Cybersecurity Maturity Model Certification (CMMC)

FILECLOUD
WWW.GETFILECLOUD.COM

Note: This white paper is intended to provide an overview and is not intended to provide legal advice. For more comprehensive information on regulations and their implications, please consult your legal counsel.

Introduction to CMMC

The theft of intellectual property and sensitive information from all industrial sectors due to malicious cyber activity threatens economic security and national security. The Council of Economic Advisors estimates that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016.

The Center for Strategic and International Studies estimates that the total global cost of cybercrime was as high as $600 billion in 2017. 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 sectors consists of over 300,000 companies that support the war fighter and contribute towards the research, engineering, development, acquisition, production, delivery, sustainment, and operations of DoD systems, networks, installations, capabilities, and services. The aggregate loss of intellectual property and certain unclassified information from the DoD supply chain can undercut U.S. technical advantages and innovation as well as significantly increase risk to national security.

As part of multiple lines of effort focused on the security and resiliency of the DIB sector, the DoD is working with industry to enhance the protection of the following types of unclassified information within the supply chain:

Federal Contract Information (FC/): FCI is information provided by or generated far the Government under contract not intended far public release.

Controlled Unclassified Information (CU/):

CUI is information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and government-wide policies, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or Atomic Energy Act of 19 54, as amended.

Towards this end, the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) has developed the Cybersecurity Maturity Model Certification (CMMC) framework in concert with DoD stakeholders, University Affiliated Research Centers (UARCs), Federally Funded Research and Development Centers (FFRDCs), and the
DIB sector.

This document focuses on the CMMC model which measures cybersecurity maturity with five levels and aligns a set of processes and practices with the type and sensitivity of information to be protected and the associated range of threats. The model consists of maturity processes and cybersecurity best practices from multiple cybersecurity standards, frameworks, and other references, as well as inputs from the broader community .

The model encompasses the baste safeguarding requirements for FCI specified in Federal Acquisition Regulation (FAR) Clause 52.204-21 and the security requirements for CUI specified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 per Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012 .

The CMMC framework adds a certification element to verify the implementation of processes   and practices associated with the achievement of a cybersecurity maturity level. CMMC is designed to provide increased assurance to the DoD that a DIB contractor adequately protect CUI at a level commensurate with the risk, accounting for information flow down to its subcontractors in a multi-tier supply chain.

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.[1]

(1): "Cybersecurity Maturity Model Certification (CMMC) Version 1.0 by Copyright 2020 Carnegie Mellon University and The Johns Hopkins University Applied Physics Laboratory LLC."

CYBERSECURITY MATURITY MODEL CERTIFICATION

Domain	Requirements	How does FileCloud Comply?
Access Control (AC)	• Establish system access requirements • Control internal system access • Control remote system access • Limit data access to authorized users and processes	FileCloud support integration with Active Directory, LDAP, and SSO. In addition, FileCloud integrates your Network Shares with NTFS permissions to provide you with better access control of the data your users are allowed to view, upload, download, share, sync, or manage. Within FileCloud you can create users and groups, and assign permissions and policies to them to allow or prevent them from accessing your data. FileCloud also supports DLP and granular folder permissions.
Asset Management (AM)	• Identify and document assets • Manage asset inventory	FileCloud's Centralized Device Management allows you to view all the devices that have access to FileCloud using our mobile and desktop clients. FileCloud also includes functionality for creating reports of these devices to aid you in creating your inventory report.
Audit and Accountability (AU)	• Define audit requirements • Perform auditing • Identify and protect audit information • Review and manage audit logs	FileCloud's auditing capabilities enable you to review who, when, where, and what are involved each time FileCloud is accessed. FileCloud also supports SIEM integration. FileCloud's data governance capabilities allow you to apply multiple retention rules to avoid the deletion of auditable records you want to store in FileCloud.
Awareness and Training (AT)	• Conduct security awareness activities • Conduct training	To complement your internal employee training, FileCloud provides you with extensive information about applying best security practices while using FileCloud. FileCloud also offers end-user training.

