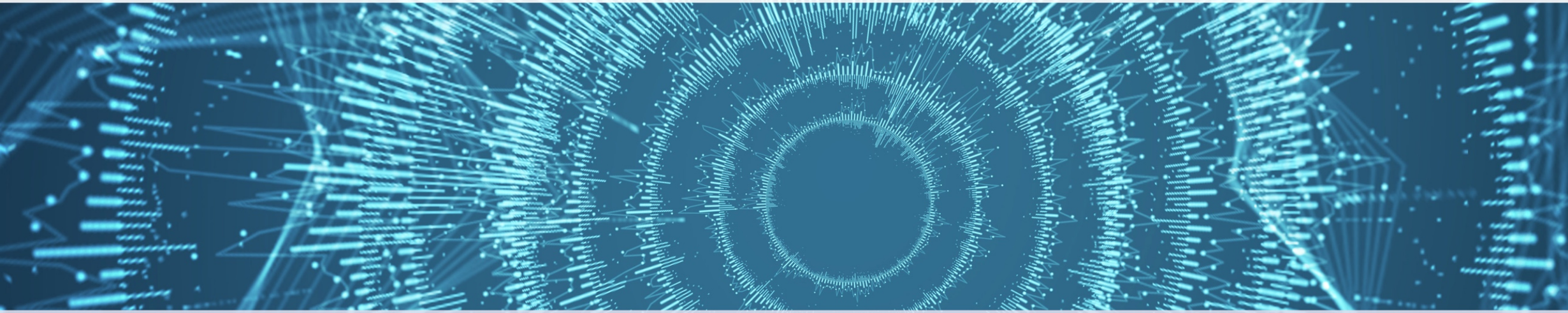
CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)



UNCLASSIFIED - DRAFT

Version 0.4

August 30, 2019

NOTICES

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center and under Contract No. HQ0034-13-D-0003 and Contract No. N00024-13-D-6400 with the Johns Hopkins University Applied Physics Laboratory, LLC, a University Affiliated Research Center.

DM19-0824

DOMAIN: ACCESS CONTROL (AC)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C1 Establish internal system access requirements	L1-1 System access is limited to authorized users, processes acting on behalf of authorized users, and devices, at least in an ad hoc manner. • NIST SP 800-171 3.1.1	L2-1 The organization has a process to limit system access to authorized users, processes acting on behalf of authorized users, and devices • NIST SP 800-171 3.1.1			
		L2-2 System logon screens display the appropriate system use notification messages. • NIST SP 800-171 3.1.9			
C2 Control internal system access	L1-1 Limit system access to the types of transactions and functions that authorized users are permitted to execute. • NIST SP 800-171 3.1.2	L2-1 Separate the duties of individuals to reduce the risk of malevolent activity without collusion. • NIST SP 800-171 3.1.4	L3-1 Use non-privileged accounts or roles when accessing nonsecurity functions. • NIST SP 800-171 3.1.6	L4-1 The organization comprehensively applies least privilege and separation of duties to identities, processes, networks, and interfaces across the enterprise. • DIB	L5-1 Network, host, and software access management is context-aware, adapting the security posture to the most restrictive viable settings based on the physical location, network connection state, time-of-day, and measured properties of the current user and role. • DIB
	L1-2 Limit unsuccessful logon attempts on a single system to 10 or less. • NIST SP 800-171 Partial 3.1.8	L2-2 Only grant privileges necessary for a system user to fulfill their assigned duties. • NIST SP 800-171 3.1.5	L3-2 Role based access is implemented to prevent non-privileged users from executing privileged functions. • NIST SP 800-171 3.1.7	L4-2 The system performs recurring scans and assessments to ensure appropriate user permissions are maintained. • CSF: PR.AC-2, PR-AC-3, PR.AC-4 • CIS: 14.5	L5-2 The organization ensures that all access to systems, services, and networks is indirect, managed via a service mediation layer that provides secure transaction processing, monitoring, and policy enforcement while hiding logical and physical locations and access methods from the accessing user, application, or service. • DIB
		L2-3 All wireless access is authorized prior to allowing such connections. • NIST SP 800-171 3.1.16	L3-3 The execution of privileged functions is recorded in audit logs. • NIST SP 800-171 3.1.7	L4-3 The organization utilizes a wireless intrusion detection system to identify and alert on unidentified wireless access points connected to the network. • CIS 7.1 • CIS 15.3	

DOMAIN: ACCESS CONTROL (AC)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C2 Control internal system access. *(continued)*			L3-4 The system is configured to lock the session after a predetermined period of inactivity. • NIST SP 800-171 3.1.10		
			L3-5 User sessions are automatically terminated after a defined condition. • NIST SP 800-171 Full 3.1.11		
			L3-6 All wireless access is protected using authentication and encryption. • NIST SP 800-171 3.1.17		
			L3-7 Mobile devices connected to the system are controlled and monitored. • NIST SP 800-171 3.1.18		
C3 Control remote system access		L2-1 Remote access sessions are monitored and controlled. • NIST SP 800-171 3.1.12	L3-1 Ensure all remote access sessions are encrypted. • NIST SP 800-171 3.1.13		L5-1 Network, host, and software access management is context-aware, adapting the security posture to the most restrictive viable settings based on their physical location, network connection state, time-of-day, and measured properties of the current user and role. • DIB
			L3-2 All remote access sessions should be routed through managed access control points. • NIST SP 800-171 3.1.14		L5-2 Access to higher value assets, as defined by 800-171B, and data are restricted based on context-aware configurations (location, network state, time-of-day, etc.). • DIB

DOMAIN: ACCESS CONTROL (AC)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C3 Control remote system access. *(continued*)			L3-3 The organization authorizes remote execution of privileged commands and remote access to security-relevant information. • NIST SP 800-171 3.1.15		L5-3 The organization ensures that all access to systems, services, and networks is indirect, managed via a service mediation layer that provides secure transaction processing, monitoring, and policy enforcement while hiding logical and physical locations and access methods from the accessing user, application, or service. • DIB
C4 Identify access requirements for each class of data accessible from the internal network	L1-1 Guidelines are developed for the use of personally owned or external information systems. • NIST SP 800-171 Partial 3.1.20, FAR	L2-1 CUI stored on portable storage devices on external systems are identified and documented. Limits on the use of such storage devices is defined. • NIST SP 800-171 Partial 3.1.21			
C5 Limit access to data to authorized users and processes acting on behalf of authorized users.	L1-1 CUI posted to publically accessible systems is identified and controlled. • NIST SP 800-171 3.1.22	L2-1 The system architecture is implemented to control the flow of data. Enforcement occurs in boundary protection devices such as gateways, routers, guards, encrypted tunnels, firewalls. • NIST SP 800-171 3.1.3	L3-1 Utilize an active discovery tool to identify sensitive data. • CIS 7.1: 14.5	L4-1 Enforce access control to data through automated tools. • CIS 7.1: 14.7	L5-1 CUI data access is context-aware, with access permissions determined based on the user and device physical location, network connection state, time-of-day, and measured properties of the current user and role. • DIB
		L2-2 Connections from personally owned or external information systems are monitored and controlled. • NIST SP 800-171 3.1.20	L3-2 Mobile devices that store and transmit CUI are identified and encrypted. • NIST SP 800-171 3.1.19	L4-2 The organization applies need-to-know and fine-grained access control for CUI data access. • DIB	L5-2 The organization applies data obfuscation and deception to reduce the confidence by an unauthorized user that the CUI data retrieved is where or what they believe it is. • DIB
					L5-3 The organization keeps all CUI data cryptographically secured at all times, to include execution. • DIB

DOMAIN: ACCESS CONTROL (AC)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C5 Limit access to data to authorized users and processes acting on behalf of authorized users. *(continued)*					L5-4 The organization ensures that access to CUI data is indirect, managed via a data mediation layer that provides secure transaction processing, monitoring, and policy enforcement while hiding logical and physical data locations and storage methods from the accessing user, application, or service. • DIB

DOMAIN: ACCESS CONTROL (AC)

MATURITY LEVEL CAPABILITY	PROCESSES				
	Maturity Level 1 (ML1)	Maturity Level 2 (ML2)	Maturity Level 3 (ML3)	Maturity Level 4 (ML4)	Maturity Level 5 (ML5)
Improve Access Control activities		ML2-1 Establish a policy for Access Control.	ML3-1 Review Access Control activities for conformance.	ML4-1 Inform high-level management.	ML5-1 Standardize documentation for Access Control.
		ML2-2 Establish practices to implement Access Control.	ML3-2 Provide resources for Access Control.	ML4-2 Review Access Control activities for effectiveness.	ML5-2 Share Access Control improvements across the organization.
		ML2-3 Establish a plan for Access Control.			

