appropriate parties responsible. Audit and Accountability requires the following:
  - Define audit requirements
  - Perform auditing and review/manage audit logs
  - Identify and protect audit information
- **Awareness and Training (AT) —** Security awareness training for all personnel. It should track and conduct security awareness activities and training.
- **Configuration Management (CM) —** Systems engineering process for handling changes to a system. It should establish and manage configurations.
- **Identification and Authentication (IA) —** An enforced process to verify the identities of users, procedures, or devices. It should grant access only to authenticated users.
- **Incident Response (IR) —** Plan in place to respond to a cybercrime, attack, event or disruption. Incident Response requires the following (or the hiring of a service provider who can perform the service):
  - Develop planned incident response methods
  - Detect and report events
  - Perform post incident reviews and test current incident response methods
- **Maintenance (MA) —** Routine system improvement and evaluation. It should manage the maintenance of IT systems.
- **Media Protection (MP) —** Focused on the protection of FCI and CUI. Media Protection requires the following:
  - Identify, protect, and control all physical and digital media containers.

- Sanitize media when no longer needed
- Protect media during transport

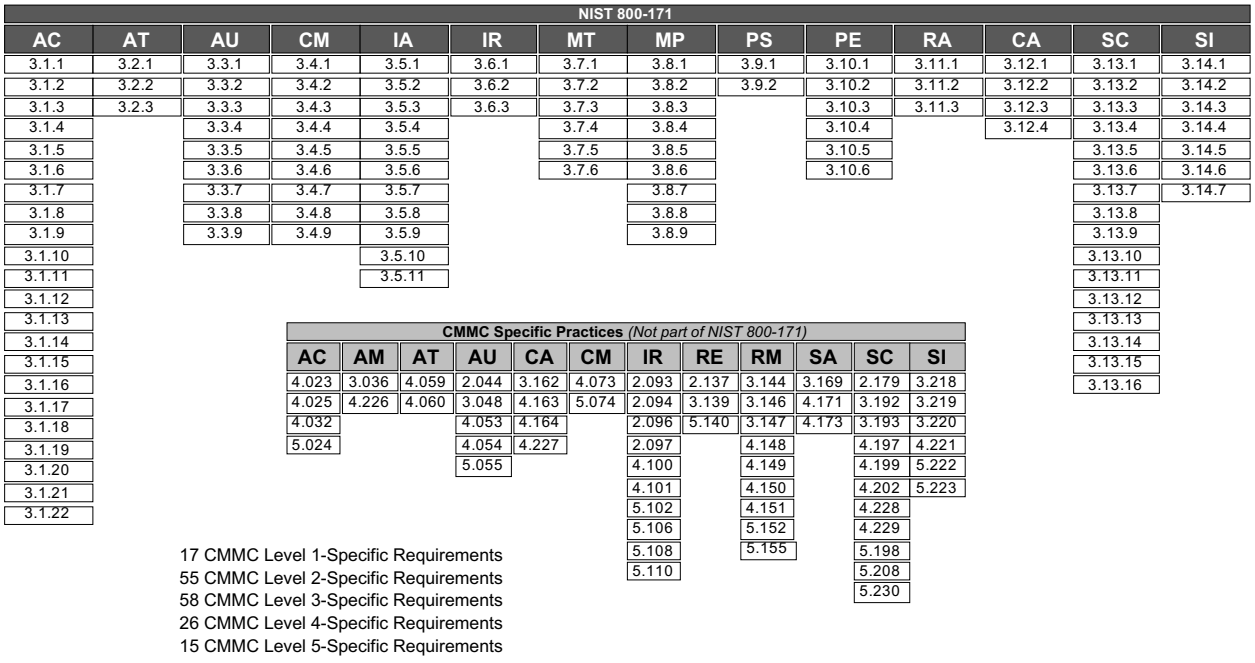
- **Personnel Security (PS) —** System to limit access to authorized users. It should limit and manages physical access from unauthorized guests.
- **Physical Protection (PE) —** Focus on protecting your physical environment: facilities, IT assets, work areas, and storage locations. It should limit and control physical access to company resources.
- **Recovery (RE) —** Data backup management. Recovery requires the following:
  - Manage data backups (should be daily or weekly)
  - Manage information security continuity- its confidentiality, integrity, and availability to only authorized personnel
- **Risk Management (RM) —** Supply chain vulnerability management. Risk Management requires the following:
  - Identify, evaluate, and manage company or organization risk
  - Manage supply chain, vendor and partner risk
- **Security Assessment (CA) —** Security testing. Security Assessment requires the following:
  - Define, develop, and manage system security plans and controls
  - Perform code reviews- Identify insecure pieces of code that may cause vulnerabilities, ultimately leading to an insecure application.
- **Situational Awareness (SA) —** Routine threat monitoring. It should implement threat monitoring. (or the hiring of a service provider who can perform the service for you – SOC as a service):
- **System and Communications Protection (SC) —** Up-to-date software protection. System and Communications Protection requires the following (or the hiring of a service provider who can perform the service):
  - Define security requirements for systems and communications
  - Control communications at system boundaries
- **System and Information Integrity (SI) —** Security strength. System and Information Integrity requires the following(or the hiring of a service provider who can perform the service):
  - Identify and manage information system flaws including malicious content
  - Perform routine network and system monitoring
  - Implement advanced email protections

Requirements for Each CMMC Level

As you start the CMMC journey, understand your current security posture, internal organizational practices, and establish a maturity baseline. This will guide you in the development a plan that is prioritized, actionable and achievable in a timely and cost-efficient manner. Figure 4 below summarizes the control compliance requirements for each level. Subsequent sections go into details of each CMMC Level requirements.

Figure 4 – CMMC Levels and Associated Control Compliance Requirements

	Practice	# Level-Specific Controls	# of Total Controls
Level 1	Basic Cyber Hygiene	17	17
Level 2	Intermediate Cyber Hygiene	55	72
Level 3	Good Cyber Hygiene	58	130
Level 4	Proactive	26	156
Level 5	Advanced/Progressive	15	171



WHITEHAWK

Path to CMMC Level 1

CMMC Level 1's objective is to safeguard Federal Contract Information (FCI) and checks if processes are being performed. Features of Level 1 Requirements are:

- **Practice**: Basic Cyber Hygiene
- **Total Number of Controls**: 17
- **Summary**: Level 1 has 17 Controls, refer to Figure 4 below, that a company should be doing every day, which are basic cyber essentials mapped to FAR 52.204-21 and 17 NIST 800-171 requirements. CMMC Level 1 covers 17% of NIST 800-171 CUI Controls.

Katie Arrington states the CMMC Audit for this level is an hour to less than two hours; and costs for auditing will be under $3,000 USD. Audits are valid for three years. It is estimated that approximately 285,000 companies are expected to be certified at this level.

Note that an organization may be able to only perform these practices and may or may not have them documented. Process Maturity is not assessed for Level 1.

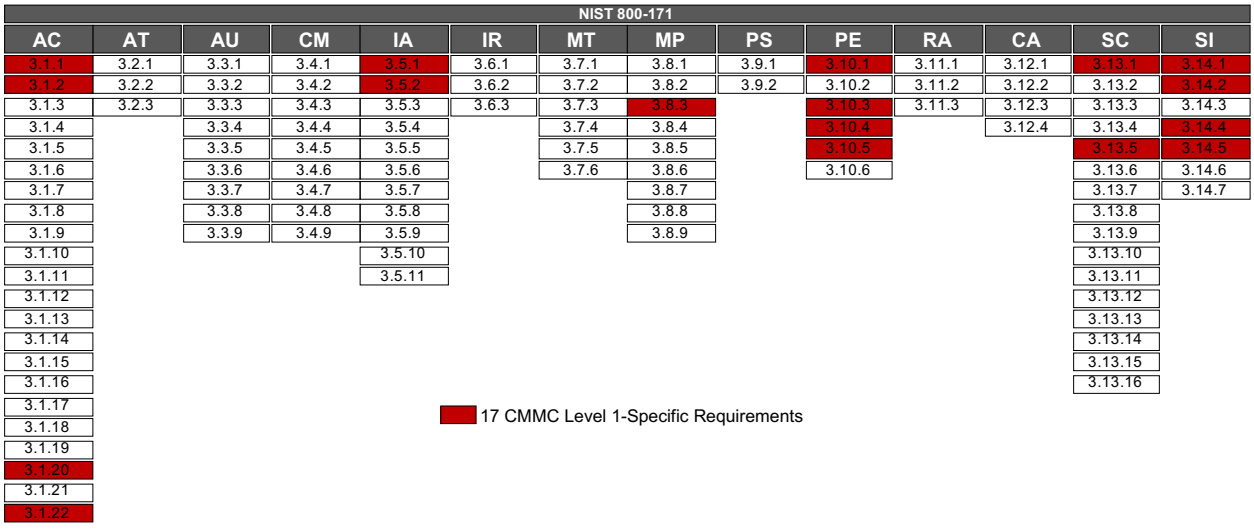


Figure 5 – CMMC Level 1 Controls

Figure 6 below details each control requirement to achieving CMMC Level 1 compliance. WhiteHawk includes additional context with Cyber Product Categories and Vendor Solution Options. For a complimentary Path to CMMC consultation with a WhiteHawk Cyber Analyst, please visit us at www.whitehawk.com.