Configuration Management (CM)	• Establish configuration baselines • Perform configuration and change management	FileCloud contains multiple configuration capabilities including but not limited to: -Centralized Device Management -Content Classification -DLP -Global Policies -Specific device configuration policies. -Customization -Data Governance. -User password enforcement -Private sharing permissions. -Granular folder level permissions.
Identification and Authentication (IA)	• Grant access to authenticated entities	Besides FileCloud's proprietary user authentication, FileCloud supports integration with Active Directory, LDAP, and SSO. FileCloud also supports Duo Security integration and 2FA.
Incident Response (IR)	• Plan incident response • Detect and report events • Develop and implement response to a declared incident • Perform post incident reviews • Test incident response	FileCloud's data governance dashboard displays potential rule violations such as DLP violations or retention policy violations. FileCloud workflows enable you to automate report generation, device approval, and other tasks.
Maintenance (MA)	• Manage maintenance	Using FileCloud workflows, administrators have the ability to perform automatic maintenance tasks within FileCloud, for example, deleting files after a specified amount of time or disabling users who have not accessed FileCloud in a specific amount of time. FileCloud also supports automatic audit log trimming and exporting to a location defined by the administrator.
Media Protection (MP)	• Identify and mark media • Protect and control media • Sanitize media • Protect media during transport	FileCloud's antivirus integration via ClamAV or ICAP protocol enables you to verify the integrity of files as they are uploaded. FileCloud's DLP provides you with granular control over your data. FileCloud supports in-transit encryption via HTTPS/SSL.

Personnel Security (PS)	• Screen personnel • Protect CUI during personnel actions	FileCloud's Smart classification and DLP enable you to classify your data based on DLP rules that deny or allow downloads or sharing.
Physical Protection (PE)	• Limit physical access	Not Applicable
Recovery (RE)	• Manage backups • Manage information security continuity	The FileCloud Server Backup tool creates backs up your data automatically.
Risk Management (RM)	• Identify and evaluate risk • Manage risk • Manage supply chain risk	Not Applicable
Security Assessment (CA)	• Develop and manage a system security plan • Define and manage controls • Perform code reviews	Not Applicable
Situational Awareness (SA)	• Implement threat monitoring	Not Applicable
Systems and Communications Protection (SC)	• Define security requirements for systems and communications • Control communications at system boundaries	Not Applicable
System and Information Integrity (SI)	• Identify and manage information system flaws • Identify malicious content • Perform network and system monitoring • Implement advanced email protections	Not Applicable

CMMC	Details	FileCloud
	Access Control (AC)	
	Level 1	
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Yes
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	Yes
AC.1.003	Verify and control/limit connections to and use of external information systems.	Yes
AC.1.004	Control information posted or processed on publicly accessible information systems.	Yes
	Level 2	
AC.2.005	Provide privacy and security notices consistent with applicable CUI rules.	Yes
AC.2.006	Limit use of portable storage devices on external systems.	N/A
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	Yes
AC.2.008	Use non-privileged accounts or roles when accessing non-security functions.	Yes
AC.2.009	Limit unsuccessful logon attempts.	Yes
AC.2.010	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	Yes
AC.2.011	Authorize wireless access prior to allowing such connections.	N/A
AC.2.013	Monitor and control remote access sessions.	N/A
AC.2.015	Route remote access via managed access control points.	N/A
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	N/A
	Level 3	
AC.3.017	Separate the duties of individua Is to reduce the risk of malevolent activity without collusion.	Yes
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs	Yes
AC.3.019	Terminate (automatically) user sessions after a defined condition.	Yes
AC.3.012	Protect wireless access using authentication and encryption.	N/A
AC.3.020	Control connection of mobile devices.	Yes
AC.3.014	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	Yes
AC.3.021	Authorize remote execution of privileged commands and remote access to security-relevant information.	N/A
AC.3.022	Encrypt CUI on mobile devices and mobile computing platforms.	N/A
	Level 4	
AC.4.023	Control information flows between security domains on connected systems.	N/A
AC.4.025	Periodically review and update CUI program access permissions.	N/A

