STIG & CMMC Control Matrix

for

Windows Server 2016

October 2021

SteelCloud
Get Compliant. Stay Compliant.

About this Document

This is one of a series of documents that have been produced by SteelCloud to assist in the CMMC compliance effort. This document cross references the different compliance control sets. It is split into three sections - the first section references the CMMC controls in relation to the STIG V-IDs, while the second section reverses this logic to show CMMC controls first. The third section is a high level CMMC matrix.

About SteelCloud

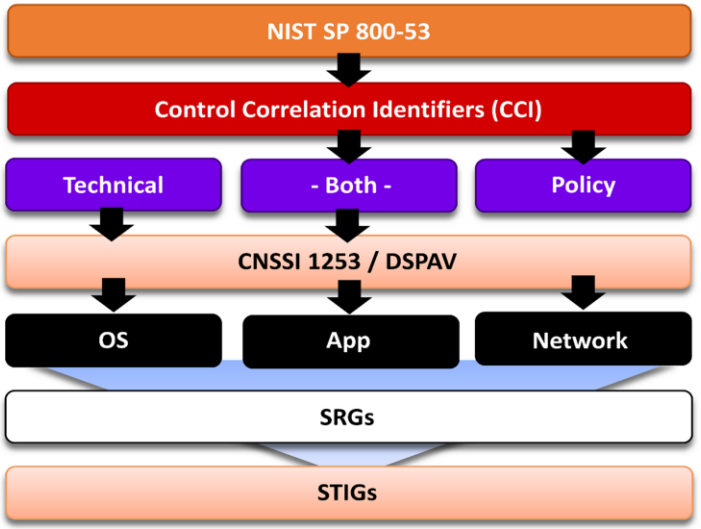
SteelCloud has spent the last decade developing patented technology to automate government policy compliance, configuration control, and cloud security. Our ConfigOS software solution was designed to reduce initial hardening time by 90% and ongoing STIG compliance effort by more than 70%. Our technology will have a significant positive impact on organizations that desire to achieve CMMC Level 2, or greater, compliance. For additional information visit www.steelcloud.com or contact us at info@steelcloud.com.

Links

CMMC Documentation – *acq.osd*
Window OS STIGs – *public.cyber.mil*
Unpacking CMMC – *steelcloud.com*
"STIG for Dummies" eBook – *steelcloud.com*

STIG, NIST 800-171, and CMMC controls, are derived from NIST 800-53 controls. Therefore, there is an interrelationship between these control sets. STIG controls identify the lower level "proof" that compliance has been met for the higher level NIST 800-171 and CMMC controls.

How are STIGs Developed



Source: DISA

SteelCloud
AUTOMATING STIG & CIS COMPLIANCE

SteelCloud

I. STIG to CMMC Matrix

WinServer 2016

STIG V-ID	Rule Title	800-53 Rev. 4	800-171	CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5
224819	Users with Administrative privileges must have separate accounts for administrative duties and normal operational tasks.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
224820	Passwords for the built-in Administrator account must be changed at least every 60 days.	IA-5(1) (d)	3.5.7 3.5.8 3.5.9 3.5.10		IA.2.078 IA.2.079 IA.2.080 IA.2.081			
224821	Administrative accounts must not be used with applications that access the Internet, such as web browsers, or with potential Internet sources, such as email.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
224822	Members of the Backup Operators group must have separate accounts for backup duties and normal operational tasks.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
224823	Manually managed application account passwords must be at least 15 characters in length.	IA-5(1) (a)	3.5.7 3.5.8 3.5.9 3.5.10		IA.2.078 IA.2.079 IA.2.080 IA.2.081			
224824	Manually managed application account passwords must be changed at least annually or when a system administrator with knowledge of the password leaves the organization.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
224825	Shared user accounts must not be permitted on the system.	IA-2	3.5.1 3.5.2	IA 1.076 IA 1.077				
224826	Windows Server 2016 must employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs.	CM-7(5) b	3.4.8			CM.3.069	CM.4.073	
224827	Windows Server 2016 domain-joined systems must have a Trusted Platform Module (TPM) enabled and ready for use.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
224828	Systems must be maintained at a supported servicing level.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
224829	The Windows Server 2016 system must use an anti-virus program.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
224830	Servers must have a host-based intrusion detection or prevention system.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
224831	Local volumes must use a format that supports NTFS attributes.	AC-3	3.1.1 3.1.2	AC.1.001 AC 1.002				
224832	Permissions for the system drive root directory (usually C:\) must conform to minimum requirements.	AC-3(4)	3.1.1 3.1.2	AC.1.001 AC 1.002				

Information in this document is provided for informational purposes only

STIG V-ID	Rule Title	800-53 Rev. 4	800-171	CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5
224833	Permissions for program file directories must conform to minimum requirements.	AC-3(4)	3.1.1 3.1.2	AC.1.001 AC 1.002				
224834	Permissions for the Windows installation directory must conform to minimum requirements.	AC-3(4)	3.1.1 3.1.2	AC.1.001 AC 1.002				
224835	Default permissions for the HKEY_LOCAL_MACHINE registry hive must be maintained.	AC-6(10)	3.1.7			AC.3.018		
224836	Non-administrative accounts or groups must only have print permissions on printer shares.	AC-3	3.1.1 3.1.2	AC.1.001 AC.1.002				
224837	Outdated or unused accounts must be removed from the system or disabled.	IA-2; IA-4 e	3.5.1 3.5.2 3.5.5 3.5.6	IA.1.076 IA.1.077		IA.3.085 IA.3.086		
224838	Windows Server 2016 accounts must require passwords.	IA-2	3.5.1 3.5.2	IA.1.076 IA.1.077				
224839	Passwords must be configured to expire.	IA-5(1) (d)	3.5.7 3.5.8 3.5.9 3.5.10		IA.2.078 IA.2.079 IA.2.080 IA.2.081			
224840	System files must be monitored for unauthorized changes.	CM-3(5)						
224841	Non-system-created file shares on a system must limit access to groups that require it.	SC-4	3.13.4			SC.3.182		
224842	Software certificate installation files must be removed from Windows Server 2016.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
224843	Systems requiring data at rest protections must employ cryptographic mechanisms to prevent unauthorized disclosure and modification of the information at rest.	SC-28; SC-28(1)	3.13.16			SC.3.191		
224844	Protection methods such as TLS, encrypted VPNs, or IPsec must be implemented if the data owner has a strict requirement for ensuring data integrity and confidentiality is maintained at every step of the data transfer and handling process.	SC-8(2)				SI.3.219		
224845	The roles and features required by the system must be documented.	CM-7 a	3.4.6		CM.2.062			
224846	A host-based firewall must be installed and enabled on the system.	CM-6 b; CA-3(5)	3.4.1 3.4.2		CM.2.061 CM.2.064			

STIG V-ID	Rule Title	800-53 Rev. 4	800-171	CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5
224847	Windows Server 2016 must employ automated mechanisms to determine the state of system components with regard to flaw remediation using the following frequency: continuously, where Host Based Security System (HBSS) is used; 30 days, for any additional internal network scans not covered by HBSS; and annually, for external scans by Computer Network Defense Service Provider (CNDSP).	SI-2(2)	3.14.1	SI.1.210				
224848	Windows Server 2016 must automatically remove or disable temporary user accounts after 72 hours.	AC-2(2)	3.1.1 3.1.2	AC.1.001 AC.1.002				
224849	Windows Server 2016 must automatically remove or disable emergency accounts after the crisis is resolved or within 72 hours.	AC-2(2)	3.1.1 3.1.2	AC.1.001 AC.1.002				
224850	The Fax Server role must not be installed.	CM-7 a	3.4.6		CM.2.062			
224851	The Microsoft FTP service must not be installed unless required.	CM-7 b	3.4.6		CM.2.062			
224852	The Peer Name Resolution Protocol must not be installed.	CM-7 a	3.4.6		CM.2.062			
224853	Simple TCP/IP Services must not be installed.	CM-7 a	3.4.6		CM.2.062			
224854	The Telnet Client must not be installed.	CM-7 b	3.4.6		CM.2.062			
224855	The TFTP Client must not be installed.	CM-7 a	3.4.6		CM.2.062			
224856	The Server Message Block (SMB) v1 protocol must be uninstalled.	CM-7 a	3.4.6		CM.2.062			
224857	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	CM-7 a	3.4.6		CM.2.062			
224858	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	CM-7 a	3.4.6		CM.2.062			
224859	Windows PowerShell 2.0 must not be installed.	CM-7 a	3.4.6		CM.2.062			
224860	FTP servers must be configured to prevent anonymous logons.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
224861	FTP servers must be configured to prevent access to the system drive.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
224862	The time service must synchronize with an appropriate DoD time source.	AU-8(1) a	3.3.7		AU.2.043			
224863	Orphaned security identifiers (SIDs) must be removed from user rights on Windows 2016.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
224864	Secure Boot must be enabled on Windows Server 2016 systems.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			