Figure 6 – CMMC Level 1 Controls, Requirements, and WhiteHawk's Solution Options

	Security Control	Formal Requirement	WhiteHawk Product Categories	Vendor Solutions**
1	CMMC AC.1.001	*"Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems)."*	Application Security Access Control	AppSec Labs, Flexera, Votiro, SolarWinds, Roboform, OneLogin
2	CMMC AC.1.002	*"Limit information system access to the types of transactions and functions that authorized users are permitted to execute."*	Application Security Access Control	AppSec Labs, Flexera, Votiro, SolarWinds, Roboform, OneLogin
3	CMMC AC.1.003	*"Verify and control/limit connections to and use of external information systems."*	Encrypted Communication Virtual Private Network	SaferNet, Preveil, VTS, VYPR
4	CMMC AC.1.004	*"Control information posted or processed on publicly accessible information systems."*	Web Filter and Training Data Leak Prevention	Cyxtera, GFI Software
5	CMMC IA.1.076	*"Identify information system users, processes acting on behalf of users, or devices."*	Application Security Access Control	AppSec Labs, Flexera, Votiro, SolarWinds, Roboform, OneLogin
6	CMMC IA.1.007	*"Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems."*	Web Filter and Training	Roboform, OneLogin
7	CMMC MP.1.118	*"Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse."*	Training & Data Leak Prevention	Secudrive, Mimecast
8	CMMC PE.1.131	*"Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals."*	Physical Security	Internal Client Controls
9	CMMC PE.1.132	*"Escort visitors and monitor visitor activity."*	Physical Security	Internal Client Controls

	Security Control	Formal Requirement	WhiteHawk Product Categories	Vendor Solutions**
10	CMMC PE.1.133	*"Maintain audit logs of physical access."*	Physical Security	Internal Client Controls
11	CMMC PE.1.134	*"Control and manage physical access devices."*	Physical Security	Internal Client Controls
12	CMMC SC.1.175	*"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. "*	Encrypted Communication Virtual Private Network	PreVeil, SaferNet, MimeCast, Boldon James
13	CMMC SC.1.176	*"Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks."*	Encrypted Communication Virtual Private Network	PreVeil, SaferNet, MimeCast, Boldon James
14	CMMC SI.1.210	*"Identify, report, and correct information and information system flaws in a timely manner."*	AntiMalware Access Control	GFI Software, MicroFocus, Mimecast, Sophos, Symantec, McAfee, TrendMicro
15	CMMC SI.1.211	*"Provide protection from malicious code at appropriate locations within organizational information systems."*	AntiMalware Access Control	GFI Software, MicroFocus, Mimecast, Sophos, Symantec, McAfee, TrendMicro
16	CMMC.SI.1.212	*"Update malicious code protection mechanisms when new releases are available."*	AntiMalware Access Control	GFI Software, MicroFocus, Mimecast, Sophos, Symantec, McAfee, TrendMicro
17	CMMC SI.1.213	*"Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed."*	AntiMalware Access Control	GFI Software, MicroFocus, Mimecast, Sophos, Symantec, McAfee, TrendMicro

Path to CMMC Level 2

CMMC Level 2's objective is To Serve as a Transition Step in Cybersecurity Maturity Progression to Protect CUI and checks if processes are being documented. Features of Level 2 Requirements are:

- **Practice**: Intermediate Cyber Hygiene
- **Total Number of Controls**: 72
- **Summary**: CMMC Level 2 requires 55 additional controls, plus the 17 controls from CMMC Level 1 totaling to 72 controls. Refer to Figure 7 below. This is where the protection of CUI is introduced and initiated. 65 of these controls are directly from NIST 800-171 requirements plus seven (7) other CMMC specific controls. A CMMC Level 2 audit covers approximately 59% of all NIST 800-171 CUI Controls.

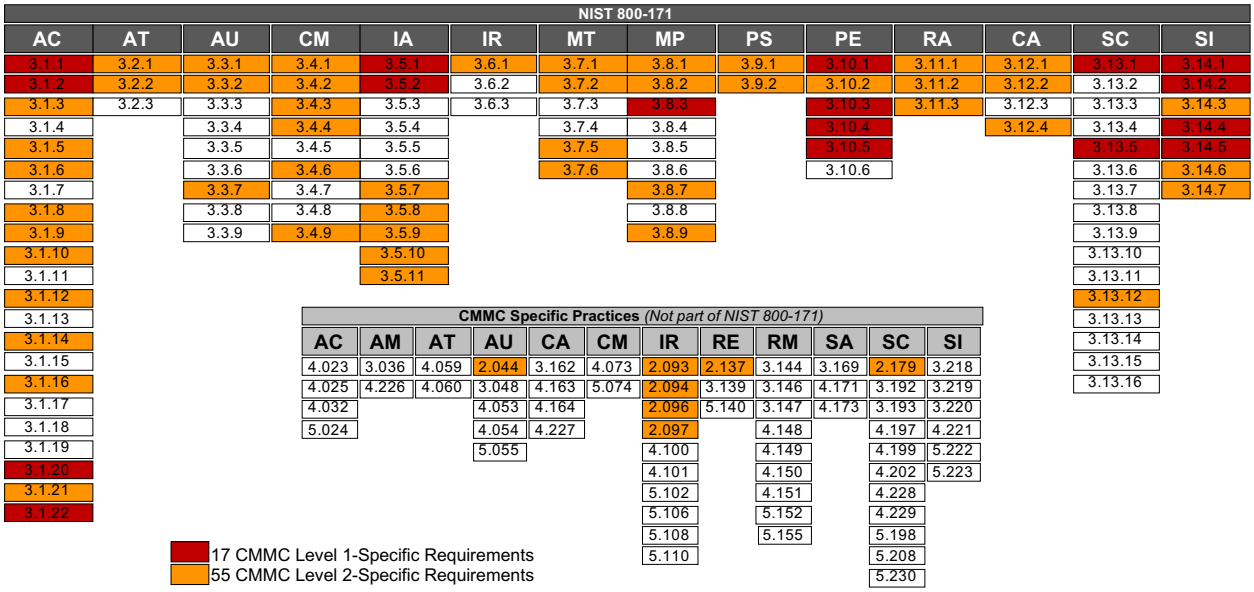


Figure 7 – CMMC Level 2 Controls

According to the DoD, no contracts will require CMMC Level 2 since it is seen as a bridge to CMMC Level 3. However, if a company wishes to get to Level 3, it will need to satisfy all Level 2 controls.

Refer to Appendix A – CMMC Level 2 Controls and Requirements for additional details of each control and associated requirement.

Path to CMMC Level 3

CMMC Level 3's objective is to Protect CUI and checks if processes are being managed. Features of Level 3 Requirements are:

- **Practice**: Good Cyber Hygiene
- **Total Number of Controls**: 130
- **Summary**: CMMC Level 3 requires 58 additional controls to the 72 controls from Level 2 for a total of 130 controls that must be met. A CMMC Level 3 audit covers 100% of all the 110 NIST 800-171 controls, plus 20 CMMC specific controls. Refer to Figure 8 below.