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.	No
Level 5		
AC.5.024	Identify and mitigate risk associated with unidentified wireless access points connected to the network.	N/A
ASSET MANAGEMENT (AM)		
Level 3		
AM.3.036	Define procedures for the handling of CUI data.	N/A
Level 4		
AM.4.226	Employ a capability to discover and identify systems with specific component attributes (e.g. firmware level, OS type) within your inventory.	N/A
AUDIT AND ACCOUNTABILITY (AU)		
Level 2		
AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions	Yes
AU.2.042	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.	Yes
AU.2.043	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	Yes
AU.2.044	Review audit logs.	Yes
Level 3		
AU.3.045	Review and update logged events.	Yes
AU.3.046	Alert in the event of an audit logging process failure.	Yes
AU.3.048	Collect audit information (e.g., logs) into one or more central repositories.	Yes
AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	Yes
AU.3.050	Limit management of audit logging functionality to a subset of privileged users.	Yes
AU.3.051	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	Yes
AU.3.052	Provide audit record reduction and report generation to support on-demand analysis and reporting.	Yes
Level 4		
AU.4.053	Automate analysis of audit logs to identify and act on critical indicators (TIPs) and/or organizationally defined suspicious activity.	Yes
AU.4.054	Review audit information for broad activity in addition to per-machine activity.	N/A

	Level 5	
AU.5.055	Identify assets not reporting audit logs and assure appropriate organizationally defined systems are logging.	N/A
	AWARENESS AND TRAINING (AT)	
	Level 2	
AT.2.056	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.	N/A
AT.2.057	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	N/A
	Level 3	
AT.3.058	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	N/A
	Level 4	
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.	N/A
AT.4.060	include practical exercises in awareness training that are aligned with current threat scenarios and provide feedback to individua ls involved in the training.	N/A
	CONFIGURATION MANAGEMENT (CM)	
	Level 2	
CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	N/A
CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	N/A
CM.2.063	Control and monitor user-installed software.	N/A
CM.2.064	Establish and enforce security configuration settings for information technology products employed in organizational systems.	N/A
CM.2.065	Track, review, approve, or disapprove, and lag changes to organizational systems.	N/A
CM.2.066	Analyze the security impact of changes prior to implementation.	N/A
	Level 3	
CM.3.067	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	N/A
CM.3.068	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	N/A
CM.3.069	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.	N/A
	Level 4	
CM.4.073	Employ application whitelisting and an application vetting process for systems identified by the organization.	N/A

	Level 5	
CM.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).	N/A
	IDENTIFICATION AND AUTHENTICATION (IA)	
	Level 1	
IA.1.076	Identify information system users, processes acting on behalf of users, or devices.	Yes
IA.1.077	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	Yes
	Level 2	
IA.2.078	Enforce a minimum password complexity and change of characters when new passwords are created.	Yes
IA.2.079	Prohibit password reuse for a specified number of generations.	Yes
IA.2.080	Allow temporary password to use for system logons with an immediate change to a permanent password.	Yes
IA.2.081	Store and transmit only cryptographically protected passwords.	Yes
IA.2.082	Obscure feedback of authentication information.	Yes
	Level 3	
IA.3.083	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	Yes
IA.3.084	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	Yes
IA.3.085	Prevent the reuse of identifiers for a defined period.	Yes
IA.3.086	Disable identifiers after a defined period of inactivity.	No
	INCIDENT RESPONSE (IR)	
	Level 2	
IR.2.092	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	N/A
IR.2.093	Detect and report events.	Yes
IR.2.094	Analyze and triage events to support event resolution and incident declaration.	N/A
IR.2.096	Develop and implement responses to declared incidents according to pre-defined procedures.	N/A
IR.2.097	Perform root cause analysis on incidents to determine underlying causes.	N/A
	Level 3	
IR.3.098	Track, document, and report incidents to designated officials and/or authorities both internal And external to the organization.	N/A
IR.3.099	Test the organizational incident response capability.	N/A