DOMAIN: ASSET MANAGEMENT (AM)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C1 Identify assets	L1-1 Organizational assets are identified and inventoried (hardware, virtual, software, firmware, and CUI information), at least in an ad hoc manner. • NIST SP 800-171 3.4.1 • RMM ADM:SG1.SP1	L2-1 The organization has a process to identify and inventory organizational assets (hardware, virtual, software, firmware, and information). • NIST SP 800-171 3.4.1 • RMM ADM:SG1.SP1	L3-1 Assets are associated with the system, organizational unit or service they support. • RMM ADM:SG2.SP1	L4-1 Asset definition and scope of cybersecurity program includes operational technology like SCADA, ICS, IoT, embedded, and real-time applications. • DIB	
	L1-2 The organization ensures that software is supported by the vendor. • CIS 7.1: 2.2	L2-2 Software inventory tools are utilized to automate and document all software within the organization. • CIS 7.1: 2.3	L3-2 The organization utilizes an active discovery tool. • CIS 7.1: 1.1	L4-2 Use DHCP logging to update assets. • CIS 7.1: 14.5	
			L3-3 A passive asset discovery tool is utilized. • CIS 7.1: 1.2		
			L3-4 The organization removes sensitive data or systems that are not regularly accessed by the organization. • CIS 7.1: 13.2		
C2 Develop a common definition for assets and their attributes		L2-1 All CUI data is identified, classified and labeled as such. • ISO: A.8.2.1 • ISO: A.8.2.2	L3-1 Inventory attributes are defined and applied, including information to support the cybersecurity strategy (e.g., location, asset owner, asset custodian, applicable security requirements, service dependencies, service level agreements, and conformance of assets to relevant industry standards). • RMM ADM:SG1.SP2		
		L2-2 The organization has procedures for the handling of CUI data. • ISO: A.8.2.3			

DOMAIN: ASSET MANAGEMENT (AM)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C3 Identify asset inventory change criteria			L3-1 Criteria are developed and documented establishing when a change in the asset inventory must be considered. • RMM ADM:SG3.SP1	L4-1 Establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components. • NIST SP 800-171B 3.4.1e	
C4 Maintain changes to assets and inventory		L2-1 Asset inventory is updated as changes occur. • RMM ADM:SG3.SP2	L3-1 The asset inventory is current (as defined by the organization). • RMM ADM:SG3.SP2	L4-1 Employ automated discovery and management tools to maintain an up-to-date, complete, accurate, and readily available inventory of system components. • NIST SP 800-171B 3.4.3e	
				L4-2 Performs periodic spot checks to ensure that the semi-automated systems managing assets are not missing any assets in the enterprise.	

DOMAIN: ASSET MANAGEMENT (AM)

MATURITY LEVEL CAPABILITY	PROCESSES				
	Maturity Level 1 (ML1)	Maturity Level 2 (ML2)	Maturity Level 3 (ML3)	Maturity Level 4 (ML4)	Maturity Level 5 (ML5)
Improve Asset Management activities		ML2-1 Establish a policy for Asset Management.	ML3-1 Review Asset Management activities for conformance.	ML4-1 Inform high-level management.	ML5-1 Standardize documentation for Asset Management.
		ML2-2 Establish practices to implement Asset Management.	ML3-2 Provide resources for Asset Management.	ML4-2 Review Asset Management activities for effectiveness.	ML5-2 Share Asset Management improvements across the organization.
		ML2-3 Establish a plan for Asset Management.			

DOMAIN: AUDIT AND ACCOUNTABILITY (AA)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C1 Define the content of audit records		L2-1 The content of audit records has been defined to ensure events can be traced back to a specific user. • NIST SP 800-171 3.3.2 • RMM MON:SG1.SP3	L3-1 The list of events to be logged is periodically reviewed and updated. • NIST SP 800-171 3.3.3		
C2 Identify stakeholders		L2-1 The organizational and external entities that rely upon information collected from the audit and accountability process are identified. • RMM MON:SG1:SP3			
C3 Define audit storage requirements		L2-1 The organization has defined audit data storage and retention requirements. • RMM MON:SG1.SP3	L3-1 Organizational systems alert upon audit processing failure. • NIST SP 800-171 3.3.4		
C4 Auditing is performed	L1-1 Audit logs are created and retained, at least in an ad hoc manner. • RMM MON:SG2.SP3 • NIST SP 800-171 3.3.1	L2-1 The organization has a process to create and retain audit logs, ensuring that all events defined are included. • RMM MON:SG2.SP3	L3-1 The organization has a process to enforce detail logging for access or changes to sensitive data. • CIS 7.1: 14.9	L4-1 The organization uses DHCP logging to update asset Inventory. • CIS 7.1: 1.3	
		L2-2 A system capability is provided that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records. • NIST SP 800-171 3.3.7	L3-2 Audit Logs are continuously collected into a central repository. • DIB	L4-2 The organization's monitoring systems are configured to record network packets passing through each of the organization's network boundaries. • CIS 7.1: 12.5	
C5 Audit information is identified and protected		L2-1 Audit information and tools are protected. • NIST SP 800-171 3.3.8 • RMM MON:SG2.SP3	L3-1 Limit management of audit logging functionality to a subset of privileged users. • NIST SP 800-171 3.3.9 • RMM MON:SG2.SP2	L4-1 Audit information is stored on physically different systems than the one generating the audited content. • NIST SP 800-53, Rev. 4 AU-9	

DOMAIN: AUDIT AND ACCOUNTABILITY (AA)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C5 Audit information is identified and protected *(continued)*				L4-2 Cryptographic mechanisms are used to protect audit information. • NIST SP 800-53, Rev. 4 AU-9	
C6 Assign staff to review and manage audit logs		L2-1 Staff are assigned to review and manage audit logs. • NIST SP 800-171 3.3.5		L4-1 Staff are assigned to oversee and guide semi-automated audit log analysis. • DIB	L5-1 Staff are assigned to validate findings from fully automated audit log analysis. • DIB
C7 Audit logs are reviewed	L1-1 Audit logs are reviewed, at least in an ad hoc manner. • NIST SP 800-171 3.3.5	L2-1 Audit logs are reviewed according to an established process. • NIST SP 800-171 3.3.5	L3-1 The organization correlates the audit review, analysis and reporting processes. • NIST SP 800-171 3.3.5	L4-1 Audit information is automatically pre-processed to identify and act on critical indicators. • DIB	
			L3-2 The logging functionality includes audit reduction and report generation capabilities. • NIST SP 800-171 3.3.6	L4-2 Audit information is reviewed for system-wide activity in addition to per-machine activity. • DIB	
C8 The information collected is distributed to the appropriate stakeholders		L2-1 The audit information collected is distributed to the appropriate stakeholders. • RMM MON:SG2.SP4			

DOMAIN: AUDIT AND ACCOUNTABILITY (AA)

MATURITY LEVEL CAPABILITY	PROCESSES				
	Maturity Level 1 (ML1)	Maturity Level 2 (ML2)	Maturity Level 3 (ML3)	Maturity Level 4 (ML4)	Maturity Level 5 (ML5)
Improve Audit and Accountability activities		ML2-1 Establish a policy for Audit and Accountability.	ML3-1 Review Audit and Accountability activities for conformance.	ML4-1 Inform high-level management.	ML5-1 Standardize documentation for Audit and Accountability.
		ML2-2 Establish practices to implement Audit and Accountability.	ML3-2 Provide resources for Audit and Accountability.	ML4-2 Review Audit and Accountability activities for effectiveness.	ML5-2 Share Audit and Accountability improvements across the organization.
		ML2-3 Establish a plan for Audit and Accountability.			

DOMAIN: AWARENESS AND TRAINING (AT)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C1 The security awareness needs of the organization are identified		L2-1 Awareness training requirements are established for managers, system administrators and users to address the security risks associated with their activities and of the applicable policies, standards, and procedures. • NIST SP 800-171 3.2.1 • RMM OTA:SG1.SP1	L3-1 Awareness training requirements are updated for managers, systems administrators and users as appropriate to address the security risks associated with their activities and of the applicable policies, standards, and procedures. • RMM OTA:SG1.SP2	L4-1 Awareness training requirements include 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. • NIST SP 800-171B 3.2.1e	
			L3-2 Awareness training requirements include recognizing and reporting potential indicators of insider threat. • NIST SP 800-171 3.2.3	L4-2 Practical exercises in awareness training that are aligned with current threat scenarios are included in training. • NIST SP 800-171B 3.2.2e	
C2 Security awareness activities are conducted for the organization		L2-1 The organization has a process for conducting security awareness training. • RMM OTA:SG2.SP1	L3-1 The organization has a process for maintaining security awareness training records. • RMM OTA:SG2.SP2	L4-1 Feedback is provided to individuals involved in awareness training and their supervisors. • NIST SP 800-171B 3.2.2e • RMM OTA:SG2.SP3	
C3 The training capabilities for information security-related duties and responsibilities within the organization are identified		L2-1 Training requirements for information security-related duties and responsibilities are established. • RMM OTA:SG3.SP1	L3-1 The training requirements for information security-related duties and responsibilities within the organization are periodically reviewed and updated. • RMM OTA:SG3.SP2	L4-1 The organization trains defensive cyber operations personnel to have full enterprise cyber understanding in order to reduce the negative impact of their defensive actions. • CSF: DE.CM-8 • CIS: 3.1, 3.2, 3.4, 3.5, 3.6, 3.7	
				L4-2 The organization leverages information from threat analysis to update training to security practitioners and administrators responsible for managing IT assets. • CSF: PR.AT-2, PR.AT-5	