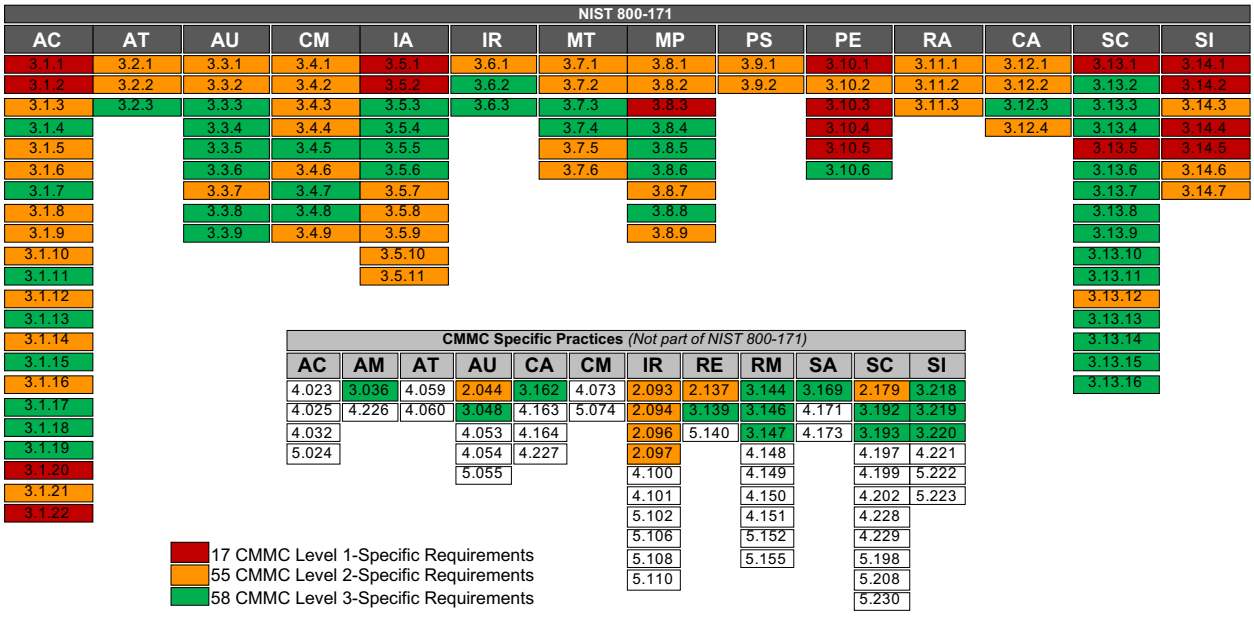


Figure x – CMMC Level 8 Controls

Any company that handles CUI in any way is required to achieve Level 3 compliance. Refer to Appendix B – CMMC Level 3 Controls and Requirements for additional details of each control and associated requirement.

Path to CMMC Level 4

CMMC Level 4's objective is to Protect CUI and Reduce Risk of Advanced Persistent Threats (APTs) and checks if processes are being reviewed. Features of Level 4 Requirements are:

- **Practice**: Proactive
- **Total Number of Controls**: 156
- **Summary**: CMMC Level 4 adds 26 controls to the 130 controls from Level 3 for a total of 156 controls that must be met. Refer to Figure 9 below.

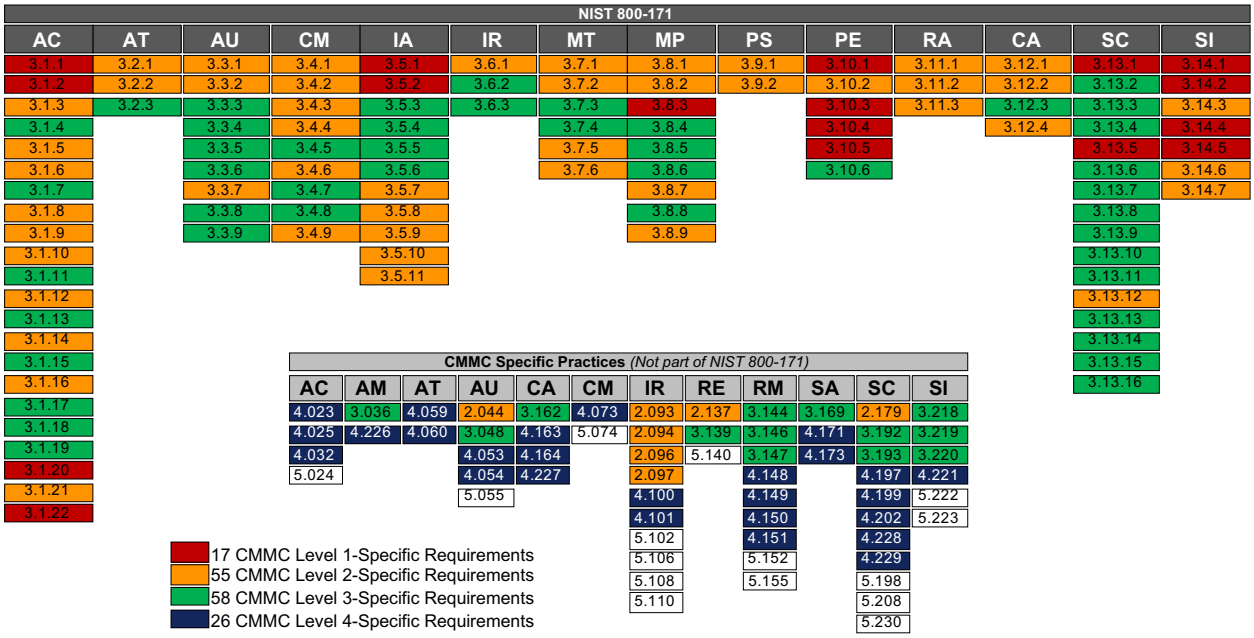


Figure 9 – CMMC Level 4 Controls

Refer to Appendix C – CMMC Level 4 Controls and Requirements for additional details of each control and associated requirement.

Path to CMMC Level 5

CMMC Level 5's objective is to Protect CUI and Reduce Risk of APTs and checks if processes are being optimized. Features of Level 5 Requirements are:

- **Practice**: Advanced/Proactive
- **Total Number of Controls**: 171
- **Summary**: CMMC Level 5 adds 15 controls to the 156 controls from Level 4 for a total of 171 controls that must be met. Refer to Figure 10 below.

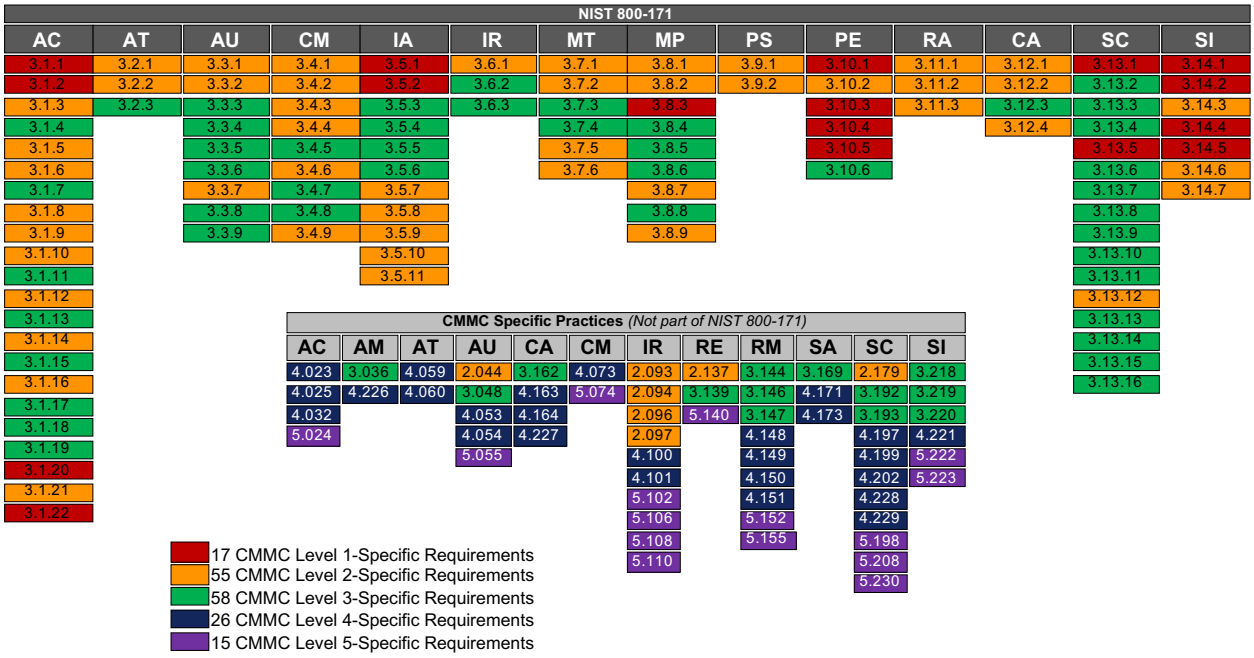


Figure 10 – CMMC Level 5 Controls

Refer to Appendix D – CMMC Level 5 Controls and Requirements for additional details of each control and associated requirement.