	Level 4	
IR.4.100	Use knowledge of attacker tactics, techniques, and procedures in incident response planning and execution.	N/A
IR.4.101	Establish and maintain a security operations center capability that facilitates a 24/7 response capability.	N/A
	Level 5	
IR.5.106	In response to cyber incidents, utilize forensic data gathering across impacted systems, ensuring the secure transfer and protection of forensic data.	N/A
IR.5.102	Use a combination of manual and automated, real-time responses to anomalous activities that match incident patterns.	N/A
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.	N/A
IR.5.110	Perform unannounced operational exercises to demonstrate technical and procedural responses.	N/A
	MAINTENANCE (MA)	
	Level 2	
MA.2.111	Perform maintenance on organizational systems.	N/A
MA.2.112	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	N/A
MA.2.113	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	N/A
MA.2.114	Supervise the maintenance activities of personnel without required access authorization.	N/A
	Level 3	
MA.3.115	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	N/A
MA.3.116	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	N/A
	MEDIA PROTECTION (MP)	
	Level 1	
MP.1.118	Sanitize or destroy information system media containing Federal Contract information before disposal or release for reuse.	N/A
	Level 2	
MP.2.119	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	N/A
MP.2.120	Limit access to CUI on system media to authorized users.	Yes
MP.2.121	Control the use of removable media on system components.	N/A
	Level 3	
MP.3.122	Mark media with necessary CUI markings and distribution limitations.	Yes
MP.3.123	Prohibit the use of portable storage devices when such devices have no identifiable owner.	N/A

MP.3.124	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas	N/A
MP.3.125	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	N/A
PERSONNEL SECURITY (PS)		
Level 2		
PS.2.127	Screen individuals prior to authorizing access to organizational systems containing CUI.	N/A
PS.2.128	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	N/A
PHYSICAL PROTECTION (PE)		
Level 1		
PE.1.131	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	N/A
PE.1.132	Escort visitors and monitor visitor activity.	N/A
PE.1.133	Maintain audit logs of physical access.	N/A
PE.1.134	Control and manage physical access devices.	N/A
Level 2		
PE.2.135	Protect and monitor the physical facility and support infrastructure for organizational systems.	N/A
Level 3		
PE.3.136	Enforce safeguarding measures for CUI at alternate work sites.	N/A
RECOVERY (RE)		
Level 2		
RE.2.137	Regularly perform and test data back-ups.	Yes
RE.2.138	Protect the confidentiality of backup CUI at storage locations.	N/A
Level 3		
RE.3.139	Regularly perform complete, comprehensive, and resilient data back-ups as organizationally defined.	N/A
Level 5		
RE.S.140	Ensure information processing facilities meet organizationally defined information security continuity, redundancy, and availability requirements.	N/A
RISK MANAGEMENT (RM)		
Level 2		
RM.2.141	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.	N/A
RM.2.142	Sean for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	N/A
RM.2.143	Remediate vulnerabilities in accordance with risk assessments.	N/A