DOMAIN: AWARENESS AND TRAINING (AT)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C4 Training is conducted for those with information security-related duties and responsibilities within the organization		L2-1 The organization trains personnel to carry out their assigned information security-related duties and responsibilities. • NIST SP 800-171 3.2.2 • RMM OTA:SG4.SP1	L3-1 The organization has a process for maintaining information security-related training records. • RMM OTA:SG4.SP2	L4-1 Feedback is provided to individuals involved in information security-related training and their supervisors. • NIST SP 800-171B 3.2.2e • RMM OTA:SG4.SP2	
				L4-2 The organization implements cross training of administrators and defensive cyber operations personnel. • DIB	

DOMAIN: AWARENESS AND TRAINING (AT)

MATURITY LEVEL CAPABILITY	PROCESSES				
	Maturity Level 1 (ML1)	Maturity Level 2 (ML2)	Maturity Level 3 (ML3)	Maturity Level 4 (ML4)	Maturity Level 5 (ML5)
Improve Awareness and Training activities		ML2-1 Establish a policy for Awareness and Training.	ML3-1 Review Awareness and Training activities for conformance.	ML4-1 Inform high-level management.	ML5-1 Standardize documentation for Awareness and Training.
		ML2-2 Establish practices to implement Awareness and Training.	ML3-2 Provide resources for Awareness and Training.	ML4-2 Review Awareness and Training activities for effectiveness.	ML5-2 Share Awareness and Training improvements across the organization.
		ML2-3 Establish a plan for Awareness and Training.			

DOMAIN: CONFIGURATION MANAGEMENT (CM)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C1 Establish change management requirements		L2-1 The organization has a change management process used to manage modifications to assets. • RMM ADM:SG3.SP2 • NIST SP 800-171 3.4.3			
C2 Establish configuration management requirements		L2-1 The organization establishes configuration management requirements for information technology. • NIST SP 800-171 3.4.2 • RMM ADM:SG3:SP1	L3-1 The organization has established requirements for which personnel are authorized to make changes and how/when those changes are permitted. • NIST SP 800-171 3.4.5		
C3 Configuration baselines are established	L1-1 Configuration baselines for organizational systems are established, at least in an ad hoc manner. • RMM KIM:SG5.SP2 • NIST SP 800-171 3.4.1	L2-1 Configuration baselines for organization systems are based on established requirements. • RMM KIM:SG5.SP2	L3-1 The organization restricts, disables, or prevents the use of nonessential programs, functions, ports, protocols, and services. • NIST SP 800-171 3.4.7	L4-1 The organization establishes and maintains an authoritative source and repository for configuration baselines of organizational systems. • NIST SP 800-171B 3.4.1e	
		L2-2 Configuration baselines for information technology employ the principle of least functionality. • NIST SP 800-171 3.4.6	L3-2 The organization applies 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. • NIST SP 800-171 3.4.8	L4-2 Employs an application vetting process prior to adding to application whitelists. • CIS 2.7,2.8 (Libraries) • CIS 2.9 (Scripts)	
		L2-3 Configuration baselines for information technology include requirements for user installed software. • NIST SP 800-171 3.4.9			
C4 Configuration and change management is performed		L2-1 The organization tracks, reviews, manages, and log changes to organizational systems based on the change management process. • NIST SP 800-171 3.4.3 • RMM KIM:SG5.SP2			

DOMAIN: CONFIGURATION MANAGEMENT (CM)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C4 Configuration and change management is performed *(continued)*		L2-2 Established security requirements are analyzed to determine impacts prior to change implementation. • NIST SP 800-171 3.4.4			
C5 Configuration management is performed	L1-1 The organization performs configuration management for organizational systems, at least in an ad hoc manner. • NIST SP 800-171 3.4.2 • RMM KIM:SG5.SP2	L2-1 The organization performs configuration management for organizational systems based on established requirements. • NIST SP 800-171 3.4.2 • RMM KIM:SG5.SP2	L3-1 The organization assigns authorized and trained personnel to perform change management processes. • NIST SP 800-171 3.4.5	L4-1 The organization employs automated mechanisms to detect misconfigured and unauthorized system configurations. • NIST SP 800-171B 3.4.2e	L5-1 The organization fully automates real-time configuration management, including inventory tracking and configuration identification, verification, and enforcement for all connected systems. • DIB
				L4-2 Employs configuration enforcement with adjustable, permissive to restrictive, modes based on threat and/or mission state. • NIST SP 800-171B 3.4.2e	
				L4-3 Employ roots of trust, formal verification, or cryptographic signatures to verify the integrity and correctness of security critical or essential software. • NIST SP 800-171B: 3.14.1e	
C5 Configuration management is performed (continued)				L4-4 The organization manages and controls the configuration of Internet of Things (IoT) devices, embedded systems, industrial control systems, real-time systems, and other hosts without a general purpose operating system, where possible. • NIST SP 800-171B: 3.14.3e	

DOMAIN: CONFIGURATION MANAGEMENT (CM)

MATURITY LEVEL CAPABILITY	PROCESSES				
	Maturity Level 1 (ML1)	Maturity Level 2 (ML2)	Maturity Level 3 (ML3)	Maturity Level 4 (ML4)	Maturity Level 5 (ML5)
Improve Configuration Management activities		ML2-1 Establish a policy for Configuration Management.	ML3-1 Review Configuration Management activities for conformance.	ML4-1 Inform high-level management.	ML5-1 Standardize documentation for Configuration Management.
		ML2-2 Establish practices to implement Configuration Management.	ML3-2 Provide resources for Configuration Management.	ML4-2 Review Configuration Management activities for effectiveness.	ML5-2 Share Configuration Management improvements across the organization.
		ML2-3 Establish a plan for Configuration Management.			

DOMAIN: CYBERSECURITY GOVERNANCE (CG)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C1 Define cybersecurity objectives	L1-1 Cybersecurity objectives are established for the organization, at least in an ad hoc manner. • RMM EF:SG1.SP1	L2-1 The organization has documented, implemented, and communicated (to all appropriate stakeholders) cybersecurity objectives. • RMM EF:SG1.SP1	L3-1 The organization has a defined process for managing cybersecurity objectives. • RMM EF:SG1:SP1	L4-1 The organization periodically reviews and updates cybersecurity objectives. • RMM EF:SG1:SP1	
		L2-2 The organization has a defined plans for achieving cybersecurity objectives. • DIB			
C2 Define cybersecurity critical success factors		L2-1 The organization has documented, implemented, and communicated (to all appropriate stakeholders) cybersecurity critical success factors. • RMM EF:SG1.SP1	L3-1 The organization has a defined process for managing cybersecurity critical success factors. • RMM EF:SG1.SP1	L4-1 The organization periodically reviews and updates cybersecurity critical success factors. • RMM EF:SG1.SP1	
C3 Manage cybersecurity plans	L1-1 Cybersecurity objectives are implemented in the organization, at least in an ad hoc manner. • RMM EF:SG1.SP1	L2-1 Cybersecurity objectives are implemented through defined cybersecurity plans. • RMM EF:SG1.SP1	L3-1 The organization has aligned funding, staffing, and accountability to cybersecurity plans. • RMM EF:SG3.SP1	L4-1 The organization collects, monitors, and controls performance data for defined cybersecurity plans. • RMM EF:SG2.SP1	
		L2-2 The cybersecurity plans include policies and procedures to carry out the organization's defined cybersecurity objectives. • DIB		L4-2 Senior management is informed on the performance of cybersecurity plans. • RMM EF:SG3.SP1	
C4 Manage cybersecurity critical success factors		L2-1 Cybersecurity critical success factors are established and monitored. • RMM EF:SG1.SP1	L3-1 The organization has aligned funding, staffing, and accountability to cybersecurity critical success factors. • RMM EF:SG3.SP1	L4-1 The organization collects, monitors, and controls performance data for cybersecurity critical success factors. • RMM EF:SG2.SP1	
				L4-2 Senior management is informed on the performance of cybersecurity critical success factors. • RMM EF:SG3.SP1	

DOMAIN: CYBERSECURITY GOVERNANCE (CG)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C4 Manage cybersecurity critical success factors *(continued)*				L4-3 The organization creates and maintains a business impact assessment including systems, data, and infrastructure. • CSF: ID.AM-3, ID-BE.1, ID.BE-2, ID.BE-4, ID.RA-4, DE.AE-1	
				L4-4 The organization creates and maintains a business impact assessment from adverse cyber activities to inform cybersecurity prioritization and incident response. • CSF: ID.BE-4	
				L4-5 The organization identifies and incorporates risk metrics and measures to monitor and improve cybersecurity governance	

DOMAIN: CYBERSECURITY GOVERNANCE (CG)

MATURITY LEVEL CAPABILITY	PROCESSES				
	Maturity Level 1 (ML1)	Maturity Level 2 (ML2)	Maturity Level 3 (ML3)	Maturity Level 4 (ML4)	Maturity Level 5 (ML5)
Improve Cybersecurity Governance activities		ML2-1 Establish a policy for Cybersecurity Governance.	ML3-1 Review Cybersecurity Governance activities for conformance.	ML4-1 Inform high-level management.	ML5-1 Standardize documentation for Cybersecurity Governance.
		ML2-2 Establish practices to implement Cybersecurity Governance.	ML3-2 Provide resources for Cybersecurity Governance.	ML4-2 Review Cybersecurity Governance activities for effectiveness.	ML5-2 Share Cybersecurity Governance improvements across the organization.
		ML2-3 Establish a plan for Cybersecurity Governance.			