Definitions

Term	Definition
Controlled Unclassified Information (CUI)	Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.
CMMC Third-Party Assessment Organizations (C3PAOs)	CMMC C3PAO's are authorized to manage the assessment process. Each C3PAO must be certified by the CMMC-Accreditation Body (AB) prior to deploying its assessors into the field.
Defense Industrial Base (DIB)	The Defense Industrial Base Sector is the worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet US military requirements.
Federal Contract Information (FCI)	Information not intended for public release that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government.
Removable Media	Portable data storage medium that can be added to or removed from a computing device or network. Examples include, but are not limited to optical discs (CD, DVD, Blu-ray); external/removable hard drives; external/removable Solid-State Disk (SSD) drives; magnetic/optical tapes; flash memory devices (USB, eSATA, Flash Drive, Thumb Drive); flash memory cards (Secure Digital, CompactFlash, Memory Stick, MMC, xD).

References

“Assessing Security Requirements for Controlled Unclassified Information,” 2/20/2018
https://csrc.nist.gov/publications/detail/sp/800-171a/final

“CMMC Appendices Version 1.02,” March 18, 2020
https://www.acq.osd.mil/cmmc/docs/CMMC_Appendices_V1.02_20200318.pdf

"CMMC Briefing - Updates from the Front Lines with Katie Arrington (until 12:34)," 4/14/2020
https://www.youtube.com/watch?v=CCYS3ntoeUU&feature=youtu.be&t=60

“CMMC Contractor requirements" 10/6/2020
https://governmentcontractsnavigator.com/2020/10/06/new-department-of-defense-regulations-clarify-contractors-responsibilities-to-comply-with-nist-sp-800-171-and-cmmc-requirements/

“CMMC FAQ’s”
https://www.acq.osd.mil/cmmc/faq.html

“CMMC Level 1 Certification and preparation (How-to),” 5/25/2020
https://www.cmmcaudit.org/cmmc-level-1-certification-and-preparation-how-to/

“CMMC Level 2 – Building a Bridge to Level 3,” 4/21/2020
https://beinetworks.com/cmmc-level-2/

"CMMC Version 1.02 Final Draft," 3/18/2020
https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf

“Cybersecurity Maturity Model Certification (CMMC) v1.02 & NIST 800-171 rev2 Compliance”
https://www.complianceforge.com/cybersecurity-maturity-model-certification-cmmc/

“Cybersecurity Maturity Model Certification Domains Explained"
https://www.cybersaint.io/blog/cmmc-domains-explained

“FIPS PUB 140-2: Security Requirements for Cryptographic Modules,” 5/25/2001
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

“CMMC Third-Party Assessment Organizations”
https://www.cmmcab.org/c3pao-lp

“Katie Arrington, CISO for DoD Acquisition Office, Named to 2020 Wash100 for Advancing New Cyber Framework, Culture Change.” 2/13/2020
http://www.govconwire.com/2020/02/katie-arrington-ciso-for-dod-acquisition-office-named-to-2020-wash100-for-advancing-new-cyber-framework-culture-change/

“NIST MEP Cybersecurity Self-Assessment Handbook for Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements,” 11/2017
https://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf

"NIST SP 800-171," 2/2020
https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

“The CMMC: Answers About What to Expect and What it Means to You,” 1/14/2020
https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/the-cmmc-answering-the-what-when-and-why/

“The Cybersecurity Maturity Model Certification Explained: What Defense Contractors Need to Know,” 4/8/2020
https://www.csoonline.com/article/3535797/the-cybersecurity-maturity-model-certification-explained-what-defense-contractors-need-to-know.html

“Understanding Cybersecurity Maturity Model Certification (CMMC),” 1/3/2020
https://securityboulevard.com/2020/01/understanding-cybersecurity-maturity-model-certification-cmmc/

“What is the Cybersecurity Maturity Model Certification (CMMC)?” 12/12/2019
https://info.summit7systems.com/blog/cmmc

Appendix A — CMMC Level 2 Controls & Requirements

CMMC Level 2 Controls & Requirements			
#	**Security Control**	**Formal Requirement**	**How to Pass**
1	CMMC AC.2.016 (NIST 800-171 Rev2 3.1.3)	*"Control the flow of CUI in accordance with approved authorizations."*	Having solutions to control the flow of system data, as well as documenting information flow control. This can include implementing firewalls and encryption to block outside traffic and restrict web requests to the internet that are not from the internal web proxy server.
2	CMMC AT.2.056 (NIST 800-171 Rev2 3.2.1)	*"Ensure that managers, system administrators and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards and procedures related to the security of those systems."*	Having employees complete annual training about their roles and responsibilities pertaining to information security and procedures related to the security of the system, as well completing security awareness training.
3	CMMC AT.2.057 (NIST 800-171 Rev2 3.2.2)	*"Ensure that personnel are trained to carry out their assigned information security- related duties and responsibilities."*	Same as above, but with an emphasis for employees with security specific roles and more technical training such as identifying suspicious email or web communications.
4	CMMC AU.2.042 (NIST 800-171 Rev2 3.3.1)	*"Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation and reporting of unlawful or unauthorized system activity."*	Having system provide alert functions and performing audit analysis/review through mechanisms in place. Retaining information audit records between 30 days to 1 year depending on data.
5	CMMC AU.2.041 (NIST 800-171 Rev2 3.3.2)	*"Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions."*	Keeping track of network activity to individual users and being able to trace accountable users for unauthorized actions to protect against a user denying having performed an action.
6	CMMC AU.2.043 (NIST 800-171 Rev2 3.3.7)	*"Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records."*	Make the system use internal system clocks to generate time stamps for audit records. Having those time stamps be mapped to Coordinated Universal Time (UTC) and compare system clocks with Network Time Protocol (NTP) servers that synchronizes the clocks on a defined frequency.
7	CMMC AU.2.044	*"Review Audit Logs."*	Review system and audit logs to keep track of what users have performed activities.

CMMC Level 2 Controls & Requirements			
#	**Security Control**	**Formal Requirement**	**How to Pass**
8	CMMC CM.2.061 (NIST 800-171 Rev2 3.4.1)	*"Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware and documentation) throughout the respective system development life cycles."*	Having baseline configurations documented and maintained for each information system type, as well as updating these as needed to accommodate security risks or software changes and having it approved by a CISO or equivalent. Using a system development lifecycle methodology that includes security considerations.
9	CMMC CM.2.064 (NIST 800-171 Rev2 3.4.2)	*"Establish and enforce security configuration settings for information technology products employed in organizational systems."*	Having security baseline configurations that reflect the most restrictive appropriate settings and documenting any changes or deviations.
10	CMMC CM.2.065 (NIST 800-171 Rev2 3.4.3)	*"Track, review, approve or disapprove and log changes to organizational systems."*	Documenting changes to the system that are authorized by company management, auditing these changes, and tracking changes through an IT service management system or equivalent tracking service.
11	CMMC CM.2.066 (NIST 800-171 Rev2 3.4.4)	*"Analyze the security impact of changes prior to implementation."*	Testing changes that affect the system security requirements prior to the implementation, the effectiveness of the changes, and ensuring that these changes are compliance- approved and documented.
12	CMMC CM.2.062 (NIST 800-171 Rev2 3.4.6)	*"Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities."*	Configuring system to exclude any function not needed in the operational environment and having system employ processing components that have minimal data storage such as diskless nodes. In certain systems, having it deliver one function when practical.
13	CMMC CM.2.063 (NIST 800-171 Rev2 3.4.9)	"*Control and monitor user-installed software."*	Placing user controls to prohibit the installation of unauthorized software, ensuring all software use on the system is approved, and having user-installed software operated with limited privileges.
14	CMMC IA.2.078 (NIST 800-171 Rev2 3.5.7)	*"Enforce a minimum password complexity and change of characters when new passwords are created."*	Require employees to have at least 12 characters in their passwords and include numbers, upper/lowercase, and special characters.
15	CMMC IA.2.079 (NIST 800-171 Rev2 3.5.8)	*"Prohibit password reuse for a specified number of generations."*	Do not let employees re-use previous passwords.
16	CMMC IA.2.080 (NIST 800-171 Rev2 3.5.9)	*"Allow temporary password use for system logons with an immediate change to a permanent password."*	Requiring employees to create a new password during the hiring process from their initial generated passwords. Ensuring that temporary password activation links are sent to employees when a password change is required and only used for a password reset.