STIG V-ID	Rule Title	800-53 Rev. 4	800-171	CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5
224865	Windows 2016 systems must have Unified Extensible Firmware Interface (UEFI) firmware and be configured to run in UEFI mode, not Legacy BIOS.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
224866	Windows 2016 account lockout duration must be configured to 15 minutes or greater.	AC-7 b	3.1.8		AC.2.009			
224867	Windows Server 2016 must have the number of allowed bad logon attempts configured to three or less.	AC-7 a	3.1.8		AC.2.009			
224868	Windows Server 2016 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater.	AC-7 a; AC-7 b	3.1.8		AC.2.009			
224869	Windows Server 2016 password history must be configured to 24 passwords remembered.	IA-5(1) (e)	3.5.7 3.5.8 3.5.9 3.5.10		IA.2.078 IA.2.079 IA.2.080 IA.2.081			
224870	Windows Server 2016 maximum password age must be configured to 60 days or less.	IA-5(1) (d)	3.5.7 3.5.8 3.5.9 3.5.10		IA.2.078 IA.2.079 IA.2.080 IA.2.081			
224871	Windows Server 2016 minimum password age must be configured to at least one day.	IA-5(1) (d)	3.5.7 3.5.8 3.5.9 3.5.10		IA.2.078 IA.2.079 IA.2.080 IA.2.081			
224872	Windows Server 2016 minimum password length must be configured to 14 characters.	IA-5(1) (a)	3.5.7 3.5.8 3.5.9 3.5.10		IA.2.078 IA.2.079 IA.2.080 IA.2.081			
224873	Windows Server 2016 must have the built-in Windows password complexity policy enabled.	IA-5(1) (a)	3.5.7 3.5.8 3.5.9 3.5.10		IA.2.078 IA.2.079 IA.2.080 IA.2.081			
224874	Windows Server 2016 reversible password encryption must be disabled.	IA-5(1) (c)	3.5.7 3.5.8 3.5.9 3.5.10		IA.2.078 IA.2.079 IA.2.080 IA.2.081			
224875	Audit records must be backed up to a different system or media than the system being audited.	AU-4(1)						

STIG V-ID	Rule Title	800-53 Rev. 4	800-171	CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5
224876	Windows Server 2016 must, at a minimum, off-load audit records of interconnected systems in real time and off-load standalone systems weekly.	AU-4(1)						
224877	Permissions for the Application event log must prevent access by non-privileged accounts.	AU-9	3.3.8			AU.3.049		
224878	Permissions for the Security event log must prevent access by non-privileged accounts.	AU-9	3.3.8			AU.3.049		
224879	Permissions for the System event log must prevent access by non-privileged accounts.	AU-9	3.3.8			AU.3.049		
224880	Event Viewer must be protected from unauthorized modification and deletion.	AU-9	3.3.8			AU.3.049		
224881	Windows Server 2016 must be configured to audit Account Logon - Credential Validation successes.	AU-12 c	3.3.1 3.3.2		AU.2.041 AU.2.042			AU.5.055 IR.5.106
224882	Windows Server 2016 must be configured to audit Account Logon - Credential Validation failures.	AU-12 c	3.3.1 3.3.2		AU.2.041 AU.2.042			AU.5.055 IR.5.106
224883	Windows Server 2016 must be configured to audit Account Management - Other Account Management Events successes.	AC-2(4); AU-12 c	3.1.1 3.1.2		AU.2.041 AU.2.042			AU.5.055 IR.5.106
224884	Windows Server 2016 must be configured to audit Account Management - Security Group Management successes.	AC-2(4); AU-12 c	3.1.1 3.1.2		AU.2.041 AU.2.042			AU.5.055 IR.5.106
224885	Windows Server 2016 must be configured to audit Account Management - User Account Management successes.	AC-2(4); AU-12 c	3.1.1 3.1.2		AU.2.041 AU.2.042			AU.5.055 IR.5.106
224886	Windows Server 2016 must be configured to audit Account Management - User Account Management failures.	AC-2(4); AU-12 c	3.1.1 3.1.2		AU.2.041 AU.2.042			AU.5.055 IR.5.106
224887	Windows Server 2016 must be configured to audit Detailed Tracking - Plug and Play Events successes.	AU-12 c	3.3.1 3.3.2		AU.2.041 AU.2.042			AU.5.055 IR.5.106
224888	Windows Server 2016 must be configured to audit Detailed Tracking - Process Creation successes.	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7		AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106
224889	Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout successes.	AC-2(4); AU-12 c	3.1.1 3.1.2		AU.2.041 AU.2.042			AU.5.055 IR.5.106
224890	Windows Server 2016 must be configured to audit Logon/Logoff - Account Lockout failures.	AC-2(4); AU-12 c	3.1.1 3.1.2		AU.2.041 AU.2.042			AU.5.055 IR.5.106
224891	Windows Server 2016 must be configured to audit Logon/Logoff - Group Membership successes.	AU-12 c	3.3.1 3.3.2		AU.2.041 AU.2.042			AU.5.055 IR.5.106

STIG V-ID	Rule Title	800-53 Rev. 4	800-171	CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5
224892	Windows Server 2016 must be configured to audit Logon/Logoff - Logoff successes.	AC-17(1); AU-12 c	3.1.12 3.3.1 3.3.2		AC.2.013 AU.2.041 AU.2.042			AU.5.055 IR.5.106
224893	Windows Server 2016 must be configured to audit Logon/Logoff - Logon successes.	AC-17(1); AU-12 c	3.1.12 3.3.1 3.3.2		AC.2.013 AU.2.041 AU.2.042			AU.5.055 IR.5.106
224894	Windows Server 2016 must be configured to audit Logon/Logoff - Logon failures.	AC-17(1); AU-12 c	3.1.12 3.3.1 3.3.2		AC.2.013 AU.2.041 AU.2.042			AU.5.055 IR.5.106
224895	Windows Server 2016 must be configured to audit Logon/Logoff - Special Logon successes.	AU-12 c	3.3.1 3.3.2		AU.2.041 AU.2.042			AU.5.055 IR.5.106
224896	Windows 2016 must be configured to audit Object Access - Other Object Access Events successes.	AU-12 c	3.3.1 3.3.2		AU.2.041 AU.2.042			AU.5.055 IR.5.106
224897	Windows 2016 must be configured to audit Object Access - Other Object Access Events failures.	AU-12 c	3.3.1 3.3.2		AU.2.041 AU.2.042			AU.5.055 IR.5.106
224898	Windows Server 2016 must be configured to audit Object Access - Removable Storage successes.	AU-12 c	3.3.1 3.3.2		AU.2.041 AU.2.042			AU.5.055 IR.5.106
224899	Windows Server 2016 must be configured to audit Object Access - Removable Storage failures.	AU-12 c	3.3.1 3.3.2		AU.2.041 AU.2.042			AU.5.055 IR.5.106
224900	Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change successes.	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7		AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106
224901	Windows Server 2016 must be configured to audit Policy Change - Audit Policy Change failures.	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7		AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106
224902	Windows Server 2016 must be configured to audit Policy Change - Authentication Policy Change successes.	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7		AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106
224903	Windows Server 2016 must be configured to audit Policy Change - Authorization Policy Change successes.	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7		AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106
224904	Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use successes.	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7		AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106

STIG V-ID	Rule Title	800-53 Rev. 4	800-171	CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5
224905	Windows Server 2016 must be configured to audit Privilege Use - Sensitive Privilege Use failures.	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7		AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106
224906	Windows Server 2016 must be configured to audit System - IPsec Driver successes.	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7		AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106
224907	Windows Server 2016 must be configured to audit System - IPsec Driver failures.	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7		AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106
224908	Windows Server 2016 must be configured to audit System - Other System Events successes.	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7		AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106
224909	Windows Server 2016 must be configured to audit System - Other System Events failures.	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7		AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106
224910	Windows Server 2016 must be configured to audit System - Security State Change successes.	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7		AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106
224911	Windows Server 2016 must be configured to audit System - Security System Extension successes.	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7		AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106
224912	Windows Server 2016 must be configured to audit System - System Integrity successes.	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7		AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106
224913	Windows Server 2016 must be configured to audit System - System Integrity failures.	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7		AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106
224914	The display of slide shows on the lock screen must be disabled.	CM-7 a	3.4.6		CM.2.062			
224915	WDigest Authentication must be disabled on Windows Server 2016.	CM-7 a	3.4.6		CM.2.062			
224916	Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
224917	Source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			