DOMAIN: IDENTIFICATION AND AUTHORIZATION (IDA)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C1 System users, processes and devices are identified before access is granted	L1-1 The organization identifies system users, processes acting on behalf of users, and devices, at least in an ad hoc manner. • NIST SP 800-171 3.5.1	L2-1 A process exists to identify system users, processes acting on behalf of users, and devices. • NIST SP 800-171 3.5.1			
	L1-2 The identities of users, processes, or devices are authenticated (or verified) as a prerequisite to allowing access to organizational systems. • NIST SP 800-171 3.5.2				
C2 Access is granted to authorized entities			L3-1 Multi-factor authentication is used for local and network access to privileged accounts and for network access to non-privileged accounts. • NIST SP 800-171 3.5.3	L4-1 Require multi-factor authentication for all user accounts, on all systems, whether managed on-site or by a third-party provider. • CIS 16.3	L5-1 The organization eliminates the use of dynamic passwords by unprivileged system users through the application of alternate means of knowledge-based or other authentication mechanisms.
			L3-2 The organization employs replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. • NIST SP 800-171 3.5.4	L4-2 Employ password managers for the generation, rotation, and management of passwords for systems and system components that do not support MFA or complex account management. • NIST SP 800-171B: 3.5.2E	L5-2 The organization's authentication and authorization scheme uses step up authentication in response to behavioral anomalies to add layers, factors, and/or forms of authentication to authorize access. • DIB
			L3-3 The organization prevents the reuse of identifiers for a defined period. • NIST SP 800-171 3.5.5		L5-3 Identify and authenticate systems and system components before establishing a network connection using bidirectional authentication that is cryptographically-based and replay resistant. • NIST SP 800-171B 3.5.1E
			L3-4 The organization disables identifiers after a defined period of inactivity. • NIST SP 800-171 3.5.6		

DOMAIN: IDENTIFICATION AND AUTHORIZATION (IDA)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C2 Access is granted to authorized entities *(continued)*			L3-5 A minimum password complexity, including change of characters, is defined and enforced. • NIST SP 800-171 3.5.7		
			L3-6 Password are prohibited from being reused for a specified number of generations. • NIST SP 800-171 3.5.8		
			L3-7 The organization allows temporary passwords for initial logon, but enforces a mandatory immediate change to permanent passwords. • NIST SP 800-171 3.5.9		
			L3-8 The organization ensures that all stored and transmitted passwords are cryptographically protected. • NIST SP 800-171 3.5.10		
			L3-9 Feedback of authentication information is obscured. • NIST SP 800-171 3.5.11		

DOMAIN: IDENTIFICATION AND AUTHORIZATION (IDA)

MATURITY LEVEL CAPABILITY	PROCESSES				
	Maturity Level 1 (ML1)	Maturity Level 2 (ML2)	Maturity Level 3 (ML3)	Maturity Level 4 (ML4)	Maturity Level 5 (ML5)
Improve Identification and Authorization activities		ML2-1 Establish a policy for Identification and Authorization.	ML3-1 Review Identification and Authorization activities for conformance.	ML4-1 Inform high-level management.	ML5-1 Standardize documentation for Identification and Authorization.
		ML2-2 Establish practices to implement Identification and Authorization.	ML3-2 Provide resources for Identification and Authorization.	ML4-2 Review Identification and Authorization activities for effectiveness.	ML5-2 Share Identification and Authorization improvements across the organization.
		ML2-3 Establish a plan for Identification and Authorization.			

DOMAIN: INCIDENT RESPONSE (IR)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C1 Detect and report events	L1-1 Events are detected and reported, at least in an ad hoc manner. • RMM IMC:SG2.SP1	L2-1 The organization has a process for detecting and reporting events. • RMM IMC:SG2.SP1	L3-1 Events are analyzed to determine if they relate to other events. • RMM IMC:SG2.SP4	L4-1 The organization identifies and classifies events in a semi-automated fashion. • CSF: DE.AE-2, DE.AE-3, DE-AE-4	
		L2-2 The organization has a process for categorizing events. • RMM IMC:SG2.SP4	L3-2 Events are prioritized. • RMM IMC:SG2.SP4		
		L2-3 The organization has a process for managing events to resolution. • RMM IMC:SG2.SP4			
		L2-4 A repository is established for tracking events. • RMM IMC:SG2.SP1			
C2 Define and maintain criteria for declaring incidents		L2-1 A repository is established for tracking incidents. • RMM IMC:SG2.SP2	L3-1 The criteria for declaring incidents is defined. • RMM IMC:SG3.SP1		
C3 Declare and report incidents	L1-1 Incidents are declared, at least in an ad hoc manner. • RMM IMC:SG3:SP1	L2-1 The organization has a process for declaring and reporting incidents to appropriate stakeholders. • RMM IMC:SG3.SP1			
C4 Escalate incidents to appropriate stakeholders for input and resolution		L2-1 The organization has a process for escalating incidents to appropriate stakeholders for input and resolution. • RMM IMC:SG4.SP1			L5-1 The organization fully employs autonomous initial response actions at machine speed and based on the current security policy and posture, without needing human intervention.
C5 Develop and implement a response to a declared incident	L1-1 Incidents are resolved, at least in an ad hoc manner. • RMM IMC:SG4.SP1	L2-1 The organization has a process for analyzing incidents to determine a response. • RMM IMC:SG3.SP2 • NIST SP 800-171 3.6.1	L3-1 The incident management capability is tested. • NIST SP 800-171 3.6.3	L4-1 The organization maintains a security operations center during relevant business hours with on call response after hours. • NIST SP 800-171B 3.6.1e	L5-1 The organization maintains a full-time security operations center. • NIST SP 800-171B 3.6.1e

DOMAIN: INCIDENT RESPONSE (IR)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C5 Develop and implement a response to a declared incident *(continued)*		L2-2 The organization has a process for developing and implementing responses including preparation, detection, analysis, containment, recovery, and user response activities. • RMM IMC:SG4.SP1 • NIST SP 800-171 3.6.1	L3-2 Test the organizational incident response capability. • NIST SP 800-171 3.6.3	L4-2 The incident management capabilities (including the SOC and CIRT) are tested and improved based on test results. • RMM IMC:SG1.SP1	L5-2 Employs autonomous response and mitigation actions (SOAR) for communications and collaboration technologies.
		L2-3 Incidents are tracked to resolution. • RMM IMC:SG4.SP4		L4-3 The organization uses a combination of manual and real-time responses to anomalous activities that matches incident patterns.	L5-3 The organization establishes and maintains a cyber incident response team that can be deployed to any location within 24 hours. • NIST SP 800-171B 3.6.2e
		L2-4 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. • NIST SP 800-171 3.6.1			
C6 Communicate incidents to relevant stakeholders as appropriate		L2-1 The organization has a process for communicating incident status and responses to affected parties. • RMM IMC:SG4.SP3 • NIST SP 800-171 3.6.2			
		L2-2 Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization. • NIST SP 800-171 3.6.2			
C7 Manage incidents to resolution		L2-1 The organization has a process for managing incidents to resolution including: declaring, escalating, and developing and implementing a response. • RMM IMC:SG1.SP1			

DOMAIN: INCIDENT RESPONSE (IR)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C7 Manage incidents to resolution *(continued)*		L2-2 Roles and responsibilities for managing incidents have been established and staff has been assigned. • RMM IMC:SG1.SP2			
C8 Perform post incident reviews to determine underlying causes			L3-1 Root cause analysis is performed on incidents to determine underlying causes. • RMM IMC:SG5.SP1	L4-1 Lessons learned from incident management is translated into improvements in organizational processes for asset protection and continuity. • RMM IMC:SG5.SP3	L5-1 The organization continually evaluates and improves incident response processes by performing simulated tabletop exercises half of which are unannounced. • DIB
			L3-2 Incidents are analyzed to determine if the incident is linked to other processes within the organization. • RMM IMC:SG5.SP3	L4-2 Establishes and improves response plans based on type and severity of incident to drive effective use of people and tools. • CSF: RS-AN-4	L5-2 The organization applies proactive, real-time forensics data gathering across all connected devices, securely transferring data in real time to forensics repositories to prevent log revision. • DIB
				L4-3 The organization periodically reviews incident response plans to ensure effectiveness across the enterprise. • CSF: RM.IM-1, RS.IM-2	L5-3 The organization employs automated, real-time methods to measure actual incidence response effectiveness for further analysis and lessons learned. • DIB
C9 Plan incident response				L4-1 Demonstrates an ability to use knowledge of attacker tactics, techniques, and procedures in incident response planning and execution.	
				L4-2 The organization implements pre-planned responses to threats. • CSF: RS-RP-1, RS.CO-1 • CIS: 19.1	

DOMAIN: INCIDENT RESPONSE (IR)

MATURITY LEVEL CAPABILITY	PROCESSES				
	Maturity Level 1 (ML1)	Maturity Level 2 (ML2)	Maturity Level 3 (ML3)	Maturity Level 4 (ML4)	Maturity Level 5 (ML5)
Improve Incident Response activities		ML2-1 Establish a policy for Incident Response.	ML3-1 Review Incident Response activities for conformance.	ML4-1 Inform high-level management.	ML5-1 Standardize documentation for Incident Response.
		ML2-2 Establish practices to implement Incident Response.	ML3-2 Provide resources for Incident Response.	ML4-2 Review Incident Response activities for effectiveness.	ML5-2 Share Incident Response improvements across the organization.
		ML2-3 Establish a plan for Incident Response.			