CMMC Level 2 Controls & Requirements			
#	**Security Control**	**Formal Requirement**	**How to Pass**
17	CMMC IA.2.081 (NIST 800-171 Rev2 3.5.10)	*"Store and transmit only cryptographically-protected passwords."*	Having passwords that cannot be reverse encrypted, using hashes and salts, and making sure passwords are encrypted in storage and in transmission.
18	CMMC IA.2.082 (NIST 800-171 Rev2 3.5.11)	*"Obscure feedback of authentication information."*	When a user types authentication information such as a password, it should show up as dots on the computer screen. Also, if a user inputs a wrong field of information. It should not specify that it was "Wrong password", or "Wrong username."
19	CMMC IR.2.092 (NIST 800-171 Rev2 3.6.1)	*"Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery and user response activities."*	Establishing an incident response policy that specifically outlines requirements for handling incidents involving CUI that include preparation, detection, analysis, containment, eradication, and recovery.
20	CMMC IR.2.093	*"Detect and report events."*	Have a system set in place such as an Intrusion Detection system to detect and report suspicious activity.
21	CMMC IR.2.094	*"Analyze and triage events to support event resolution and incident declaration."*	Have a plan set in place to categorize and prioritize events and handle them as appropriate.
22	CMMC IR.2.096	*"Develop and implement responses to declared incidents according to pre- defined procedures."*	Write procedures ahead of time when responding to incidents depending on the type of incident. Responses should prevent or contain the impact of an incident while it is occurring or shortly after.
23	CMMC IR.2.097	*"Perform root cause analysis on incidents to determine underlying causes."*	Examining the causes of the event or incident and how your organization responded to it by looking at administrative, technical, and physical control weaknesses that may have allowed the incident to occur. Making improvements after examining by updating plans.
24	CMMC MA.2.111 (NIST 800-171 Rev2 3.7.1)	"Perform maintenance on organizational systems."	Managing IT system maintenance tools such as diagnostics and patching tools and supporting systems and devices per manufacturer recommendations. Maintenance should be performed on the system and has to be approved by management.
25	CMMC MA.2.112 (NIST 800-171 Rev2 3.7.2)	*"Provide controls on the tools, techniques, mechanisms and personnel used to conduct system maintenance."*	Placing controls that limit the tools, and resources that employees use to maintain the system and devices. This may include authorized tools, employees, or techniques and settings.
26	CMMC MA.2.113 (NIST 800-171 Rev2 3.7.5)	*"Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete."*	Requiring multifactor authentication for remote access to a system and ensuring that the connections are terminated when the session is completed.

CMMC Level 2 Controls & Requirements			
#	**Security Control**	**Formal Requirement**	**How to Pass**
27	CMMC MA.2.114 (NIST 800-171 Rev2 3.7.6)	*"Supervise the maintenance activities of personnel without required access authorization."*	Ensuring all activities of maintenance personnel are monitored and that the company has defined methods for supervision.
28	CMMC MP.2.119 (NIST 800-171 Rev2 3.8.1)	*"Protect (e.g., physically control and securely store) system media containing Federal Contract Information, both paper and digital."*	Having responsible parties for the data in the systems document and ensure proper authorization controls for data in media and print, securely storing system media in protected areas, making sure only approved individuals have access to media from CUI systems, and removing the audit log of any media from these systems.
29	CMMC MP.2.120 (NIST 800-171 Rev2 3.8.2)	*"Limit access to CUI on system media to authorized users."*	Managing all CUI systems under least access rules and limiting CUI media access to authorized users.
30	CMMC MP.2.121 (NIST 800-171 Rev2 3.8.7)	*"Control the use of removable media on system components."*	Restricting the use of writable and removable media on the system.
31	CMMC RE.2.138 (NIST 800-171 Rev2 3.8.9)	*"Protect the confidentiality of backup CUI at storage locations."*	Encrypting data backups on media before removal from a secured facility, protecting the confidentiality and integrity of backup information at the storage location, and having cryptographic mechanisms that comply with FIPS 140-2 (Security Requirements for Cryptographic Modules.)
32	CMMC RE.2.137	*"Regularly perform and test data back-ups."*	Back up organizational data often. Test these backups by verifying that the operating system, application, and data are intact and functional.
33	CMMC PS.2.127 (NIST 800-171 Rev2 3.9.1)	*"Screen individuals prior to authorizing access to organizational systems containing CUI."*	Ensuring that individuals are screened before granting them access to any systems that contain CUI.
34	CMMC PS.2.128 (NIST 800-171 Rev2 3.9.2)	*"Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers."*	Disabling information system access prior to employee termination, retrieving all company information and property from terminated or transferred employee, reviewing electronic and physical access permissions when employees are reassigned or transferred.
35	CMMC PE.2.135 (NIST 800-171 Rev2 3.10.2)	*"Protect and monitor the physical facility and support infrastructure for organizational systems"*	Having the facility manager review the location and type of physical security in use such as locks, card readers, etc., and evaluating the suitability for the company's needs.
36	CMMC RM.2.141 (NIST 800-171 Rev2 3.11.1)	*"Periodically assess the risk to organizational operations (including mission, functions, image or reputation), organizational assets and individuals, resulting from the operation of organizational systems and the associated processing, storage or transmission of CUI."*	Establishing a risk management policy, conducting initial and periodic risk assessments, documenting and assessing changes in use or infrastructure.

CMMC Level 2 Controls & Requirements			
#	**Security Control**	**Formal Requirement**	**How to Pass**
37	CMMC RM.2.142 (NIST 800-171 Rev2 3.11.2)	*"Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified."*	Performing vulnerability scanning periodically for common and new vulnerabilities. Creating reports regarding the scans for company management and keeping documentation.
38	CMMC RM.2.143 (NIST 800-171 Rev2 3.11.3)	*"Remediate vulnerabilities in accordance with risk assessments."*	Creating an action plan for remediation, acceptance or avoidance upon recognition of any vulnerability. Prioritizing high vulnerabilities and including a reasonable time frame for implementation.
39	CMMC CA.2.158 (NIST 800-171 Rev2 3.12.1)	*"Periodically assess the security controls in organizational systems to determine if the controls are effective in their application."*	Conducting periodic security assessments to ensure that security controls are implemented correctly and meet security requirements. This includes vulnerability scanning, pen testing, log reviews, and speaking with company employees.
40	CMMC CA.2.159 (NIST 800-171 Rev2 3.12.2)	*"Develop and implement plans of action (e.g., POA&M) designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems."*	Developing an action plan to remediate identified weaknesses or deficiencies that designates remediation dates for each item.
41	CMMC CA.2.157 (NIST 800-171 Rev2 3.12.4)	*"Develop, document and periodically update System Security Plans (SSPs) that describe system boundaries, system environments of operation, how security requirements are implemented and the relationships with or connections to other systems."*	Ensuring that security plans are consistent with the company's enterprise architecture, authorization boundaries, operational context, operational environment, and security requirements.
42	CMMC SC.2.178 (NIST 800-171 Rev2 3.13.12)	*"Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device."*	Configuring collaborative computing devices so they cannot be remotely activated, having users notified when collaborative computing devices are in use.
43	CMMC SC.2.179	*"Use encrypted sessions for the management of network devices."*	When accessing devices over the network, you should use a secure encryption method such as Secure Shell (SSH).
44	CMMC SI.2.214 (NIST 800-171 Rev2 3.14.3)	*"Monitor system security alerts and advisories and take action in response."*	Having the company receive security alerts, advisories, and directives from reputable external organizations, responding to alerts in a timely manner, and generating internal security alerts.
45	CMMC SI.2.216 (NIST 800-171 Rev2 3.14.6)	*"Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks."*	Monitor system to detect attacks as well as unauthorized local, network, and remote connections. Deploy monitoring devices to collect information and monitor inbound and outbound communications for unusual activity.
46	CMMC SI.2.217 (NIST 800-171 Rev2 3.14.7)	"Identify unauthorized use of organizational systems."	Monitoring the system to identify unauthorized access and use and log monitoring.