STIG V-ID	Rule Title	800-53 Rev. 4	800-171	CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5
224918	Windows Server 2016 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
224919	Windows Server 2016 must be configured to ignore NetBIOS name release requests except from WINS servers.	SC-5						
224920	Hardened UNC paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
224921	Insecure logons to an SMB server must be disabled.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
224922	Command line data must be included in process creation events.	AU-3(1)	3.3.1 3.3.2		AU.2.041 AU.2.042			
224923	Windows Server 2016 virtualization-based security must be enabled with the platform security level configured to Secure Boot or Secure Boot with DMA Protection.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
224924	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
224925	Group Policy objects must be reprocessed even if they have not changed.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
224926	Downloading print driver packages over HTTP must be prevented.	CM-7 a	3.4.6		CM.2.062			
224927	Printing over HTTP must be prevented.	CM-7 a	3.4.6		CM.2.062			
224928	The network selection user interface (UI) must not be displayed on the logon screen.	CM-7 a	3.4.6		CM.2.062			
224929	Users must be prompted to authenticate when the system wakes from sleep (on battery).	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
224930	Users must be prompted to authenticate when the system wakes from sleep (plugged in).	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
224931	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	CM-7 a	3.4.6		CM.2.062			
224932	AutoPlay must be turned off for non-volume devices.	CM-7(2)	3.4.7			CM.3.068		
224933	The default AutoRun behavior must be configured to prevent AutoRun commands.	CM-7(2)	3.4.7			CM.3.068		
224934	AutoPlay must be disabled for all drives.	CM-7(2)	3.4.7			CM.3.068		
224935	Administrator accounts must not be enumerated during elevation.	SC-3						

STIG V-ID	Rule Title	800-53 Rev. 4	800-171	CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5
224936	Windows Telemetry must be configured to Security or Basic.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
224937	The Application event log size must be configured to 32768 KB or greater.	AU-4						
224938	The Security event log size must be configured to 196608 KB or greater.	AU-4						
224939	The System event log size must be configured to 32768 KB or greater.	AU-4						
224940	Windows Server 2016 Windows SmartScreen must be enabled.	CM-7 a	3.4.6		CM.2.062			
224941	Explorer Data Execution Prevention must be enabled.	SI-16						
224942	Turning off File Explorer heap termination on corruption must be disabled.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
224943	File Explorer shell protocol must run in protected mode.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
224944	Passwords must not be saved in the Remote Desktop Client.	IA-11						
224945	Local drives must be prevented from sharing with Remote Desktop Session Hosts.	SC-4	3.13.4			SC.3.182		
224946	Remote Desktop Services must always prompt a client for passwords upon connection.	IA-11						
224947	The Remote Desktop Session Host must require secure Remote Procedure Call (RPC) communications.	AC-17(2)	3.1.13			AC.3.014		
224948	Remote Desktop Services must be configured with the client connection encryption set to High Level.	AC-17(2)	3.1.13			AC.3.014		
224949	Attachments must be prevented from being downloaded from RSS feeds.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
224951	Basic authentication for RSS feeds over HTTP must not be used.	CM-7 a	3.4.6		CM.2.062			
224952	Indexing of encrypted files must be turned off.	CM-7 a	3.4.6		CM.2.062			
224953	Users must be prevented from changing installation options.	CM-11(2)	3.4.9		CM.2.063			
224954	The Windows Installer Always install with elevated privileges option must be disabled.	CM-11(2)	3.4.9		CM.2.063			
224955	Users must be notified if a web-based program attempts to install software.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
224956	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			

STIG V-ID	Rule Title	800-53 Rev. 4	800-171	CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5
224957	PowerShell script block logging must be enabled.	AU-3(1)	3.3.1 3.3.2		AU.2.041 AU.2.042			
224958	The Windows Remote Management (WinRM) client must not use Basic authentication.	MA-4 c	3.7.5		MA.2.113			
224959	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	MA-4(6)	3.7.5		MA.2.113			
224960	The Windows Remote Management (WinRM) client must not use Digest authentication.	MA-4 c	3.7.5		MA.2.113			
224961	The Windows Remote Management (WinRM) service must not use Basic authentication.	MA-4 c	3.7.5		MA.2.113			
224962	The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	MA-4(6)	3.7.5		MA.2.113			
224963	The Windows Remote Management (WinRM) service must not store RunAs credentials.	IA-11						
224964	Only administrators responsible for the domain controller must have Administrator rights on the system.	AC-6(10)	3.1.7			AC.3.018		
224965	Kerberos user logon restrictions must be enforced.	IA-2(8); IA-2(9)	3.5.4			IA.3.084		
224966	The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	IA-2(8); IA-2(9)	3.5.4			IA.3.084		
224967	The Kerberos user ticket lifetime must be limited to 10 hours or less.	IA-2(8); IA-2(9)	3.5.4			IA.3.084		
224968	The Kerberos policy user ticket renewal maximum lifetime must be limited to seven days or less.	IA-2(8); IA-2(9)	3.5.4			IA.3.084		
224969	The computer clock synchronization tolerance must be limited to 5 minutes or less.	IA-2(8); IA-2(9)	3.5.4			IA.3.084		
224970	Permissions on the Active Directory data files must only allow System and Administrators access.	AC-6(10)	3.1.7			AC.3.018		
224971	The Active Directory SYSVOL directory must have the proper access control permissions.	AC-6(10)	3.1.7			AC.3.018		
224972	Active Directory Group Policy objects must have proper access control permissions.	AC-6(10)	3.1.7			AC.3.018		
224973	The Active Directory Domain Controllers Organizational Unit (OU) object must have the proper access control permissions.	AC-6(10)	3.1.7			AC.3.018		

STIG V-ID	Rule Title	800-53 Rev. 4	800-171	CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5
224974	Domain-created Active Directory Organizational Unit (OU) objects must have proper access control permissions.	AC-6(10)	3.1.7			AC.3.018		
224975	Data files owned by users must be on a different logical partition from the directory server data files.	SC-4	3.13.4			SC.3.182		
224976	Domain controllers must run on a machine dedicated to that function.	CM-7 a	3.4.6		CM.2.062			
224977	Separate, NSA-approved (Type 1) cryptography must be used to protect the directory data in transit for directory service implementations at a classified confidentiality level when replication data traverses a network cleared to a lower level than the data.	SC-13	3.13.11			SC.3.177		
224978	Directory data (outside the root DSE) of a non-public directory must be configured to prevent anonymous access.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
224979	The directory service must be configured to terminate LDAP-based network connections to the directory server after 5 minutes of inactivity.	SC-10	3.13.9			SC.3.186		
224980	Active Directory Group Policy objects must be configured with proper audit settings.	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7		AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106
224981	The Active Directory Domain object must be configured with proper audit settings.	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7		AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106
224982	The Active Directory Infrastructure object must be configured with proper audit settings.	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7		AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106
224983	The Active Directory Domain Controllers Organizational Unit (OU) object must be configured with proper audit settings.	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7		AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106
224984	The Active Directory AdminSDHolder object must be configured with proper audit settings.	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7		AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106
224985	The Active Directory RID Manager$ object must be configured with proper audit settings.	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7		AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106

STIG V-ID	Rule Title	800-53 Rev. 4	800-171	CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5
224986	Windows Server 2016 must be configured to audit Account Management - Computer Account Management successes.	AC-2(4); AU-12 c	3.1.1 3.1.2		AU.2.041 AU.2.042			AU.5.055 IR.5.106
224987	Windows Server 2016 must be configured to audit DS Access - Directory Service Access successes.	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7		AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106
224988	Windows Server 2016 must be configured to audit DS Access - Directory Service Access failures.	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7		AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106
224989	Windows Server 2016 must be configured to audit DS Access - Directory Service Changes successes.	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7		AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106
224990	Windows Server 2016 must be configured to audit DS Access - Directory Service Changes failures.	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7		AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106
224991	Domain controllers must have a PKI server certificate.	IA-5(2) (a)						
224992	Domain Controller PKI certificates must be issued by the DoD PKI or an approved External Certificate Authority (ECA).	IA-5(2) (a)						
224993	PKI certificates associated with user accounts must be issued by the DoD PKI or an approved External Certificate Authority (ECA).	IA-5(2) (a)						
224994	Active Directory user accounts, including administrators, must be configured to require the use of a Common Access Card (CAC), Personal Identity Verification (PIV)-compliant hardware token, or Alternate Logon Token (ALT) for user authentication.	IA-2(1); IA-2(2); IA-2(3); IA-2(4); IA-2(11)	3.5.3			IA.3.083		
224995	Domain controllers must require LDAP access signing.	SC-8; SC-8 (1)	3.13.8			SC.3.185 SI.3.219		
224996	Domain controllers must be configured to allow reset of machine account passwords.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
224997	The Access this computer from the network user right must only be assigned to the Administrators, Authenticated Users, and Enterprise Domain Controllers groups on domain controllers.	AC-3	3.1.1 3.1.2	AC.1.001 AC 1.002				
224998	The Add workstations to domain user right must only be assigned to the Administrators group.	AC-6(10)	3.1.7			AC.3.018		
224999	The Allow log on through Remote Desktop Services user right must only be assigned to the Administrators group.	AC-3	3.1.1 3.1.2	AC.1.001 AC 1.002				