DOMAIN: MAINTENANCE (MA)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C1 Maintenance is performed	L1-1 The organization performs maintenance on its organizational systems, at least in an ad hoc manner. • NIST SP 800-171 3.7.1 • RMM TM:SG5.SP2	L2-1 The organization schedules, performs, and reviews records of maintenance activities performed on organizational systems. • NIST SP 800-171 3.7.1 • RMM TM:SG5.SP2			
C2 Maintenance is controlled		L2-1 The organization identifies approved tools and techniques to conduct system maintenance. • NIST SP 800-171 3.7.2			
		L2-2 The organization identifies and implements controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. • NIST SP 800-171 3.7.2			
		L2-3 The organization identifies multifactor authentication requirements for maintenance sessions via external network connections. • NIST SP 800-171 3.75	L3-1 The organization follows information asset disposal guidelines for equipment removed for off-site maintenance. • NIST SP 800-171 3.7.3	L4-1 All maintenance systems are treated as if they contain the highest level of CUI data contained on any system they maintain. • CSF: PR.MA-1, PR.MA-2	
		L2-4 The organization supervises maintenance activities of personnel without required access authorization. • NIST SP 800-171 3.7.6	L3-2 The organization scans media containing diagnostic and test programs for malicious code before using the media in organizational systems. • NIST SP 800-171 3.7.4		

DOMAIN: MAINTENANCE (MA)

MATURITY LEVEL CAPABILITY	PROCESSES				
	Maturity Level 1 (ML1)	Maturity Level 2 (ML2)	Maturity Level 3 (ML3)	Maturity Level 4 (ML4)	Maturity Level 5 (ML5)
Improve Maintenance activities		ML2-1 Establish a policy for Maintenance.	ML3-1 Review Maintenance activities for conformance.	ML4-1 Inform high-level management.	ML5-1 Standardize documentation for Maintenance.
		ML2-2 Establish practices to implement Maintenance.	ML3-2 Provide resources for Maintenance.	ML4-2 Review Maintenance activities for effectiveness.	ML5-2 Share Maintenance improvements across the organization.
		ML2-3 Establish a plan for Maintenance.			

DOMAIN: MEDIA PROTECTION (MP)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C1 Media is identified		L2-1 The organization has a process for identifying non-digital and digital media containing CUI. • NIST SP 800-171 3.8.1 • RMM MON:SG2.SP4			
C2 Media is protected		L2-1 The organization has a process for physically protecting media (non-digital and digital) containing CUI. • NIST SP 800-171 3.8.1 • KIM:SG2.SP2	L3-1 The organization has a process for implementing cryptographic mechanisms to protect the confidentiality of CUI digital data at rest. • CIS 7.1: 14.8		
		L2-2 The organization has a process for limiting access to media containing CUI to authorized users. • NIST SP 800-171 3.8.2 • RMM MON:SG2.SP4			
C3 Media is sanitized	L1-1 Non-digital and digital media containing CUI is sanitized or destroyed before disposal or release for reuse, at least in an ad hoc manner. •NIST SP 800-171 3.8.3	L2-1 The organization has a process for sanitizing or destroying non-digital and digital media containing CUI before disposal or release for reuse. • NIST SP 800-171 3.8.3			
C4 Media is marked			L3-1 The organization has a process for marking media with necessary CUI markings and distribution limitations. • NIST SP 800-171 3.8.4 • RMM MON:SG2.SP4		

DOMAIN: MEDIA PROTECTION (MP)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C5 Media is protected during transport			L3-1 The organization has a process for controlling access to media containing CUI to control and maintain accountability during transport outside of controlled areas. • NIST SP 800-171 3.8.5 • RMM MON:SG2.SP4		L5-1 Maintains consistent awareness of the locations and times of use of removable media storing critical technology CUI, and can take action to mitigate risk of compromise leveraging this information. • CSF: PR.PT-2
			L3-2 The organization has a process for implementing cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport (unless otherwise protected by alternative physical safeguards). • NIST SP 800-171 3.8.6		
C6 Control the use of removable media on system components		L2-1 The organization has a process for controlling the use of removable media on system components. • NIST SP 800-171 3.8.7 • RMM MON:SG2.SP4			
C7 Prohibit the use of portable storage devices when such devices have no identifiable owner			L3-1 The organization has a process that prohibits the use of portable storage devices which have no identifiable owner. • NIST SP 800-171 3.8.8 • RMM MON:SG2.SP4		
C8 Protect the confidentiality of backup CUI at storage locations		L2-1 The organization has a process to protect the confidentiality of backup CUI at storage locations. • NIST SP 800-171 3.8.9 • RMM MON:SG2.SP4			

DOMAIN: MEDIA PROTECTION (MP)

MATURITY LEVEL CAPABILITY	PROCESSES				
	Maturity Level 1 (ML1)	Maturity Level 2 (ML2)	Maturity Level 3 (ML3)	Maturity Level 4 (ML4)	Maturity Level 5 (ML5)
Improve Media Protection activities		ML2-1 Establish a policy for Media Protection.	ML3-1 Review Media Protection activities for conformance.	ML4-1 Inform high-level management.	ML5-1 Standardize documentation for Media Protection.
		ML2-2 Establish practices to implement Media Protection.	ML3-2 Provide resources for Media Protection.	ML4-2 Review Media Protection activities for effectiveness.	ML5-2 Share Media Protection improvements across the organization.
		ML2-3 Establish a plan for Media Protection.			

DOMAIN: PERSONNEL SECURITY (PS)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C1 Screen personnel	L1-1 Individuals are screened prior to authorizing access to organizational systems containing CUI at least in an ad hoc manner. • NIST SP 800-171 3.9.1 • RMM HRM:SG2.SP1	L2-1 The organization has a process for screening individuals prior to authorizing access to organizational systems containing CUI. • NIST SP 800-171 3.9.1 • RMM HRM:SG2.SP1		L4-1 The organization has a process for conducting enhanced personnel screening and rescreening on an ongoing basis. • NIST SP 800-171B 3.9.1e • RMM AM:SG1.SP2 • RMM AM:GG2.GP8	
C2 Protect CUI during personnel actions	L1-1 CUI is protected during personnel actions at least in an ad hoc manner. • NIST SP 800-171 3.9.2 • RMM HRM:SG4.SP2	L2-1 The organization has a process to ensure CUI is protected during personnel actions. • NIST SP 800-171 3.9.2 • RMM HRM:SG4.SP2			

DOMAIN: PERSONNEL SECURITY (PS)

MATURITY LEVEL CAPABILITY	PROCESSES				
	Maturity Level 1 (ML1)	Maturity Level 2 (ML2)	Maturity Level 3 (ML3)	Maturity Level 4 (ML4)	Maturity Level 5 (ML5)
Improve Personnel Security activities		ML2-1 Establish a policy for Personnel Security.	ML3-1 Review Personnel Security activities for conformance.	ML4-1 Inform high-level management.	ML5-1 Standardize documentation for Personnel Security.
		ML2-2 Establish practices to implement Personnel Security.	ML3-2 Provide resources for Personnel Security.	ML4-2 Review Personnel Security activities for effectiveness.	ML5-2 Share Personnel Security improvements across the organization.
		ML2-3 Establish a plan for Personnel Security.			