CMMC Level 2 Controls & Requirements			
#	**Security Control**	**Formal Requirement**	**How to Pass**
47	CMMC AC.2.007 (NIST 800-171 Rev2 3.1.5)	*"Employ the principle of least privilege, including for specific security functions and privileged accounts."*	Only granting enough privileges to users to allow them to do their jobs. Restricting access to privileged functions and security information to authorized employees.
48	CMMC AC.2.008 (NIST 800-171 Rev2 3.1.6)	*"Use non-privileged accounts or roles when accessing nonsecurity functions."*	Having users with multiple account log ons with the least privileged account when not performing privileged functions, making sure that this can be described or demonstrated.
49	CMMC AC.2.009 (NIST 800-171 Rev2 3.1.8)	*"Limit unsuccessful logon attempts."*	Lock the computer or account after a certain number of failed log on attempts.
50	CMMC AC.2.010 (NIST 800-171 Rev2 3.1.10)	*"Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity."*	Configuring the system to lock sessions after a predetermined period of inactivity, using pattern hiding displays when sessions are locked, giving users the option to lock sessions for temporary absence.
51	CMMC AC.2.011 (NIST 800-171 Rev2 3.1.16)	*"Authorize wireless access prior to allowing such connections."*	Approving the use of wireless technologies by company management, having established guidelines for the use of wireless technologies, and monitoring wireless access to the system.
52	CMMC AC.2.013 (NIST 800-171 Rev2 3.1.12)	*"Monitor and control remote access sessions."*	Running network and system monitoring applications to monitor remote system access and log, accordingly, controlling remote access by running only necessary applications, using firewalls and end-to-end encryption.
53	CMMC AC.2.015 (NIST 800-171 Rev2 3.1.14)	*"Route remote access via managed access control points."*	Allowing remote access only by authorized methods, maintained by one department, and route all remote access through a limited number of managed access control points.
54	CMMC AC.2.005 (NIST 800-171 Rev2 3.1.9)	*"Provide privacy and security notices consistent with applicable Controlled Unclassified Information (CUI) rules."*	Having log on screen display notices upon initial login, display the system use information before granting access, referencing monitoring, recording, or auditing consistent with privacy accommodation.
55	CMMC AC.2.006 (NIST 800-171 Rev2 3.1.21)	*"Limit use of portable storage devices on external systems."*	Placing restrictions on the use of portable storage devices such as thumb drives, imposing restrictions on authorized individuals regarding the use of company controlled removable media on external systems.

Appendix B — CMMC Level 3 Controls & Requirements

CMMC Level 3 Controls & Requirements			
#	**Security Control**	**Formal Requirement**	**How to Pass**
1	CMMC AC.3.017 (NIST 800-171 Rev2 3.1.4)	*"Separate the duties of individuals to reduce the risk of malevolent activity without collusion."*	Divide responsibilities among individuals.
2	CMMC AC.3.018 (NIST 800-171 Rev2 3.1.7)	*"Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs."*	Only let those with authorized access perform privileged functions with classified and sensitive information.
3	CMMC AC.3.019 (NIST 800-171 Rev2 3.1.11)	*"Terminate (automatically) user sessions after a defined condition."*	Have a reaction to end a user's session when a condition set in place is triggered.
4	CMMC AC.3.014 (NIST 800-171 Rev2 3.1.13)	*"Employ cryptographic mechanisms to protect the confidentiality of remote access sessions."*	Enable employees to establish configurations to protect the confidential needs of work done remotely.
5	CMMC AC.3.021 (NIST 800-171 Rev2 3.1.15)	*"Authorize remote execution of privileged commands and remote access to security-relevant information."*	Restrict those who have privileged access, including when they can access and from where.
6	CMMC AC.3.012 (NIST 800-171 Rev2 3.1.17)	*"Protect wireless access using authentication and encryption."*	Require passwords before allowing access to wireless networks.
7	CMMC AC.3.020 (NIST 800-171 Rev2 3.1.18)	*"Control connection of mobile devices."*	Only allow authorized mobile devices to connect to wireless networks.
8	CMMC AC.3.022 (NIST 800-171 Rev2 3.1.19)	*"Encrypt CUI on mobile devices and mobile computing platforms."*	Ensure CUI is disguised on mobile platforms.
9	CMMC AT.3.058 (NIST 800-171 Rev2 3.2.3)	*"Provide security awareness training on recognizing and reporting potential indicators of insider threat."*	Enable entire employee base to report and recognize insider threats through routine security awareness training.
10	CMMC AU.3.045 (NIST 800-171 Rev2 3.3.3)	*"Review and update logged events."*	Keep events updated and frequently review and verify them.
11	CMMC AU.3.046 (NIST 800-171 Rev2 3.3.4)	*"Alert in the event of an audit logging process failure."*	Report any failures in logging the audit process.
12	CMMC AU.3.051 (NIST 800-171 Rev2 3.3.5)	*"Correlate audit record review, analysis and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious or unusual activity."*	Have an established reviewing and reporting process for incident response and suspicious activity.

CMMC Level 3 Controls & Requirements			
#	**Security Control**	**Formal Requirement**	**How to Pass**
13	CMMC AU.3.052 (NIST 800-171 Rev2 3.3.6)	*"Provide audit record reduction and report generation to support on-demand analysis and reporting."*	Implement a SIEM with built-in AI or rules that will be able to filter your audit logs into meaningful reports.
14	CMMC AU.3.049 (NIST 800-171 Rev2 3.3.8)	*"Protect audit information and audit logging tools from unauthorized access, modification and deletion."*	Have secure backups in place to protect information from being manipulated or removed.
15	CMMC AU.3.050 (NIST 800-171 Rev2 3.3.9)	*"Limit management of audit logging functionality to a subset of privileged users."*	Limit access to audit logging functionality to authorized users.
16	CMMC CM.3.067 (NIST 800-171 Rev2 3.4.5)	*"Define, document, approve and enforce physical and logical access restrictions associated with changes to organizational systems."*	Have a policy in place that defines restrictions and requirements for logical access and update it regularly.
17	CMMC CM.3.068 (NIST 800-171 Rev2 3.4.7)	*"Restrict, disable or prevent the use of nonessential programs, functions, ports, protocols and services."*	Restrict programs to only those essential to the desired functions; to minimize outside threats.
18	CMMC CM.3.069 (NIST 800-171 Rev2 3.4.8)	*"Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software."*	Explicitly deny all but authorized users to access certain software.
19	CMMC IA.3.083 (NIST 800-171 Rev2 3.5.3)	*"Use multi-factor authentication for local and network access to privileged accounts and for network access to non-privileged accounts."*	Enable multifactor authentication across all authorized users before granting network access.
20	CMMC IA.3.084 (NIST 800-171 Rev2 3.5.4)	*"Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts."*	Promote policies such as Transport Layer Security (TLS) before providing network access to any accounts.
21	CMMC IA.3.085 (NIST 800-171 Rev2 3.5.5)	*"Prevent the reuse of identifiers for a defined period."*	Change passwords or user identifications frequently to prevent them from being compromised.
22	CMMC IA.3.086 (NIST 800-171 Rev2 3.5.6)	*"Disable identifiers after a defined period of inactivity."*	Remove access from unused identifiers.
23	CMMC IR.3.098 (NIST 800-171 Rev2 3.6.2)	*"Track, document and report incidents to designated officials and/or authorities both internal and external to the organization."*	Identify, record, and report all incidents to any authorized authorities in house and if necessary, legal authorities.
24	CMMC IR.3.099 (NIST 800-171 Rev2 3.6.3)	*"Test the organizational incident response capability."*	Send tests such as fake phishing attempts to evaluate the quality of incident response.
25	CMMC MA.3.115 (NIST 800-171 Rev2 3.7.3)	*"Ensure equipment removed for off-site maintenance is sanitized of any CUI."*	Adopt a clean desk policy.

CMMC Level 3 Controls & Requirements			
#	**Security Control**	**Formal Requirement**	**How to Pass**
26	CMMC MA.3.116 (NIST 800-171 Rev2 3.7.4)	*"Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems."*	Verify devices on a separate system before allowing media to be run on organizational systems.
27	CMMC MP.3.122 (NIST 800-171 Rev2 3.8.4)	*"Mark media with necessary CUI markings and distribution limitations."*	Ensure CUI is distinguished, clearly marked, and only distributed to necessary audiences.
28	CMMC MP.3.124 (NIST 800-171 Rev2 3.8.5)	*"Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas."*	Know who has access to CUI media and who is responsible for keeping access secured in and outside of controlled areas.
29	CMMC MP.3.125 (NIST 800-171 Rev2 3.8.6)	*"Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards."*	Enable two-factor authentication, firewalls, or other virtual safeguards if media is not already physically contained.
30	CMMC MP.3.123 (NIST 800-171 Rev2 3.8.8)	*"Prohibit the use of portable storage devices when such devices have no identifiable owner."*	Ensure all storage devices and flash drives are identified and assigned to an authorized owner.
31	CMMC PE.3.136 (NIST 800-171 Rev2 3.10.6)	*"Enforce safeguarding measures for CUI at alternate work sites."*	Ensure safeguarding standards are established and enforced across all work locations.
32	CMMC CA.3.161 (NIST 800-171 Rev2 3.12.3)	*"Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls."*	Run network and system monitoring applications to monitor remote system access and log, accordingly. Control remote access by running only necessary applications and use firewalls and end-to-end encryption.
33	CMMC SC.3.180 (NIST 800-171 Rev2 3.13.2)	*"Employ architectural designs, software development techniques and systems engineering principles that promote effective information security within organizational systems."*	Build all software and technical innovations with security included in the planning.
34	CMMC SC.3.181 (NIST 800-171 Rev2 3.13.3)	*"Separate user functionality from system management functionality."*	Divide responsibilities among individuals dependent on functionality.
35	CMMC SC.3.182 (NIST 800-171 Rev2 3.13.4)	*"Prevent unauthorized and unintended information transfer via shared system resources."*	Establish gateways and restrictions for information transfer and establish secure teams within the online workspace.
36	CMMC SC.3.183 (NIST 800-171 Rev2 3.13.6)	*"Deny network communications traffic by default and allow network communications traffic by exception (e.g., deny all, permit by exception)."*	Explicitly deny all but authorized users which fill an established criterion to access certain software.