IR.4.100	Use knowledge of attacker tactics, techniques, and procedures in incident response planning and execution.	N/A
IR.4.101	Establish and maintain a security operations center capability that facilitates a 24/7 response capability.	N/A
Level 5		
IR.5.106	In response to cyber incidents, utilize forensic data gathering across impacted systems, ensuring the secure transfer and protection of forensic data.	N/A
IR.5.102	Use a combination of manual and automated, real-time responses to anomalous activities that match incident patterns.	N/A
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.	N/A
IR.5.110	Perform unannounced operational exercises to demonstrate technical and procedural responses.	N/A
MAINTENANCE (MA)		
Level 2		
MA.2.111	Perform maintenance on organizational systems.	N/A
MA.2.112	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	N/A
MA.2.113	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	N/A
MA.2.114	Supervise the maintenance activities of personnel without required access authorization.	N/A
Level 3		
MA.3.115	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	N/A
MA.3.116	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	N/A
MEDIA PROTECTION (MP)		
Level 1		
MP.1.118	Sanitize or destroy information system media containing Federal Contract information before disposal or release for reuse.	N/A
Level 2		
MP.2.119	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	N/A
MP.2.120	Limit access to CUI on system media to authorized users.	Yes
MP.2.121	Control the use of removable media on system components.	N/A
Level 3		
MP.3.122	Mark media with necessary CUI markings and distribution limitations.	Yes
MP.3.123	Prohibit the use of portable storage devices when such devices have no identifiable owner.	N/A

MP.3.124	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas	N/A
MP.3.125	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	N/A
PERSONNEL SECURITY (PS)		
Level 2		
PS.2.127	Screen individuals prior to authorizing access to organizational systems containing CUI.	N/A
PS.2.128	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	N/A
PHYSICAL PROTECTION (PE)		
Level 1		
PE.1.131	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	N/A
PE.1.132	Escort visitors and monitor visitor activity.	N/A
PE.1.133	Maintain audit logs of physical access.	N/A
PE.1.134	Control and manage physical access devices.	N/A
Level 2		
PE.2.135	Protect and monitor the physical facility and support infrastructure for organizational systems.	N/A
Level 3		
PE.3.136	Enforce safeguarding measures for CUI at alternate work sites.	N/A
RECOVERY (RE)		
Level 2		
RE.2.137	Regularly perform and test data back-ups.	Yes
RE.2.138	Protect the confidentiality of backup CUI at storage locations.	N/A
Level 3		
RE.3.139	Regularly perform complete, comprehensive, and resilient data back-ups as organizationally defined.	N/A
Level 5		
RE.S.140	Ensure information processing facilities meet organizationally defined information security continuity, redundancy, and availability requirements.	N/A
RISK MANAGEMENT (RM)		
Level 2		
RM.2.141	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.	N/A
RM.2.142	Sean for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	N/A
RM.2.143	Remediate vulnerabilities in accordance with risk assessments.	N/A

Level 3		
RM.3.144	Periodically perform risk assessments to identify and prioritize risks according to the defined risk categories, risk sources, and risk measurement criteria.	N/A
RM.3.146	Develop and implement risk mitigation plans.	N/A
RM.3.147	Manage non-vendor-supported products (e.g., end of life) separately and restricts necessary to reduce risk.	N/A
Level 4		
RM.4.149	Catalog and periodically update threat profiles and adversary TIPs.	N/A
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.	N/A
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.	N/A
RM.4.148	Develop and update as required, a plan for managing supply chain risks associated with the IT supply chain.	N/A
Level 5		
RM.5.152	Utilize an exception process for non-whitelisted software that includes mitigation techniques.	N/A
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.	N/A
SECURITY ASSESSMENT (CA)		
Level 2		
CA.2.157	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	N/A
CA.2.158	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	N/A
CA.2.159	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	N/A
Level 3		
CA.3.161	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	N/A
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.	N/A
Level 4		
CA.4.163	Create, maintain, and leverage a security strategy and roadmap for organizational cybersecurity improvement.	N/A
CA.4.164	Conduct penetration testing periodically, leveraging automated scanning tools and ad hoc tests using human experts.	N/A
CA.4.227	Periodically perform red teaming against organizational assets in ardor to validate defensive capabilities.	N/A