DOMAIN: PHYSICAL PROTECTION (PP)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C1 Identify organizational systems, equipment, and respective operating environments that require limiting physical access		L2-1 The organization identifies systems, equipment, and respective operating environments that require limited physical access. • RMM KIM:SG4.SP2			
C2 Develop physical access requirements for identified organizational systems, equipment, and respective operating environments		L2-1 The organization develops physical access and audit requirements for identified organizational systems, equipment, and respective operating environments. • NIST SP 800-171 3.10.1	L3-1 The organization develops security requirements for alternate work sites. • NIST SP 800-171 3.10.6		
		L2-2 The organization develops security requirements for visitors. • NIST SP 800-171 3.10.3			
		L2-3 The organization develops access and audit requirements for physical access devices (keys, locks, card readers, etc.). • NIST SP 800-171 3.10.5			
		L2-4 The organization develops security requirements for the physical facility and supporting infrastructure. • NIST SP 800-171 10.3.2			
C3 Manage physical access requirements for identified organizational systems, equipment, and respective operating environments			L3-1 The organization reviews and updates physical security requirements at a frequency defined by the organization. • NIST SP 800-171 3.10.*		

DOMAIN: PHYSICAL PROTECTION (PP)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C4 Limit physical access to organizational systems, equipment, and respective operation environments based on defined physical security access requirements	L1-1 The organization limits physical access to systems, equipment, and the respective operating environment, at least in an ad hoc manner. • NIST SP 800-171 3.10.1 • RMM KIM:SG4.SP2	L2-1 The organization protects and monitors the physical facility and support infrastructure based on established requirements. • NIST SP 800-171 3.10.1 • RMM KIM:SG4.SP2	L3-1 The organization enforces security requirements at alternate work sites. • NIST SP 800-171 3.10.6		
	L1-2 The organization controls and manages physical access to devices, at least in an ad hoc manner. • NIST SP 800-171 3.10.5 • RMM KIM:SG4.SP2	L2-2 The organization controls and manages physical access to devices based on established requirements. • NIST SP 800-171 3.10.5 • RMM KIM:SG4.SP2			
C5 Monitor physical facilities for adherence to physical security access requirements	L1-1 The organization escorts visitors and monitors visitor activity, at least in an ad hoc manner. • NIST SP 800-171 3.10.3	L2-1 The organization escorts visitors and monitors visitor activity based on established requirements. • NIST SP 800-171 3.10.3			
	L1-2 The organization maintains audit logs of physical access, at least in an ad hoc manner. • NIST SP 800-171 3.10.4	L2-2 The organization protects and monitors the physical facility and support infrastructure based on established requirements. • NIST SP 800-171 3.10.2			
		L2-3 The organization maintains audit logs of physical access based on established requirements. • NIST SP 800-171 3.10.4			

DOMAIN: PHYSICAL PROTECTION (PP)

MATURITY LEVEL CAPABILITY	PROCESSES				
	Maturity Level 1 (ML1)	Maturity Level 2 (ML2)	Maturity Level 3 (ML3)	Maturity Level 4 (ML4)	Maturity Level 5 (ML5)
Improve Physical Protection activities		ML2-1 Establish a policy for Physical Protection.	ML3-1 Review Physical Protection activities for conformance.	ML4-1 Inform high-level management.	ML5-1 Standardize documentation for Physical Protection.
		ML2-2 Establish practices to implement Physical Protection.	ML3-2 Provide resources for Physical Protection.	ML4-2 Review Physical Protection activities for effectiveness.	ML5-2 Share Physical Protection improvements across the organization.
		ML2-3 Establish a plan for Physical Protection.			

DOMAIN: RECOVERY (RE)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C1 Manage back-ups		L2-1 Automated information back-ups are regularly performed. • ISO 27001 A.12.3.1 • CSF: PR.IP-4, CIS 7.1 10.1	L3-1 Complete and automated system back-ups are regularly performed. • CIS 7.1: 10.1, 10.2	L4-1 Ensure all back-ups have at least one offline back-up destination. • CIS 7.1: 10.5	
		L2-2 Data on back-up media is routinely tested. • CIS 7.1 10.3			
C2 Manage information security continuity		L2-1 Implement information security continuity. • ISO 27001 A.17.1.2	L3-1 Develop an information security continuity plan that includes redundancy and availability requirements. • ISO 27001 A.17.1.1	L4-1 The organization periodically tests information security continuity controls. • ISO 27001 A.17.1.3	
			L3-2 Ensure information processing facilities meet redundancy and availability requirements. • ISO 27001 A.17.2.1		

DOMAIN: RECOVERY (RE)

MATURITY LEVEL CAPABILITY	PROCESSES				
	Maturity Level 1 (ML1)	Maturity Level 2 (ML2)	Maturity Level 3 (ML3)	Maturity Level 4 (ML4)	Maturity Level 5 (ML5)
Improve Recovery activities		ML2-1 Establish a policy for Recovery.	ML3-1 Review Recovery activities for conformance.	ML4-1 Inform high-level management.	ML5-1 Standardize documentation for Recovery.
		ML2-2 Establish practices to implement Recovery.	ML3-2 Provide resources for Recovery.	ML4-2 Review Recovery activities for effectiveness.	ML5-2 Share Recovery improvements across the organization.
		ML2-3 Establish a plan for Recovery.			

DOMAIN: RISK MANAGEMENT (RM)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C1 Determine risk categories, risk sources, and risk measurement criteria			L3-1 The organization has documented risk sources, risk categories, risk tolerances, and risk measurement criteria. • RMM RISK:SG1.SP1	L4-1 Develops threat models appropriate to the environment to inform risk management. • DIB	
			L3-2 The organization has a risk management strategy that defines the processes for identifying, analyzing, managing, and mitigating risk. • RMM RISK:SG1	L4-2 Determination of risk tolerance is informed by the organization's role in critical infrastructure and sector specific risk analysis. • CSF: ID.RM-1, ID.RM-3	
			L3-3 The organization has processes established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources. • CSF: RS.AN-5		
C2 Document organizational risk		L2-1 The organization has a process for recording risks in the risk register or structured risk repository. • NIST SP 800-171 3.11.1 • RMM RISK:SG2.SP2 • RMM RISK:SG5.SP1 • RMM RISK:SG5.SP2			
C3 Identify risk		L2-1 The organization has a process for identifying risks. • RMM RISK:SG3	L3-1 Risk assessments are performed to identify risks according to the defined risk categories, risk sources, and risk measurement criteria. • RMM RISK:SG3	L4-1 Threat profiles and adversary TTPs are cataloged and routinely updated. • CSF: DE.AE-2	L5-1 The organization employs advanced automation and analytics capabilities to predict and identify risks to organizations, systems, or system components. • NIST SP 800-171B 3.11.3e
		L2-2 Vulnerability scans are performed to identify new vulnerabilities. • NIST SP 800-171 3.11.2		L4-2 The organization creates threat profiles for organizational assets and likely targets based on threat intelligence. • CSF: ID.RA-2, ID.RA-3 • NIST SP 800-171B 3.11.1e	

DOMAIN: RISK MANAGEMENT (RM)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C3 Identify risk *(continued)*				L4-3 Vulnerability scans are performed in an automated manner • DIB	
				L4-4 Scan are performed for unauthorized connections across trusted network boundaries. • CIS 7.1: 12.2	
C4 Evaluate and prioritize risk based on defined measurement criteria		L2-1 The organization has a process for periodically analyzing risks. • NIST SP 800-171 3.11.1 • RMM RISK:SG4		L4-1 The system and security architecture, system components, boundary isolation or protection mechanisms, and dependencies on external service providers is used to perform risk analysis. • NIST SP 800-171B 3.11.4e	
		L2-2 The organization has a process for prioritizing risks. • RMM RISK:SG4.SP3			
C5 Manage risk		L2-1 The organization has a process to assign a risk disposition. • RMM RISK:SG4.SP3 • RMM RISK:SG5.SP1 • RMM RISK:SG5.SG2	L3-1 The organization has a process to develop and implement risk mitigation plans. • RMM RISK:SG5.SP1	L4-1 Risk mitigation plans are assessed to ensure they are effective and the results are communicated to management. • DIB	L5-1 The effectiveness of security solutions are assessed at least annually to address anticipated risk to the system and the organization based on current and accumulated threat intelligence. • NIST SP 800-171B 3.11.5e • RMM RISK:SG6.SP1
		L2-2 Risk mitigation plans are developed. • RMM RISK:SG5.SP1	L3-2 Risk responses are tracked to ensure responses are met. • RMM RISK:SG4.SP3	L4-2 Maintains a list of trustworthy vendors based on past performance and prior vetting or assessment outcomes. • NIST SP 800-171B: 3.11.6e	L5-2 Maintains a process to prioritize subcontractors and vendors who incorporate anti-tamper techniques in delivered hardware and software. • DIB