CMMC Level 3 Controls & Requirements			
#	**Security Control**	**Formal Requirement**	**How to Pass**
37	CMMC SC.3.184 (NIST 800-171 Rev2 3.13.7)	*"Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (e.g., split tunneling)."*	Ensure a valid Business Associate Agreement (BAA), which requires the third parties to verify the remote workstations are protected. Internal employees and contractors should have an established Acceptable Use Policy (AUP) that outlines the acceptable use of equipment.
38	CMMC SC.3.185 (NIST 800-171 Rev2 3.13.8)	*"Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards."*	Enable two-factor authentication, firewalls, or other virtual safeguards, if media is not already physically contained.
39	CMMC SC.3.186 (NIST 800-171 Rev2 3.13.9)	*"Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity."*	Remove access from unused identifiers/
40	CMMC SC.3.187 (NIST 800-171 Rev2 3.13.10)	*"Establish and manage cryptographic keys for cryptography employed in organizational systems."*	When accessing devices over the network, you should use a secure encryption method such as SSH.
41	CMMC SC.3.177 (NIST 800-171 Rev2 3.13.11)	*"Employ FIPS-validated cryptography when used to protect the confidentiality of CUI."*	Ensure any hardware or software cryptographic module implements algorithms from an approved FIPS list.
42	CMMC SC.3.188 (NIST 800-171 Rev2 3.13.13)	*"Control and monitor the use of mobile code."*	Only use mobile code on trusted sites in line with company policy.
43	CMMC SC.3.189 (NIST 800-171 Rev2 3.13.14)	*"Control and monitor the use of Voice over Internet Protocol (VoIP) technologies."*	Only use VoIP technology on trusted sites in line with company policy.
44	CMMC SC.3.190 (NIST 800-171 Rev2 3.13.15)	*"Protect the authenticity of communications sessions."*	Ensure all parties in communication sessions are authorized and are who they say they are.
45	CMMC SC.3.191 (NIST 800-171 Rev2 3.13.16)	*"Protect the confidentiality of CUI at rest."*	Ensure classified information is stored in a safe location.
46	CMMC AM.3.036	*"Define procedures for the handling of CUI data."*	Have established guidelines for handling, distributing, and storing all classified data.
47	CMMC AU.3.048	*"Collect audit information (e.g., logs) into one or more central repositories."*	Store audit information into backup locations accessible to authorized users.
48	CMMC RE.3.139	*"Regularly perform complete, comprehensive and resilient data backups as organizationally defined."*	Back up organizational data often. Test these backups by verifying that the Operating system, application, and data are intact and functional.

CMMC Level 3 Controls & Requirements			
#	**Security Control**	**Formal Requirement**	**How to Pass**
49	CMMC RM.3.144	*"Periodically perform risk assessments to identify and prioritize risks according to the defined risk categories, risk sources, and risk measurement criteria."*	Develop an action plan to remediate identified weaknesses or deficiencies that designates remediation dates for each item.
50	CMMC RM.3.146	*"Develop and implement risk mitigation plans."*	Have a policy in place that enables your business to prioritize, identify, and mitigate risk.
51	CMMC RM.3.147	*"Manage non-vendor-supported products (e.g., end of life) separately and restrict as necessary to reduce risk."*	Keep products not supported by your supply chain separate and restrict access to minimize risk.
52	CMMC CA.3.162	*"Employ a security assessment of enterprise software that has been developed internally, for internal use, and that has been organizationally defined as an area of risk."*	Conduct periodic security assessments to ensure security controls are implemented correctly and meet security requirements. Include vulnerability scanning, pen testing, log reviews, and speaking with company employees during these assessments.
53	CMMC SA.3.169	*"Receive and respond to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders."*	Have an incident response plan established and train necessary personnel.
54	CMMC SC.3.192	*"Implement Domain Name System (DNS) filtering services."*	Use the DNS to block malicious websites and filter out harmful or inappropriate content. Ensure company data remains secure and controls what employees can access on company-managed networks.
55	CMMC SC.3.193	*"Implement a policy restricting the publication of CUI on externally-owned, publicly-accessible websites (e.g., forums, LinkedIn, Facebook, Twitter, etc.)."*	Have clear policy guidelines forbidding the use of anything labeled as CUI to be posted on any websites not owned by the company.
56	CMMC SI.3.218	*"Employ spam protection mechanisms at information system access entry and exit points."*	Employ spam protection mechanisms at critical information system entry points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network.
57	CMMC SI.3.219	*"Implement email forgery protections."*	Use different engines, protocols, and software, such as anti-spam, anti-virus, SPF (Sender Policy Framework), DKIM (Domain Keys Identified Mail) and DMARC (Domain-based Message Authentication Reporting & Conformance) to protect from forgery.
58	CMMC SI.3.220	*"Utilize email sandboxing to detect or block potentially malicious email."*	Use an email protection software like Barracuda to filter spam or malicious emails.

Appendi C — CMMC Level 4 Controls & Requirements

CMMC Level 4 Controls & Requirements			
#	**Security Control**	**Formal Requirement**	**How to Pass**
1	CMMC AC.4.023	*"Control information flows between security domains on connected systems."*	Implement network segmentation specific to data classification zones. Set user permissions on files containing CUI.
2	CMMC AC.4.025	*"Periodically review and update CUI program access permissions."*	Have a schedule in place to review the current CUI program and if necessary, change who has access to CUI program.
3	CMMC AC.4.032	*"Restrict remote network access based on organizationally defined risk factors such as time of day, location of access, physical location, network connection state, and measured properties of the current user and role."*	Only granting authorized individuals' external access, placing guidelines on the use of personally owned or external system access, and limiting the number of access points to the system to better monitor network traffic.
4	CMMC AM.4.226	*"Employ a capability to discover and identify systems with specific component attributes (e.g., firmware level, OS type) within your inventory."*	Having a capability in place that can identify attributes of a specific system's components such as OS information and firmware.
5	CMMC AU.4.053	*"Automate analysis of audit logs to identify and act on critical indicators (TTPs) and/or organizationally defined suspicious activity."*	Automate the process of scanning audit logs for tactics, techniques, and procedures and identify and prioritize any suspicious activity.
6	CMMC AU.4054	*"Review audit information for broad activity in addition to per-machine activity."*	Review all audit information at a broad and specific level to get a holistic view of activity.
7	CMMC AT.4.059	*"Provide awareness training focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors; update the training at least annually or when there are significant changes to the threat."*	Ensure awareness training is focused on recognizing and responding to persistent adversaries and social engineering threat vectors such as phishing. Review and update training annually.
8	CMMC AT.4.060	*"Include practical exercises in awareness training that are aligned with current threat scenarios and provide feedback to individuals involved in the training."*	Design and practice realistic cyber threat scenarios to provide individuals with real hands-on experience.
9	CMMC CM.4.073	*"Employ application whitelisting and an application vetting process for systems identified by the organization."*	Ensure you have an application review process in place before allowing the installation of software on company-owned assets.