STIG V-ID	Rule Title	800-53 Rev. 4	800-171	CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5
225000	The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	AC-3	3.1.1 3.1.2	AC.1.001 AC 1.002				
225001	The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	AC-3	3.1.1 3.1.2	AC.1.001 AC 1.002				
225002	The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	AC-3	3.1.1 3.1.2	AC.1.001 AC 1.002				
225003	The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.	AC-3	3.1.1 3.1.2	AC.1.001 AC 1.002				
225004	The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.	AC-17(1)	3.1.12		AC.2.013			
225005	The Enable computer and user accounts to be trusted for delegation user right must only be assigned to the Administrators group on domain controllers.	AC-6(10)	3.1.7			AC.3.018		
225006	The password for the krbtgt account on a domain must be reset at least every 180 days.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
225007	Only administrators responsible for the member server or standalone system must have Administrator rights on the system.	AC-6(10)	3.1.7			AC.3.018		
225008	Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	SC-3						
225009	Local users on domain-joined computers must not be enumerated.	CM-7 a	3.4.6		CM.2.062			
225010	Unauthenticated Remote Procedure Call (RPC) clients must be restricted from connecting to the RPC server.	IA-3(1)	3.5.1 3.5.2	IA 1.076 IA 1.077				
225011	Caching of logon credentials must be limited.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
225012	Windows Server 2016 must be running Credential Guard on domain-joined member servers.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
225013	Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.	AC-6(10)	3.1.7			AC.3.017		
225014	The Access this computer from the network user right must only be assigned to the Administrators and Authenticated Users groups on member servers.	AC-3	3.1.1 3.1.2	AC.1.001 AC 1.002				

STIG V-ID	Rule Title	800-53 Rev. 4	800-171	CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5
225015	The Deny access to this computer from the network user right on member servers must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems, and from unauthenticated access on all systems.	AC-3	3.1.1 3.1.2	AC.1.001 AC 1.002				
225016	The Deny log on as a batch job user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	AC-3	3.1.1 3.1.2	AC.1.001 AC 1.002				
225017	The Deny log on as a service user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	AC-3	3.1.1 3.1.2	AC.1.001 AC 1.002				
225018	The Deny log on locally user right on member servers must be configured to prevent access from highly privileged domain accounts on domain systems and from unauthenticated access on all systems.	AC-3	3.1.1 3.1.2	AC.1.001 AC 1.002				
225019	The Deny log on through Remote Desktop Services user right on member servers must be configured to prevent access from highly privileged domain accounts and all local accounts on domain systems and from unauthenticated access on all systems.	AC-17(1)	3.1.12		AC.2.013			
225020	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts on member servers.	AC-6(10)	3.1.7			AC.3.018		
225021	The DoD Root CA certificates must be installed in the Trusted Root Store.	IA-5(2) (a); SC-23(5)						
225022	The DoD Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	IA-5(2) (a); SC-23(5)						
225023	The US DoD CCEB Interoperability Root CA cross-certificates must be installed in the Untrusted Certificates Store on unclassified systems.	IA-5(2) (a); SC-23(5)						
225024	Windows Server 2016 built-in guest account must be disabled.	IA-8						
225025	Local accounts with blank passwords must be restricted to prevent access from the network.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
225026	Windows Server 2016 built-in administrator account must be renamed.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			

STIG V-ID	Rule Title	800-53 Rev. 4	800-171	CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5
225027	Windows Server 2016 built-in guest account must be renamed.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
225028	Audit policy using subcategories must be enabled.	AU-12 c	3.3.1 3.3.2		AU.2.041 AU.2.042			AU.5.055 IR.5.106
225029	The setting Domain member: Digitally encrypt or sign secure channel data (always) must be configured to Enabled.	SC-8; SC-8(1)	3.13.8			SC.3.185 SI.3.219		
225030	The setting Domain member: Digitally encrypt secure channel data (when possible) must be configured to enabled.	SC-8; SC-8(1)	3.13.8			SC.3.185 SI.3.219		
225031	The setting Domain member: Digitally sign secure channel data (when possible) must be configured to Enabled.	SC-8; SC-8(1)	3.13.8			SC.3.185 SI.3.219		
225032	The computer account password must not be prevented from being reset.	IA-3(1)	3.5.1 3.5.2	IA 1.076 IA 1.077				
225033	The maximum age for machine account passwords must be configured to 30 days or less.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
225034	Windows Server 2016 must be configured to require a strong session key.	SC-8; SC-8(1)	3.13.8			SC.3.185 SI.3.219		
225035	The machine inactivity limit must be set to 15 minutes, locking the system with the screen saver.	AC-11 a	3.1.10		AC.2.010			
225036	The required legal notice must be configured to display before console logon.	AC-8 a; AC-8 b; AC-8 c 1; AC-8 c 2; AC-8 c 3	3.1.9		AC2.005			
225037	The Windows dialog box title for the legal banner must be configured with the appropriate text.	AC-8 a; AC-8 c 1; AC-8 c 2; AC-8 c 3	3.1.9		AC2.005			
225038	The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
225039	The setting Microsoft network client: Digitally sign communications (always) must be configured to Enabled.	SC-8; SC-8(1)	3.13.8			SC.3.185 SI.3.219		
225040	The setting Microsoft network client: Digitally sign communications (if server agrees) must be configured to Enabled.	SC-8; SC-8(1)	3.13.8			SC.3.185 SI.3.219		

STIG V-ID	Rule Title	800-53 Rev. 4	800-171	CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5
225041	Unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers.	IA-5(1) (c)	3.5.7 3.5.8 3.5.9 3.5.10		IA.2.078 IA.2.079 IA.2.080 IA.2.081			
225042	The setting Microsoft network server: Digitally sign communications (always) must be configured to Enabled.	SC-8; SC-8(1)	3.13.8			SC.3.185 SI.3.219		
225043	The setting Microsoft network server: Digitally sign communications (if client agrees) must be configured to Enabled.	SC-8; SC-8(1)	3.13.8			SC.3.185 SI.3.219		
225044	Anonymous SID/Name translation must not be allowed.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
225045	Anonymous enumeration of Security Account Manager (SAM) accounts must not be allowed.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
225046	Anonymous enumeration of shares must not be allowed.	SC-4	3.13.4			SC.3.182		
225047	Windows Server 2016 must be configured to prevent anonymous users from having the same permissions as the Everyone group.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
225048	Anonymous access to Named Pipes and Shares must be restricted.	SC-4	3.13.4			SC.3.182		
225049	Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity instead of authenticating anonymously.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
225050	NTLM must be prevented from falling back to a Null session.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
225051	PKU2U authentication using online identities must be prevented.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
225052	Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.	IA-7						
225053	Windows Server 2016 must be configured to prevent the storage of the LAN Manager hash of passwords.	IA-5(1) (c)	3.5.7 3.5.8 3.5.9 3.5.10		IA.2.078 IA.2.079 IA.2.080 IA.2.081			
225054	The LAN Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
225055	Windows Server 2016 must be configured to at least negotiate signing for LDAP client signing.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
225056	Session security for NTLM SSP-based clients must be configured to require NTLMv2 session security and 128-bit encryption.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			