DOMAIN: RISK MANAGEMENT (RM)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C5 Manage risk *(continued)*		L2-3 Risk mitigation plans are implemented. • RMM RISK:SG5.SP1		L4-3 Organization applies cybersecurity elements to Governance, Risk, and Compliance (GRC) processes. • DIB	L5-3 The organization procures sensitive products or services using methods to obfuscate the true identity of the purchaser, and purchases functionally similar products from multiple vendors where possible. • DIB
		L2-4 Actions are taken to manage exposure to vulnerabilities. • RMM VAR:SG3:SP1 • NIST SP 800-171 3.11.3		L4-4 Non-vendor-supported products (e.g., end of life) are managed separately and restricted as necessary to reduce risk. • DIB	L5-4 The organization applies additional risk-based monitoring (on a case-by-case basis) to software that is permitted to execute by exception. • DIB
C6 Manage supply chain risk				L4-1 Supply chain management processes are periodically reviewed, properly resourced, and improved across the enterprise. • NIST SP 800-171B: 3.11.7e (partial)	L5-1 The organization uniformly includes requirements for and incentivizes the use of anti-tamper techniques for subcontracted hardware and software. • DIB
				L4-2 Preserve integrity of supplier software, hardware, and firmware through the combined use of integrity measurement, data labeling, and source authentication. • NIST SP 800-171B: 3.14.1e (interpreted for supply chain)	
				L4-3 Develop and update as required, a plan for managing supply chain risks associated with organizational systems. • NIST SP 800-171B: 3.11.7e	
C6 Manage supply chain risk *(continued)*				L4-4 Employs periodic monitoring of supply chain including the use of third-party services leveraging Publicly Available Information (PAI). • NIST SP 800-171B: 3.11.6e	

DOMAIN: RISK MANAGEMENT (RM)

MATURITY LEVEL CAPABILITY	PROCESSES				
	Maturity Level 1 (ML1)	Maturity Level 2 (ML2)	Maturity Level 3 (ML3)	Maturity Level 4 (ML4)	Maturity Level 5 (ML5)
Improve Risk Management activities		ML2-1 Establish a policy for Risk Management.	ML3-1 Review Risk Management activities for conformance.	ML4-1 Inform high-level management.	ML5-1 Standardize documentation for Risk Management.
		ML2-2 Establish practices to implement Risk Management.	ML3-2 Provide resources for Risk Management.	ML4-2 Review Risk Management activities for effectiveness.	ML5-2 Share Risk Management improvements across the organization.
		ML2-3 Establish a plan for Risk Management.			

DOMAIN: SECURITY ASSESSMENT (SAS)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C1 Develop a system security plan		L2-1 Develop and document a system security plan that defines security requirements for the organization to include (system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems). • NIST SP 800-171 3.12.4		L4-1 Creates, maintains, and leverages a security roadmap for improvement. • CSF: ID.RM-1, RS.IM-1, RS.IM-2, RC.IM-1, RC.IM-2	
				L4-2 The organization applies cybersecurity analysis to all acquisition and merger activities.	
C2 Manage the system security plan		L2-1 Periodically update system security plans as security requirements change. • NIST SP 800-171 3.12.4			
		L2-2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. • NIST SP 800-171 3.12.2			
C3 Define controls objectives		L2-1 Document control objectives based on the system security plan defined security requirements. • RMM CTRL:SG1.SP1			
C4 Define controls	L1-1 Define controls, at least in an ad hoc manner. • RMM CTRL:SG2.SP1	L2-1 Ensure the selected controls are documented and satisfy control objectives. • RMM CTRL:SG2.SP1			
C5 Manage controls		L2-1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. • NIST SP 800-171 3.12.1	L3-1 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. • NIST SP 800-171 3.12.3	L4-1 Conduct penetration testing at least annually, leveraging automated scanning tools and ad hoc tests using human experts. • NIST SP 800-171B:3.12.1e	L5-1 The organization creates a testbed for elements not typically tested in production. • CIS7.1: 20.5

DOMAIN: SECURITY ASSESSMENT (SAS)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C5 Manage controls *(continued)*				L4-2 Has the ability to perform red teaming against defensive capabilities. • DIB	
				L4-3 Employs an independent organization to perform advanced adversarial assessment, at least annually. • DIB	
C6 Perform code reviews to identify weaknesses in in-house-developed software.			L3-1 Employs human performed code reviews to identify areas of concern that require additional improvements. • NIST SP 800-171B: 3.11.6e partial assessment	L4-1 Employs code reviews, and uses static and dynamic analysis methods, on included open source software as a part of an application vetting process prior to being included in the organization's approved software list. • NIST SP 800-171B: 3.11.6e • NIST SP 800-171B: 3.11.7e	

DOMAIN: SECURITY ASSESSMENT (SAS)

MATURITY LEVEL CAPABILITY	PROCESSES				
	Maturity Level 1 (ML1)	Maturity Level 2 (ML2)	Maturity Level 3 (ML3)	Maturity Level 4 (ML4)	Maturity Level 5 (ML5)
Improve Security Assessment activities		ML2-1 Establish a policy for Security Assessment.	ML3-1 Review Security Assessment activities for conformance.	ML4-1 Inform high-level management.	ML5-1 Standardize documentation for Security Assessment.
		ML2-2 Establish practices to implement Security Assessment.	ML3-2 Provide resources for Security Assessment.	ML4-2 Review Security Assessment activities for effectiveness.	ML5-2 Share Security Assessment improvements across the organization.
		ML2-3 Establish a plan for Security Assessment.			

DOMAIN: SITUATIONAL AWARENESS (SA)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C1 Establish threat monitoring requirements		L2-1 The organization has established threat monitoring procedures. • RMM MON:SG2.SP2		L4-1 Implements and continuously improves a process for monitoring, reporting, and alerting that increases effectiveness in threat hunting and monitoring operations. • NIST SP 800-171B: 3.11.1e, 3.11.3e	
				L4-2 Threat monitoring on the specific organization is actively performed, including the use of open source and social media intelligence, to perform analysis, identify threats, and develop trend. • CSF: RS.AN-3	
C2 Implement threat monitoring based on defined requirements	L1-1 The organization receives cyber threat intelligence from information sharing forums and sources, at least in an ad hoc manner. • NIST SP 800-171 3.14.3	L2-1 The organization receives and manages cyber threat intelligence based on established threat monitoring procedures. • NIST SP 800-171 3.14.3		L4-1 The organization maintains a threat intelligence capability that informs the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, and response and recovery activities. • NIST SP 800-171B 3.11.1e	L5-1 The organization employs advanced automation and analytics capabilities to predict and identify risks to organizations, systems, or system components. • NIST SP 800-171B 3.11.3
				L4-2 The organization maintains a cyber threat hunting capability to search for indicators of compromise in organizational systems and detect, track, and disrupt threats that evade existing controls. • NIST SP 800-171B 3.11.2e • CSF: DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM.7,DE.CM-8	L5-2 The organization maintains a dedicated, full-time cyber hunting capability. • DIB

DOMAIN: SITUATIONAL AWARENESS (SA)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C2 Implement threat monitoring based on defined requirements *(continued)*				L4-3 Maintains a centralized intelligence database for defensive cyber operations, threat hunting, and to provide indicator sharing for automated tools and techniques. • DIB Input: Primes	
C3 Establish the requirements for communicating threat information			L3-1 The organization has established the requirements for communicating threat information. • RMM COMM:SG1.SP2	L4-1 The organization designs network and system security capabilities to integrate and share indicators of compromise in real-time to other devices or appliances on the network. • NIST SP 800-171B: 3.11.1e	
			L3-2 The organization has identified stakeholders to whom threat information must be communicated. • RMM COMM:SG1.SP1		
C4 Communicate threat information to stakeholders	L1-1 Threat information is communicated to internal and external stakeholders, at least in an ad hoc manner. • CSF: RS.CO-5		L3-1 The organization communicates threat information to identified stakeholders. • CSF: RS.CO-5	L4-1 The organization automates ingestion and initial analysis of intel feed, and shares initial indicators within 24 hours. • DIB	L5-1 The organization automates the response to intel analysis and sharing of indicators. • DIB

DOMAIN: SITUATIONAL AWARENESS (SA)

MATURITY LEVEL CAPABILITY	PROCESSES				
	Maturity Level 1 (ML1)	Maturity Level 2 (ML2)	Maturity Level 3 (ML3)	Maturity Level 4 (ML4)	Maturity Level 5 (ML5)
Improve Situational Awareness activities		ML2-1 Establish a policy for Situational Awareness.	ML3-1 Review Situational Awareness activities for conformance.	ML4-1 Inform high-level management.	ML5-1 Standardize documentation for Situational Awareness.
		ML2-2 Establish practices to implement Situational Awareness.	ML3-2 Provide resources for Situational Awareness.	ML4-2 Review Situational Awareness activities for effectiveness.	ML5-2 Share Situational Awareness improvements across the organization.
		ML2-3 Establish a plan for Situational Awareness.			