CMMC Level 4 Controls & Requirements			
#	**Security Control**	**Formal Requirement**	**How to Pass**
10	CMMC IR.4.100	*"Use knowledge of attacker tactics, techniques, and procedures in incident response planning and execution."*	Apply realistic attack methodologies and concepts when updating or executing the procedures of incident response.
11	CMMC IR.4.101	*"Establish and maintain a security operations center capability that facilitates a 24/7 response capability"*	Ensure that your organization has a 24/7 security operations center in place to respond to incidents promptly.
12	CMMC RM.4.148	*"Develop and update as required, a plan for managing supply chain risks associated with the IT supply chain."*	Ensure that there is a documented plan for managing and mitigating supply chain risk that Is reviewing on an annual basis.
13	CMMC RM.4.149	"Catalog and periodically update threat profiles and adversary TTPs "	Keep records of tactics, techniques, and practices of threat actors updated.
14	CMMC RM.4.150	*"Employ threat intelligence to inform the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, and response and recovery activities."*	Utilize information about cyber threat actors to keep the system and security structure up to date and apply that Information to Increase Information security maturity.
15	CMMC RM.4.151	*"Perform scans for unauthorized ports available across perimeter network boundaries over the organization's Internet network boundaries and other organizationally defined boundaries."*	Have a plan to perform vulnerability scans over the network environment, from outside and inside perspectives, on a regular scheduled basis.
16	CMMC SI.4.163	*"Create, maintain, and leverage a security strategy and roadmap for organizational cybersecurity improvement."*	Updating information system protection mechanisms within five days of new releases and completing these updates with configuration management policy and procedures.
17	CMMC SI.4.164	*"Conduct penetration testing periodically, leveraging automated scanning tools, and ad hoc tests using human experts."*	Performing periodic penetration testing of the system for malware and other vulnerabilities as defined in company policy, performing real-time scans of files from external sources, and disinfecting or quarantining infected files.
18	CMMC SA.4.171	*"Establish and maintain a cyber threat hunting capability to search for indicators of compromise in organizational systems and detect, track, and disrupt threats that evade existing controls."*	Have a method or program in place to identify, prioritize, and mitigate cyber threats that have evaded controls from level 3.
19	CMMC SA.4.173	*"Design network and system security capabilities to leverage, integrate, and share indicators of compromise."*	Create centralized system capabilities to be able to share and integrate IoC's
20	CMMC CA.4.227	*"Periodically perform red teaming against organizational assets to validate defensive capabilities."*	Perform scheduled red team assessments of your organizational assets to understand the strength of its defense against threat actors
21	CMMC SC.4.197	*"Employ physical and logical isolation techniques in the system and security architecture and/or where deemed appropriate by the organization"*	Separate assets within the system to ensure that users can control which users can access, view, or modify policies and resource

CMMC Level 4 Controls & Requirements			
#	**Security Control**	**Formal Requirement**	**How to Pass**
22	CMMC SC.4.228	*"Isolate administration of organizationally defined high-value critical network infrastructure components and servers."*	Keep access to high-value information within the network and available to authorized personnel only
23	CMMC SC.4.199	*"Utilize threat intelligence to proactively block DNS requests from reaching malicious domains."*	Only allow access to secure domains by restricting requests from known malicious domains or any server that is not "HTTPS."
24	CMMC SC.4.202	*"Employ mechanisms to analyze executable code and scripts (e.g., sandbox) traversing Internet network boundaries or other organizationally defined boundaries."*	Use a testing environment in a virtual machine, for example, to isolate any code changes that have not yet been tested in a way that is risk-free from compromising any systems
25	CMMC SC.4.229	*"Utilize a URL categorization service and implement techniques to enforce URL filtering of websites that are not approved by the organization."*	Create a blacklist of unauthorized websites that you could restrict access to when connected to the network.
26	CMMC SI.4.221	*"Use threat indicator information relevant to the information and systems being protected and effective mitigations obtained from external organizations to inform intrusion detection and threat hunting."*	Utilize information about cyber threat actors to keep the system and security structure up to date with means to effectively secure yourself from adversaries with techniques and mitigations from other organizations.

Appendix D — CMMC Level 5 Controls & Requirements

CMMC Level 5 Controls & Requirements			
#	**Security Control**	**Formal Requirement**	**How to Pass**
1	CMMC AC.5.024	*"Identify and mitigate risk associated with unidentified wireless access points connected to the network."*	Record all authorized devices connected to the network and identify any unauthorized connections
2	CMMC AU.5.055	*"Identify assets not reporting audit logs and assure appropriate organizationally defined systems are logging."*	Ensure all assets have a security-relevant record, a source for those records, and the sequence of activities involved recorded. Identify any assets not following that procedure and make corrections
3	CMMC AC.5.074	*"Verify the integrity and correctness of security critical or essential software as defined by the organization (e.g., roots of trust, formal verification, or cryptographic signatures)."*	Read the terms of agreement for all software essential to the organization or its security and verify that the inner mechanisms can be trusted to use.
4	CMMC IR.5.106	*"In response to cyber incidents, utilize forensic data gathering across impacted systems, ensuring the secure transfer and protection of forensic data."*	Collect data in a way that can protect authorized users and identify where, on what device, and who was responsible for any cyber incidents that may have occurred.
5	CMMC IR.5.102	*"Use a combination of manual and automated, real-time responses to anomalous activities that match incident patterns."*	Combine human and machine capabilities to ensure a timely and effective response to incidents.
6	CMMC IR.5.108	*"Establish and maintain a cyber incident response team that can investigate an issue physically or virtually at any location within 24 hours."*	Place personnel in charge of responding and investigating cyber incidents both in-person and remote within 24 hours of its occurrence
7	CMMC IR.5.110	*"Perform unannounced operational exercises to demonstrate technical and procedural responses."*	Perform drills to test personnel knowledge and effectiveness in following procedures.
8	CMMC RE.5.140	*"Ensure information processing facilities meet organizationally defined information security continuity, redundancy, and availability requirements."*	Use facilities that can be trusted and secure under the definition of the organization's requirements.

CMMC Level 5 Controls & Requirements			
#	**Security Control**	**Formal Requirement**	**How to Pass**
9	CMMC RM.5.152	*"Utilize an exception process for non-whitelisted software that includes mitigation techniques."*	For software not on the whitelist, have a procedure in place that minimizes defined risk.
10	CMMC RM.5.155	*"Analyze the effectiveness of security solutions at least annually to address anticipated risk to the system and the organization based on current and accumulated threat intelligence."*	Routinely test security solutions with anticipated risk scenarios to measure its effectiveness in incident response.
11	CMMC SC.5.198	*"Configure monitoring systems to record packets passing through the organization's Internet network boundaries and other organizationally defined boundaries."*	Setup boundaries within the network to record packets as they pass through from checkpoint to checkpoint and monitor for consistency.
12	CMMC SC.5.230	*"Enforce port and protocol compliance."*	Enforce protocol compliance by properly configuring your IDS/IPS and develop a policy that outlines the tools used.
13	CMMC SC.5.208	*"Employ organizationally defined and tailored boundary protections in addition to commercially available solutions."*	Have in and out of house protections in place to enhance security capabilities and protections.
14	CMMC SI.5.222	*"Analyze system behavior to detect and mitigate the execution of normal system commands and scripts that indicate malicious actions."*	Implement Endpoint detection and response software. These tools continuously monitor the system for any scripts or code that could lead to malicious actions.
15	CMMC SI.5.223	*"Monitor individuals and system components on an ongoing basis for anomalous or suspicious behavior.*	Implement a User and Entity Behavior Analytics service that continuously monitors individuals and systems for any unusual behavior that may be indicative of malicious behavior.

About Us

Easily find out where the biggest risks are

In near real time make the changes you need to protect your organization

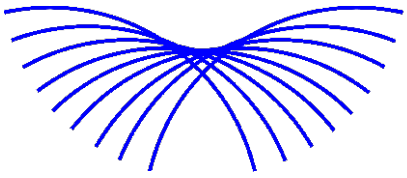
Get alerted to new threats that are targeting you

Track how your network vulnerabilities change over time

WhiteHawk, Inc., is the first online Cybersecurity Exchange based on a platform architecture that is Artificial Intelligence (AI)-driven, with a focus on identifying, prioritizing, and mitigating cyber risks for businesses of all sizes. WhiteHawk continually vets and assesses risk-focused technologies, methodologies, and solutions that are impactful, affordable, and scalable to stay up to date on current cyber threat vectors to businesses, organizations, family offices, and individuals. We have an online approach to determining your key cyber risks through a Cyber Threat Readiness Questionnaire, and as appropriate, a cyber risk assessment. Using this information, we then match tailored risk mitigation solution options to companies and organizations based on current threat trends across key sectors. Our Cyber Consultants on staff help build a tailored cyber maturity plan customized to meet your business or mission objectives.

For more information, visit www.whitehawk.com.

WhiteHawk CEC, Inc.
Terry Roberts - Founder, President, & CEO
consultingservices@whitehawk.com



CMMC Overview Whitepaper

WhiteHawk CEC Inc.

www.whitehawk.com