STIG V-ID	Rule Title	800-53 Rev. 4	800-171	CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5
225057	Session security for NTLM SSP-based servers must be configured to require NTLMv2 session security and 128-bit encryption.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
225058	Users must be required to enter a password to access private keys stored on the computer.	IA-5(2)						
225059	Windows Server 2016 must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	AC-17(2); SC-13	3.1.13 3.13.11			AC.3.014 SC.3.177		
225060	The default permissions of global system objects must be strengthened.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
225061	User Account Control approval mode for the built-in Administrator must be enabled.	IA-11						
225062	UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	SC-3						
225063	User Account Control must, at a minimum, prompt administrators for consent on the secure desktop.	SC-3						
225064	User Account Control must automatically deny standard user requests for elevation.	IA-11						
225065	User Account Control must be configured to detect application installations and prompt for elevation.	SC-3						
225066	User Account Control must only elevate UIAccess applications that are installed in secure locations.	SC-3						
225067	User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	IA-11						
225068	User Account Control must virtualize file and registry write failures to per-user locations.	SC-3						
225069	Zone information must be preserved when saving attachments.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
225070	The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	AC-6(10)	3.1.7			AC.3.018		
225071	The Act as part of the operating system user right must not be assigned to any groups or accounts.	AC-6(10)	3.1.7			AC.3.018		
225072	The Allow log on locally user right must only be assigned to the Administrators group.	AC-3	3.1.1 3.1.2	AC.1.001 AC 1.002				
225073	The Back up files and directories user right must only be assigned to the Administrators group.	AC-6(10)	3.1.7			AC.3.018		
225074	The Create a pagefile user right must only be assigned to the Administrators group.	AC-6(10)	3.1.7			AC.3.018		

STIG V-ID	Rule Title	800-53 Rev. 4	800-171	CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5
225076	The Create global objects user right must only be assigned to Administrators, Service, Local Service, and Network Service.	AC-6(10)	3.1.7			AC.3.018		
225077	The Create permanent shared objects user right must not be assigned to any groups or accounts.	AC-6(10)	3.1.7			AC.3.018		
225078	The Create symbolic links user right must only be assigned to the Administrators group.	AC-6(10)	3.1.7			AC.3.018		
225079	The Debug programs user right must only be assigned to the Administrators group.	AC-6(10)	3.1.7			AC.3.018		
225080	The Force shutdown from a remote system user right must only be assigned to the Administrators group.	AC-6(10)	3.1.7			AC.3.018		
225081	The Generate security audits user right must only be assigned to Local Service and Network Service.	AC-6(10)	3.1.7			AC.3.018		
225082	The Impersonate a client after authentication user right must only be assigned to Administrators, Service, Local Service, and Network Service.	AC-6(10)	3.1.7			AC.3.018		
225083	The Increase scheduling priority user right must only be assigned to the Administrators group.	AC-6(10)	3.1.7			AC.3.018		
225084	The Load and unload device drivers user right must only be assigned to the Administrators group.	AC-6(10)	3.1.7			AC.3.018		
225085	The Lock pages in memory user right must not be assigned to any groups or accounts.	AC-6(10)	3.1.7			AC.3.018		
225086	The Manage auditing and security log user right must only be assigned to the Administrators group.	AU-9; AU-12 b; AU-12(3)	3.3.1 3.3.2 3.3.8		AU.2.041 AU.2.042	AC.3.018 AU.3.049 AU.3.050		AU.5.055 IR.5.106
225087	The Modify firmware environment values user right must only be assigned to the Administrators group.	AC-6(10)	3.1.7			AC.3.018		
225088	The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	AC-6(10)	3.1.7			AC.3.018		
225089	The Profile single process user right must only be assigned to the Administrators group.	AC-6(10)	3.1.7			AC.3.018		
225091	The Create a token object user right must not be assigned to any groups or accounts.	AC-6(10)	3.1.7			AC.3.018		
225092	The Restore files and directories user right must only be assigned to the Administrators group.	AC-6(10)	3.1.7			AC.3.018		
225093	The Take ownership of files or other objects user right must only be assigned to the Administrators group.	AC-6(10)	3.1.7			AC.3.018		

CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5	800-53 Rev. 4	800-171	STIG V-ID
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**224819**
	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5(1) (d)	3.5.7 3.5.8 3.5.9 3.5.10	**224820**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**224821**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**224822**
	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5(1) (a)	3.5.7 3.5.8 3.5.9 3.5.10	**224823**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**224824**
IA 1.076 IA 1.077					IA-2	3.5.1 3.5.2	**224825**
		CM.3.069	CM.4.073		CM-7(5) b	3.4.8	**224826**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**224827**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**224828**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**224829**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**224830**
AC.1.001 AC 1.002					AC-3	3.1.1 3.1.2	**224831**
AC.1.001 AC 1.002					AC-3(4)	3.1.1 3.1.2	**224832**

CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5	800-53 Rev. 4	800-171	STIG V-ID
AC.1.001 AC 1.002					AC-3(4)	3.1.1 3.1.2	**224833**
AC.1.001 AC 1.002					AC-3(4)	3.1.1 3.1.2	**224834**
		AC.3.018			AC-6(10)	3.1.7	**224835**
AC.1.001 AC.1.002					AC-3	3.1.1 3.1.2	**224836**
IA.1.076 IA.1.077		IA.3.085 IA.3.086			IA-2; IA-4 e	3.5.1 3.5.2 3.5.5 3.5.6	**224837**
IA.1.076 IA.1.077					IA-2	3.5.1 3.5.2	**224838**
	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5(1) (d)	3.5.7 3.5.8 3.5.9 3.5.10	**224839**
					CM-3(5)		**224840**
		SC.3.182			SC-4	3.13.4	**224841**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**224842**
		SC.3.191			SC-28; SC-28(1)	3.13.16	**224843**
		SI.3.219			SC-8(2)		**224844**
	CM.2.062				CM-7 a	3.4.6	**224845**
	CM.2.061 CM.2.064				CM-6 b; CA-3(5)	3.4.1 3.4.2	**224846**
SI.1.210					SI-2(2)	3.14.1	**224847**
AC.1.001 AC.1.002					AC-2(2)	3.1.1 3.1.2	**224848**

CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5	800-53 Rev. 4	800-171	STIG V-ID
AC.1.001 AC.1.002					AC-2(2)	3.1.1 3.1.2	**224849**
	CM.2.062				CM-7 a	3.4.6	**224850**
	CM.2.062				CM-7 b	3.4.6	**224851**
	CM.2.062				CM-7 a	3.4.6	**224852**
	CM.2.062				CM-7 a	3.4.6	**224853**
	CM.2.062				CM-7 b	3.4.6	**224854**
	CM.2.062				CM-7 a	3.4.6	**224855**
	CM.2.062				CM-7 a	3.4.6	**224856**
	CM.2.062				CM-7 a	3.4.6	**224857**
	CM.2.062				CM-7 a	3.4.6	**224858**
	CM.2.062				CM-7 a	3.4.6	**224859**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**224860**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**224861**
	AU.2.043				AU-8(1) a	3.3.7	**224862**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**224863**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**224864**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**224865**
	AC.2.009				AC-7 b	3.1.8	**224866**
	AC.2.009				AC-7 a	3.1.8	**224867**
	AC.2.009				AC-7 a; AC-7 b	3.1.8	**224868**
	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5(1) (e)	3.5.7 3.5.8 3.5.9 3.5.10	**224869**

CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5	800-53 Rev. 4	800-171	STIG V-ID
	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5(1) (d)	3.5.7 3.5.8 3.5.9 3.5.10	**224870**
	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5(1) (d)	3.5.7 3.5.8 3.5.9 3.5.10	**224871**
	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5(1) (a)	3.5.7 3.5.8 3.5.9 3.5.10	**224872**
	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5(1) (a)	3.5.7 3.5.8 3.5.9 3.5.10	**224873**
	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5(1) (c)	3.5.7 3.5.8 3.5.9 3.5.10	**224874**
					AU-4(1)		**224875**
					AU-4(1)		**224876**
		AU.3.049			AU-9	3.3.8	**224877**
		AU.3.049			AU-9	3.3.8	**224878**
		AU.3.049			AU-9	3.3.8	**224879**
		AU.3.049			AU-9	3.3.8	**224880**
	AU.2.041 AU.2.042			AU.5.055 IR.5.106	AU-12 c	3.3.1 3.3.2	**224881**
	AU.2.041 AU.2.042			AU.5.055 IR.5.106	AU-12 c	3.3.1 3.3.2	**224882**

CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5	800-53 Rev. 4	800-171	STIG V-ID
	AU.2.041 AU.2.042			AU.5.055 IR.5.106	AC-2(4); AU-12 c	3.1.1 3.1.2	**224883**
	AU.2.041 AU.2.042			AU.5.055 IR.5.106	AC-2(4); AU-12 c	3.1.1 3.1.2	**224884**
	AU.2.041 AU.2.042			AU.5.055 IR.5.106	AC-2(4); AU-12 c	3.1.1 3.1.2	**224885**
	AU.2.041 AU.2.042			AU.5.055 IR.5.106	AC-2(4); AU-12 c	3.1.1 3.1.2	**224886**
	AU.2.041 AU.2.042			AU.5.055 IR.5.106	AU-12 c	3.3.1 3.3.2	**224887**
	AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7	**224888**
	AU.2.041 AU.2.042			AU.5.055 IR.5.106	AC-2(4); AU-12 c	3.1.1 3.1.2	**224889**
	AU.2.041 AU.2.042			AU.5.055 IR.5.106	AC-2(4); AU-12 c	3.1.1 3.1.2	**224890**
	AU.2.041 AU.2.042			AU.5.055 IR.5.106	AU-12 c	3.3.1 3.3.2	**224891**
	AC.2.013 AU.2.041 AU.2.042			AU.5.055 IR.5.106	AC-17(1); AU-12 c	3.1.12 3.3.1 3.3.2	**224892**
	AC.2.013 AU.2.041 AU.2.042			AU.5.055 IR.5.106	AC-17(1); AU-12 c	3.1.12 3.3.1 3.3.2	**224893**
	AC.2.013 AU.2.041 AU.2.042			AU.5.055 IR.5.106	AC-17(1); AU-12 c	3.1.12 3.3.1 3.3.2	**224894**
	AU.2.041 AU.2.042			AU.5.055 IR.5.106	AU-12 c	3.3.1 3.3.2	**224895**

CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5	800-53 Rev. 4	800-171	STIG V-ID
	AU.2.041 AU.2.042			AU.5.055 IR.5.106	AU-12 c	3.3.1 3.3.2	**224896**
	AU.2.041 AU.2.042			AU.5.055 IR.5.106	AU-12 c	3.3.1 3.3.2	**224897**
	AU.2.041 AU.2.042			AU.5.055 IR.5.106	AU-12 c	3.3.1 3.3.2	**224898**
	AU.2.041 AU.2.042			AU.5.055 IR.5.106	AU-12 c	3.3.1 3.3.2	**224899**
	AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7	**224900**
	AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7	**224901**
	AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7	**224902**
	AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7	**224903**
	AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7	**224904**
	AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7	**224905**
	AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7	**224906**

CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5	800-53 Rev. 4	800-171	STIG V-ID
	AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7	**224907**
	AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7	**224908**
	AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7	**224909**
	AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7	**224910**
	AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7	**224911**
	AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7	**224912**
	AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7	**224913**
	CM.2.062				CM-7 a	3.4.6	**224914**
	CM.2.062				CM-7 a	3.4.6	**224915**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**224916**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**224917**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**224918**
					SC-5		**224919**

CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5	800-53 Rev. 4	800-171	STIG V-ID
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**224920**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**224921**
	AU.2.041 AU.2.042				AU-3(1)	3.3.1 3.3.2	**224922**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**224923**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**224924**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**224925**
	CM.2.062				CM-7 a	3.4.6	**224926**
	CM.2.062				CM-7 a	3.4.6	**224927**
	CM.2.062				CM-7 a	3.4.6	**224928**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**224929**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**224930**
	CM.2.062				CM-7 a	3.4.6	**224931**
		CM.3.068			CM-7(2)	3.4.7	**224932**
		CM.3.068			CM-7(2)	3.4.7	**224933**
		CM.3.068			CM-7(2)	3.4.7	**224934**
					SC-3		**224935**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**224936**
					AU-4		**224937**
					AU-4		**224938**
					AU-4		**224939**
	CM.2.062				CM-7 a	3.4.6	**224940**
					SI-16		**224941**

CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5	800-53 Rev. 4	800-171	STIG V-ID
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**224942**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**224943**
					IA-11		**224944**
		SC.3.182			SC-4	3.13.4	**224945**
					IA-11		**224946**
		AC.3.014			AC-17(2)	3.1.13	**224947**
		AC.3.014			AC-17(2)	3.1.13	**224948**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**224949**
	CM.2.062				CM-7 a	3.4.6	**224951**
	CM.2.062				CM-7 a	3.4.6	**224952**
	CM.2.063				CM-11(2)	3.4.9	**224953**
	CM.2.063				CM-11(2)	3.4.9	**224954**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**224955**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**224956**
	AU.2.041 AU.2.042				AU-3(1)	3.3.1 3.3.2	**224957**
	MA.2.113				MA-4 c	3.7.5	**224958**
	MA.2.113				MA-4(6)	3.7.5	**224959**
	MA.2.113				MA-4 c	3.7.5	**224960**
	MA.2.113				MA-4 c	3.7.5	**224961**
	MA.2.113				MA-4(6)	3.7.5	**224962**

CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5	800-53 Rev. 4	800-171	STIG V-ID
					IA-11		**224963**
		AC.3.018			AC-6(10)	3.1.7	**224964**
		IA.3.084			IA-2(8); IA-2(9)	3.5.4	**224965**
		IA.3.084			IA-2(8); IA-2(9)	3.5.4	**224966**
		IA.3.084			IA-2(8); IA-2(9)	3.5.4	**224967**
		IA.3.084			IA-2(8); IA-2(9)	3.5.4	**224968**
		IA.3.084			IA-2(8); IA-2(9)	3.5.4	**224969**
		AC.3.018			AC-6(10)	3.1.7	**224970**
		AC.3.018			AC-6(10)	3.1.7	**224971**
		AC.3.018			AC-6(10)	3.1.7	**224972**
		AC.3.018			AC-6(10)	3.1.7	**224973**
		AC.3.018			AC-6(10)	3.1.7	**224974**
		SC.3.182			SC-4	3.13.4	**224975**
	CM.2.062				CM-7 a	3.4.6	**224976**
		SC.3.177			SC-13	3.13.11	**224977**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**224978**
		SC.3.186			SC-10	3.13.9	**224979**
	AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7	**224980**
	AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7	**224981**

CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5	800-53 Rev. 4	800-171	STIG V-ID
	AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7	**224982**
	AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7	**224983**
	AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7	**224984**
	AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7	**224985**
	AU.2.041 AU.2.042			AU.5.055 IR.5.106	AC-2(4); AU-12 c	3.1.1 3.1.2	**224986**
	AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7	**224987**
	AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7	**224988**
	AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7	**224989**
	AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106	AC-6(9); AU-12 c	3.3.1 3.3.2 3.1.7	**224990**
					IA-5(2) (a)		**224991**
					IA-5(2) (a)		**224992**
					IA-5(2) (a)		**224993**

CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5	800-53 Rev. 4	800-171	STIG V-ID
		IA.3.083			IA-2(1); IA-2(2); IA-2(3); IA-2(4); IA-2(11)	3.5.3	**224994**
		SC.3.185 SI.3.219			SC-8; SC-8 (1)	3.13.8	**224995**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**224996**
AC.1.001 AC 1.002					AC-3	3.1.1 3.1.2	**224997**
		AC.3.018			AC-6(10)	3.1.7	**224998**
AC.1.001 AC 1.002					AC-3	3.1.1 3.1.2	**224999**
AC.1.001 AC 1.002					AC-3	3.1.1 3.1.2	**225000**
AC.1.001 AC 1.002					AC-3	3.1.1 3.1.2	**225001**
AC.1.001 AC 1.002					AC-3	3.1.1 3.1.2	**225002**
AC.1.001 AC 1.002					AC-3	3.1.1 3.1.2	**225003**
	AC.2.013				AC-17(1)	3.1.12	**225004**
		AC.3.018			AC-6(10)	3.1.7	**225005**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**225006**
		AC.3.018			AC-6(10)	3.1.7	**225007**
					SC-3		**225008**
	CM.2.062				CM-7 a	3.4.6	**225009**
IA 1.076 IA 1.077					IA-3(1)	3.5.1 3.5.2	**225010**

CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5	800-53 Rev. 4	800-171	STIG V-ID
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**225011**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**225012**
		AC.3.017			AC-6(10)	3.1.7	**225013**
AC.1.001 AC 1.002					AC-3	3.1.1 3.1.2	**225014**
AC.1.001 AC 1.002					AC-3	3.1.1 3.1.2	**225015**
AC.1.001 AC 1.002					AC-3	3.1.1 3.1.2	**225016**
AC.1.001 AC 1.002					AC-3	3.1.1 3.1.2	**225017**
AC.1.001 AC 1.002					AC-3	3.1.1 3.1.2	**225018**
	AC.2.013				AC-17(1)	3.1.12	**225019**
		AC.3.018			AC-6(10)	3.1.7	**225020**
					IA-5(2) (a); SC-23(5)		**225021**
					IA-5(2) (a); SC-23(5)		**225022**
					IA-5(2) (a); SC-23(5)		**225023**
					IA-8		**225024**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**225025**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**225026**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**225027**

CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5	800-53 Rev. 4	800-171	STIG V-ID
	AU.2.041 AU.2.042			AU.5.055 IR.5.106	AU-12 c	3.3.1 3.3.2	**225028**
		SC.3.185 SI.3.219			SC-8; SC-8(1)	3.13.8	**225029**
		SC.3.185 SI.3.219			SC-8; SC-8(1)	3.13.8	**225030**
		SC.3.185 SI.3.219			SC-8; SC-8(1)	3.13.8	**225031**
IA 1.076 IA 1.077					IA-3(1)	3.5.1 3.5.2	**225032**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**225033**
		SC.3.185 SI.3.219			SC-8; SC-8(1)	3.13.8	**225034**
	AC.2.010				AC-11 a	3.1.10	**225035**
	AC2.005				AC-8 a; AC-8 b; AC-8 c 1; AC-8 c 2; AC-8 c 3	3.1.9	**225036**
	AC2.005				AC-8 a; AC-8 c 1; AC-8 c 2; AC-8 c 3	3.1.9	**225037**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**225038**
		SC.3.185 SI.3.219			SC-8; SC-8(1)	3.13.8	**225039**
		SC.3.185 SI.3.219			SC-8; SC-8(1)	3.13.8	**225040**

CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5	800-53 Rev. 4	800-171	STIG V-ID
	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5(1) (c)	3.5.7 3.5.8 3.5.9 3.5.10	**225041**
		SC.3.185 SI.3.219			SC-8; SC-8(1)	3.13.8	**225042**
		SC.3.185 SI.3.219			SC-8; SC-8(1)	3.13.8	**225043**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**225044**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**225045**
		SC.3.182			SC-4	3.13.4	**225046**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**225047**
		SC.3.182			SC-4	3.13.4	**225048**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**225049**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**225050**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**225051**
					IA-7		**225052**
	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5(1) (c)	3.5.7 3.5.8 3.5.9 3.5.10	**225053**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**225054**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**225055**

CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5	800-53 Rev. 4	800-171	STIG V-ID
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**225056**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**225057**
					IA-5(2)		**225058**
		AC.3.014 SC.3.177			AC-17(2); SC-13	3.1.13 3.13.11	**225059**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**225060**
					IA-11		**225061**
					SC-3		**225062**
					SC-3		**225063**
					IA-11		**225064**
					SC-3		**225065**
					SC-3		**225066**
					IA-11		**225067**
					SC-3		**225068**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**225069**
		AC.3.018			AC-6(10)	3.1.7	**225070**
		AC.3.018			AC-6(10)	3.1.7	**225071**
AC.1.001 AC 1.002					AC-3	3.1.1 3.1.2	**225072**
		AC.3.018			AC-6(10)	3.1.7	**225073**
		AC.3.018			AC-6(10)	3.1.7	**225074**
		AC.3.018			AC-6(10)	3.1.7	**225076**
		AC.3.018			AC-6(10)	3.1.7	**225077**
		AC.3.018			AC-6(10)	3.1.7	**225078**
		AC.3.018			AC-6(10)	3.1.7	**225079**
		AC.3.018			AC-6(10)	3.1.7	**225080**
		AC.3.018			AC-6(10)	3.1.7	**225081**

CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5	800-53 Rev. 4	800-171	STIG V-ID
		AC.3.018			AC-6(10)	3.1.7	**225082**
		AC.3.018			AC-6(10)	3.1.7	**225083**
		AC.3.018			AC-6(10)	3.1.7	**225084**
		AC.3.018			AC-6(10)	3.1.7	**225085**
	AU.2.041 AU.2.042	AC.3.018 AU.3.049 AU.3.050		AU.5.055 IR.5.106	AU-9; AU-12 b; AU-12(3)	3.3.1 3.3.2 3.3.8	**225086**
		AC.3.018			AC-6(10)	3.1.7	**225087**
		AC.3.018			AC-6(10)	3.1.7	**225088**
		AC.3.018			AC-6(10)	3.1.7	**225089**
		AC.3.018			AC-6(10)	3.1.7	**225091**
		AC.3.018			AC-6(10)	3.1.7	**225092**
		AC.3.018			AC-6(10)	3.1.7	**225093**

SteelCloud

III. CMMC Control MATRIX

Capability	CMMC Control #	NIST 800-171 R1	NIST 800-171 B	NIST 800-53 R4	Control	Maturity Level				
						ML 1	ML 2	ML 3	ML 4	ML 5
PROCESS MATURITY (ML)										
MC01 Improve [DOMAIN NAME] activities	ML.2.999				Establish a policy that includes [DOMAIN NAME].		X			
	ML.2.998				Document the CMMC practices to implement the [DOMAIN NAME] policy.		X			
	ML.3.997				Establish, maintain, and resource a plan that includes [DOMAIN NAME]			X		
	ML.4.996				Review and measure [DOMAIN NAME] activities for effectiveness.				X	
	ML.5.995				Standardize and optimize a documented approach for [DOMAIN NAME] across all applicable organizational units.					X
ACCESS CONTROL (AC)										
C001 Establish system access requirements	AC.1.001	3.1.1		AC-2; AC-3; AC-17	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	X				
	AC.2.005	3.1.9		AC-8	Provide Privacy and security notices consistent with applicable CUI rules.		X			
	AC.2.006	3.1.21		AC-20(2)	Limit use of portable storage device on external systems.		X			
C002 Control internal system access	AC.1.002	3.1.2		AC-2; AC-3; AC-17	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	X				
	AC.2007	3.1.5		AC-6; AC-6(1); AC-6(5)	Employ the principle of least privilege, including for specific security functions and privileged accounts.		X			
	AC.2008	3.1.6		AC-6(2)	Use non-privileged accounts or roles when accessing nonsecurity functions.		X			
	AC.2009	3.1.8		AC-7	Limit unsuccessful logon attempts.		X			
	AC.2010	3.1.10		AC-11 AC-11(1)	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.		X			
	AC.2.011	3.1.16		AC-18	Authorize wireless access prior to allowing such connections.		X			
	AC.3.017	3.1.4		AC-5	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.			X		

III. CMMC Control MATRIX

Capability	CMMC Control #	NIST 800-171 R1	NIST 800-171 B	NIST 800-53 R4	Control	Maturity Level				
						ML 1	ML 2	ML 3	ML 4	ML 5
	AC.3.018	3.1.7		AC-6(9); AC-6(10)	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.			X		
	AC.3.019	3.1.11		AC-12	Terminate (automatically) user sessions after a defined condition.			X		
	AC.3.012	3.1.17		AC-18(1)	Protect wireless access using authentication and encryption.			X		
	AC.3.020	3.1.18		AC-19	Control Connection of mobile devices.			X		
	AC.4.023		3.1.3e	AC-4; AC-4(1); AC-4(6); AC-4(8); AC-4(12); AC-4(13); AC-4(15); AC-4(20)	Control information flows between security domains on connected systems.				X	
	AC.4.025				Periodically review and update CUI program access permissions.				X	
	AC.5.024			SI-4(14)	Identify and mitigate risk associated with unidentified wireless access points connected to the network.					X
C003 Control remote system access	AC.2.013	3.1.12		AC-17(1)	Monitor and control remote access sessions.		X			
	AC.2.015	3.1.14		AC-17(3)	Route remote access via managed access control points.		X			
	AC.3.014	3.1.13		AC-17(2)	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.			X		
	AC.3.021	3.1.15		AC-17(4)	Authorize remote execution of privileged commands and remote access to security-relevant information.			X		
	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.				X	

SteelCloud

III. CMMC Control MATRIX

Capability	CMMC Control #	NIST 800-171 R1	NIST 800-171 B	NIST 800-53 R4	Control	Maturity Level				
						ML 1	ML 2	ML 3	ML 4	ML 5
C004 Limit data access to authorized users and processes	AC.1.003	3.1.20		AC-20; AC-20(1)	Verify and control/limit connections to and use of external information systems.	X				
	AC.1.004	3.1.22		AC-22	Control information posted or processed on publicly accessible information systems.	X				
	AC.2.016	3.1.3		AC-4	Control the flow of CUI in accordance with approved authorizations.		X			
	AC.3.022	3.1.19		AC-19(5)	Encrypt CUI on mobile devices and mobile computing platforms.			X		
ASSET MANAGEMENT (AM)										
C005 Identify and document assets	AM.3.036				Define procedures for the handling of CUI data.			X		
C006 Manage asset inventory	AM.4.226		3.4.3e	CM-8	Employ a capability to discover and identify systems with specific component attributes (e.g., firmware level, OS type) within your inventory.				X	
AUDIT AND ACCOUNTABILITY (AU)										
C007 Define audit requirements	AU.2.041	3.3.2		AU-2; AU-3; AU-3(1); AU-6; AU-11; AU-12	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.		X			
	AU.3.045	3.3.3		AU-2(3)	Review and update logged events.			X		
	AU.3.046	3.3.4		AU-5	Alert in the event of an audit logging process failure.			X		
C008 Perform auditing	AU.2.042	3.3.1		AU-2; AU-3; AU-3(1); AU-6; AU-11; AU-12	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.		X			
	AU.2.043	3.3.7		AU-8; AU-8(1)	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.		X			