SITUATIONAL AWARENESS (SA)		
Level 3		
SA.3.169	Receive and respond to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders.	**N/A**
Level 4		
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.	**N/A**
SA.4.173	Design network and system security capabilities to leverage, integrate, and share indicators of compromise.	**N/A**
SYSTEM AND COMMUNICATIONS PROTECTION (SC)		
Level 1		
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.	**N/A**
SC.1.176	implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	**N/A**
Level 2		
SC.2.178	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	**N/A**
SC.2.179	Use encrypted sessions for the management of network devices	**Yes**
Level 3		
SC.3.177	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	**Yes**
SC.3.180	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	**N/A**
SC.3.181	Separate user functionality from system management functionality.	**Yes**
SC.3.182	Prevent unauthorized and unintended information transfer via shared system resources	**Yes**
SC.3.183	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	**Yes**
SC.3.184	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via sore other connection to resources in external networks (i.e., split tunneling).	**N/A**
SC.3.185	implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	**Yes**
SC.3.186	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	**N/A**
SC.3.187	Establish and manage cryptographic keys for cryptography employed in organizational systems.	**Yes**
SC.3.188	Control and monitor the use of mobile code.	**N/A**

SC.3.189	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	N/A
SC.3.190	Protect the authenticity of communications sessions.	N/A
SC.3.191	Protect the confidentiality of CUI at rest.	Yes
SC.3.192	Implement Domain Name System (DNS) filtering services.	N/A
SC.3.193	implement a policy restricting the publication of CUI on externally owned, publicly accessible websites (e.g., forums, LinkedIn, Facebook, Twitter).	N/A
Level 4		
SC.4.197	Employ physical and logical isolation techniques in the system and security architecture and/or where deemed appropriate by the organization.	N/A
SC.4.228	isolate administration of organizationally defined high-value critical! network infrastructure components and servers.	N/A
SC.4.199	Utilize threat intelligence to proactively block DNS requests from reaching malicious domains.	N/A
SC.4.202	Employ mechanisms to analyze executable code and scripts (e.g., sandbox) traversing Internet network boundaries or other organizationally defined boundaries.	N/A
SC.4.229	Utilize a URL categorization service and implement techniques to enforce URL filtering of websites that are not approved by the organization.	N/A
Level 5		
SC.5.198	Configure monitoring systems to record packets passing through the organization's Internet network boundaries and other organizationally defined boundaries.	N/A
SC.5.230	Enforce port and protocol compliance.	
SC.5.208	Employ organizationally defined and tailored boundary protections in addition to commercially available solutions.	N/A
	SYSTEM AND INFORMATION INTEGRITY (SI)	
	Level 1	
SI.1.210	identify, report, and correct information and information system flaws in a timely manner.	N/A
SI.1.211	Provide protection from malicious code at appropriate locations within organizational information systems.	N/A
SI.1.212	Update malicious code protection mechanisms when new releases are available.	N/A
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.	N/A
	Level 2	
SI.2.214	Monitor system security alerts and advisories and take action in response.	N/A
SI.2.216	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	N/A

Sl.2.217	**identify unauthorized use of organizational systems.**	**N/A**
Level 3		
Sl.3.218	**Employ spam protection mechanisms at information system access entry and exit points.**	**N/A**
Sl.3.219	**implement email forgery protections.**	**N/A**
Sl.3.220	**Utilize sandboxing to detector block potentially malicious email.**	**N/A**
Level 4		
Sl.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.**	**N/A**
Level 5		
Sl.5.222	**Analyze system behavior to detect and mitigate execution of normal system commands and scripts that indicate malicious actions.**	**N/A**
Sl.5.223	**Monitor individuals and system components on an ongoing basis for anomalous or suspicious behavior.**	**N/A**

About Us

FileCloud Server is the commercial of the shelf software solution that helps businesses to securely share, manage, and govern enterprise content. FileCloud software provides the necessary capabilities for organizations to obtain CMMC compliance.

The end-user is responsible for utilizing suitable FileCloud capabilities as well as managing and maintaining the environment where FileCloud is being hosted to ensure the CMMC requirements are being met.

Filecloud aids with your CMMC compliance efforts under the shared responsibility model.