DOMAIN: SYSTEM AND COMMUNICATIONS PROTECTION (SCP)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C1 Define security requirements for systems and communications		L2-1 The organization has a process to establish security requirements for monitoring, controlling, and protecting system boundaries. • NIST SP 800-171 3.13.1	L3-1 The organization separates user functionality from system management functionality. • NIST SP 800-171 3.13.3	L4-1 The organization establishes architectural design guidelines that require physical and logical isolation techniques within organizational systems. • NIST SP 800-171B 3.13.4e	L5-1 The organization disrupts the attack surface of organizational systems through unpredictability, moving target defense, or non-persistence. • NIST SP 800-171B 3.13.2e
		L2-2 The organization has a process to require that publicly accessible systems are physically or logically separated from internal networks. • NIST SP 800-171 3.13.5	L3-2 The organization prevents unauthorized and unintended information transfer via shared system resources. • NIST SP 800-171 3.13.4	L4-2 Administration of high value critical network infrastructure components and servers are physically separated from production networks (e.g., through out-of-band networks). • enhancement of NIST SP 800-171 3.13.2	L5-2 The organization employs technical and procedural means to confuse and mislead adversaries. • NIST SP 800-171B 3.13.3e
		L2-3 The organization establishes and manages cryptography keys for cryptography implemented in organizational systems. • NIST SP 800-171 3.13.10	L3-3 The organization denies network communications by default and allows network communication by exception. • NIST SP 800-171 3.13.6	L4-3 The organization establishes architectural design guidelines that require diverse system components within organizational systems to mitigate malicious code propagation. • NIST SP 800-171B 3.13.1e	L5-3 The organization establishes architectural design guidelines that employ zero trust concepts. • DIB
		L2-4 The organization establishes FIPS-validated cryptography when protecting the confidentiality of organizational information. • NIST SP 800-171 3.13.11	L3-4 The organization prevents split tunneling. • NIST SP 800-171 3.13.7	L4-4 The organization periodically assesses and improves secure cryptographic schemes implemented within the organization [enhancement of • NIST SP 800-171 3.13.11	L5-4 Employ advanced, automated infrastructure implementation and configuration management techniques (e.g., software defined infrastructure). • Enhancement to NIST SP 800-171 3.13.2
		L2-5 The organization establishes architectural design guidelines that promote effective information security within organizational systems. • NIST SP 800-171 3.13.2	L3-5 The organization implements cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. • NIST SP 800-171 3.13.8	L4-5 All outgoing network traffic including email (including personal emails) are analyzed for the presence of CUI data	L5-5 The organization monitors outbound traffic to detect any unauthorized use of encryption. • CIS 7.1: 13.5

DOMAIN: SYSTEM AND COMMUNICATIONS PROTECTION (SCP)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C1 Define security requirements for systems and communications *(continued)*		L2-6 The organization establishes software development technique guidelines that promote effective information security within organizational systems. • NIST SP 800-171 3.13.2	L3-6 The organization protects the authenticity of communications sessions. • NIST SP 800-171 3.13.15		
		L2-7 The organization establishes system engineering guidelines that promote effective information security within organizational systems. • NIST SP 800-171 3.13.2	L3-7 The organization establishes requirements to protect CUI at rest. • NIST SP 800-171 3.13.16		
		L2-8 The organization prohibits remote activation of collaborative computing devices and provides indication of devices in use to users present at the device. • NIST SP 800-171 3.13.12	L3-8 The organization manages and updates the security requirements for external system boundaries at a frequency defined by the organization. • NIST SP 800-171 3.13.1		
		L2-9 The organization uses encrypted sessions for the management of network devices. • CIS 7.1: 11.5	L3-9 The organization manages and updates the architectural, software development, and systems engineering principles at a frequency defined by the organization. • NIST SP 800-171 3.13.2		
			L3-10 The organization terminates network connections at the end of the sessions or after a defined period of inactivity. • NIST SP 800-171 3.13.9		
			L3-11 The organization establishes requirements to control and monitor the use of mobile code. • NIST SP 800-171 3.13.13		

DOMAIN: SYSTEM AND COMMUNICATIONS PROTECTION (SCP)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C1 Define security requirements for systems and communications (continued)			L3-12 The organization establishes requirements to control and monitor the use of Internet Protocol VoIP technologies. • NISP SP 800-171 3.13.14		
C2 Control communications at system boundaries	L1-1 The organization monitors, controls, and protects communications at system boundaries, at least in an ad hoc manner. • NIST SP 800-171 3.13.1	L2-1 The organization monitors, controls, and protects communications at system boundaries based on established requirements. • NIST 800-171 3.13.1	L3-1 The organization implements Domain Name System (DNS) filtering services. • DIB 5 • CIS 7.7	L4-1 The organization uses public and private threat intelligence to proactively block DNS requests from reaching malicious domains. • DIB 5	L5-1 The organization employs custom or otherwise not widely deployed boundary protection systems. • DIB
	L1-2 Publicly accessible systems are physically or logically separated from internal networks, at least in an ad hoc manner. • NIST SP 800-171 3.13.5			L4-2 The organization implements techniques to enforce URL filtering of websites that are not approved by the organization. • DIB 2 • CIS 7.4	L5-2 Implements granular network control (e.g., microsegmentation) to enforce access policies. • DIB
				L4-3 The organization utilizes a URL categorization service and ensures the categorization is kept up-to-date. • DIB 2 • CIS 7.5	
				L4-4 Employs mechanisms to sandbox and analyze executable code and scripts traversing network boundaries. • DIB	
				L4-5 The organization employs mobile device security capabilities to enforce additional access controls for all CUI data. • DIB	

DOMAIN: SYSTEM AND COMMUNICATIONS PROTECTION (SCP)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C2 Control communications at system boundaries *(continued)*				L4-6 The organization employs company-controlled protection mechanisms (e.g., encryption) for CUI data when sharing with subcontractors. • DIB	
				L4-7 Implements network segmentation to limit scope of potential malicious activity. • DIB	
C3 Ensure each system baseline is trusted and unmodified					L5-1 The organization employs hardware-rooted integrity verification of system software, firmware and hardware; extends to provide secure boot, boot attestation, and measured boot. • DIB

DOMAIN: SYSTEM AND COMMUNICATIONS PROTECTION (SCP)

MATURITY LEVEL CAPABILITY	PROCESSES				
	Maturity Level 1 (ML1)	Maturity Level 2 (ML2)	Maturity Level 3 (ML3)	Maturity Level 4 (ML4)	Maturity Level 5 (ML5)
Improve System and Communications Protection activities		ML2-1 Establish a policy for System and Communications Protection.	ML3-1 Review System and Communications Protection activities for conformance.	ML4-1 Inform high-level management.	ML5-1 Standardize documentation for System and Communications Protection.
		ML2-2 Establish practices to implement System and Communications Protection.	ML3-2 Provide resources for System and Communications Protection.	ML4-2 Review System and Communications Protection activities for effectiveness.	ML5-2 Share System and Communications Protection improvements across the organization.
		ML2-3 Establish a plan for System and Communications Protection.			

DOMAIN: SYSTEM AND INFORMATIONAL INTEGRITY (SII)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C1 Information system flaws are identified and corrected	L1-1 Information system flaws are identified and corrected, at least in an ad hoc manner. • NIST SP 800-171 3.14.1	L2-1 A process exists to identify and correct information system flaws. • NIST SP 800-171 3.14.1			
		L2-2 The organization utilizes automated patch management tools. • CIS 7.1: 3.4			
C2 Sources of vulnerability Information are identified and monitored		L2-1 Monitor system security alerts and advisories and take action in response. • NIST SP 800-171 3.14.3			
C3 Malicious content is being identified	L1-1 Malicious code protection (e.g., anti-virus) is installed on all applicable machines. • NIST SP 800-171 3.14.2				
	L1-2 Malicious code protection (e.g., anti-virus) is updated when new releases are available. • NIST SP 800-171 3.14.4				
	L1-3 Scanning of files downloaded from external sources occurs in real-time. • NIST SP 800-171 3.14.5				
C4 Network and system monitoring is performed		L2-1 Operational environments are monitored for anomalous behavior that may indicate a cybersecurity event. • NIST SP 800-171 3.14.6			L5-1 The organization only allows access to authorized cloud storage or email providers. • CIS 7.1: 13.4
		L2-2 Organizational systems are monitored for unauthorized use. • NIST SP 800-171 3.14.7			

DOMAIN: SYSTEM AND INFORMATIONAL INTEGRITY (SII)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C5 Implement advanced email protections				L4-1 Implement DNS or asymmetric cryptography email protections. • DIB 3 • DIB Input: Primes	L5-1 Implement email authenticity and integrity technologies. • DIB 3 • DIB Input: Primes
				L4-2 Email sandboxing is used to block potentially malicious email attachments all emails. • CIS 7.1: 7.10	

DOMAIN: SYSTEM AND INFORMATIONAL INTEGRITY (SII)

MATURITY LEVEL CAPABILITY	PROCESSES				
	Maturity Level 1 (ML1)	Maturity Level 2 (ML2)	Maturity Level 3 (ML3)	Maturity Level 4 (ML4)	Maturity Level 5 (ML5)
Improve System and Information Integrity activities		ML2-1 Establish a policy for System and Information Integrity.	ML3-1 Review System and Information Integrity activities for conformance.	ML4-1 Inform high-level management.	ML5-1 Standardize documentation for System and Information Integrity.
		ML2-2 Establish practices to implement System and Information Integrity.	ML3-2 Provide resources for System and Information Integrity.	ML4-2 Review System and Information Integrity activities for effectiveness.	ML5-2 Share System and Information Integrity improvements across the organization.
		ML2-3 Establish a plan for System and Information Integrity.			