III. CMMC Control MATRIX

Capability	CMMC Control #	NIST 800-171 R1	NIST 800-171 B	NIST 800-53 R4	Control	Maturity Level				
						ML 1	ML 2	ML 3	ML 4	ML 5
	AU.3.048			AU-6(4)	Collect audit information (e.g., logs) into one or more central repositories.			X		
	AU.5.055			AU-12	Identify assets not reporting audit logs and assure appropriate organizationally defined systems are logging.					X
C009 Identify and protect audit information	AU.3.049	3.3.8		AU-6(7); AU-9	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.			X		
	AU.3.050	3.3.9		AU-6(7); AU-9(4)	Limit management of audit logging functionality to a subset of privileged users.			X		
C010 Review and manage audit logs	AU.2.044			AU-6	Review audit logs.		X			
	AU.3.051	3.3.5		AU-6(3)	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.			X		
	AU.3.052	3.3.6		AU-7	Provide audit record reduction and report generation to support on-demand analysis and reporting.			X		
	AU.4.053			SI-4(2)	Automate analysis of audit logs to identify and act on critical indicators (TTPs) and/or organizationally defined suspicious activity.				X	
	AU.4.054			RA-5(6); RA-5(8); RA-5(10)	Review audit information for broad activity in addition to per-machine activity.				X	
AWARENESS AND TRAINING (AT)										
C011 Conduct security awareness activities	AT.2.056	3.2.1		AT-2; AT-3	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.		X			
	AT.3.058	3.2.3		AT-2(2)	Provide security awareness training on recognizing and reporting potential indicators of insider threat.			X		
	AT.4.059		3.2.1e	AT-2	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.				X	
	AT.4.060		3.2.2e	AT-2(1)	Include practical exercises in awareness training that are aligned with current threat scenarios and provide feedback to individuals involved in the training.				X	

III. CMMC Control MATRIX

Capability	CMMC Control #	NIST 800-171 R1	NIST 800-171 B	NIST 800-53 R4	Control	Maturity Level				
						ML 1	ML 2	ML 3	ML 4	ML 5
C012 Conduct training	AT.2.057	3.2.2		AT-2; AT-3	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.		X			
CONFIGURATION MANAGEMENT (CM)										
C013 Establish configuration baselines	CM.2.061	3.4.1		CM-2; CM-6; CM-8; CM-8(1)	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.		X			
	CM.2.062	3.4.6		CM-7	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.		X			
	CM.2.063	3.4.9		CM-11	Control and monitor user-installed software.		X			
C014 Perform configuration and change management	CM.2.064	3.4.2		CM-2; CM-6; CM-8; CM-8(1)	Establish and enforce security configuration settings for information technology products employed in organizational systems.		X			
	CM.2.065	3.4.3		CM-3	Track, review, approve, or disapprove, and log changes to organizational systems.		X			
	CM.2.066	3.4.4		CM-4	Analyze the security impact of changes prior to implementation.		X			
	CM.3.067	3.4.5		CM-5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.			X		
	CM.3.068	3.4.7		CM-7(1); CM-7(2)	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.			X		
	CM.3.069	3.4.8		CM-7(4); CM-7(5)	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.			X		
	CM.4.073	3.4.8		CM-7(4); CM-7(5)	Employ application whitelisting and an application vetting process for systems identified by the organization.				X	
	CM.5.074		3.14.1e	SI-7(6); SI-7(9); SI-7(10); SA-17	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).					X

SteelCloud

III. CMMC Control MATRIX

Capability	CMMC Control #	NIST 800-171 R1	NIST 800-171 B	NIST 800-53 R4	Control	Maturity Level				
						ML 1	ML 2	ML 3	ML 4	ML 5
IDENTIFICATION AND AUTHENTICATION (IA)										
C015 Grant access to authenticated entities	IA.1.076	3.5.1		IA-2; IA-3; IA-5	Identify information system users, processes acting on behalf of users, or devices.	X				
	IA.1.077	3.5.2		IA-2; IA-3; IA-5	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	X				
	IA.2.078	3.5.7		IA-5(1)	Enforce a minimum password complexity and change of characters when new passwords are created.		X			
	IA.2.079	3.5.8		IA-5(1)	Prohibit password reuse for a specified number of generations.		X			
	IA.2.080	3.5.9		IA-5(1)	Allow temporary password use for system logons with an immediate change to a permanent password.		X			
	IA.2.081	3.5.10		IA-5(1)	Store and transmit only cryptographically-protected passwords.		X			
	IA.2.082	3.5.11		IA-6	Obscure feedback of authentication information.		X			
	IA.3.083	3.5.3		IA-2(1); IA-2(2); IA-2(3)	Use multifactor authentication for local and network access to privileged accounts and for network access to nonprivileged accounts.			X		
	IA.3.084	3.5.4		IA-2(8); IA-2(9)	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.			X		
	IA.3.085	3.5.5		IA-4	Prevent the reuse of identifiers for a defined period.			X		
	IA.3.086	3.5.6		IA-4	Disable identifiers after a defined period of inactivity.			X		

III. CMMC Control MATRIX

Capability	CMMC Control #	NIST 800-171 R1	NIST 800-171 B	NIST 800-53 R4	Control	Maturity Level				
						ML 1	ML 2	ML 3	ML 4	ML 5
INCIDENT RESPONSE (IR)										
C016 Plan incident response	IR.2.092	3.6.1		IR-2; IR-4	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.		X			
	IR.4.100				Use knowledge of attacker tactics, techniques, and procedures in incident response planning and execution.				X	
	IR.5.106			AU-12	In response to cyber incidents, utilize forensic data gathering across impacted systems, ensuring the secure transfer and protection of forensic data.					X
C017 Detect and report events	IR.2.093			IR-6	Detect and report events.		X			
	IR.2.094			IR-4(3)	Analyze and triage events to support event resolution and incident declaration.		X			
C018 Develop and implement a response to a declared incident	IR.2.096			IR-4	Develop and implement responses to declared incidents according to pre-defined procedures.		X			
	IR.3.098	3.6.2		IR-6; IR-7	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.			X		
	IR.4.101		3.6.1e		Establish and maintain a security operations center capability that facilitates a 24/7 response capability.				X	
	IR.5.102			IR-4(1)	Use a combination of manual and automated, real-time responses to anomalous activities that match incident patterns.					X
	IR.5.108		3.6.2e		Establish and maintain a cyber incident response team that can investigate an issue physically or virtually at any location within 24 hours.					X
C019 Perform post incident reviews	IR.2.097			AU-2	Perform root cause analysis on incidents to determine underlying causes.		X			
C020 Test incident response	IR.3.099	3.6.3		IR-3	Test the organizational incident response capability.			X		
	IR.5.110				Perform unannounced operational exercises to demonstrate technical and procedural responses.					X
MAINTENANCE (MA)										

SteelCloud

III. CMMC Control MATRIX

Capability	CMMC Control #	NIST 800-171 R1	NIST 800-171 B	NIST 800-53 R4	Control	Maturity Level				
						ML 1	ML 2	ML 3	ML 4	ML 5
C021 Manage maintenance	MA.2.111	3.7.1		MA-2	Perform maintenance on organizational systems.		X			
	MA.2.112	3.7.2		MA-3	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.		X			
	MA.2.113	3.7.5		MA-4	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.		X			
	MA.2.114	3.7.6		MA-5	Supervise the maintenance activities of personnel without required access authorization.		X			
	MA.3.115	3.7.3		MA-2	Ensure equipment removed for off-site maintenance is sanitized of any CUI.			X		
	MA.3.116	3.7.4		MA-3(2)	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.			X		
MEDIA PROTECTION (MP)										
C022 Identify and mark media	MP.3.122	3.8.4		MP-3	Mark media with necessary CUI markings and distribution limitations.			X		
C023 Protect and control media	MP.2.119	3.8.1		MP-4	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.		X			
	MP.2.120	3.8.2		MP-2	Limit access to CUI on system media to authorized users.		X			
	MP.2.121	3.8.7		MP-7	Control the use of removable media on system components.		X			
	MP.3.123	3.8.8		MP-7(1)	Prohibit the use of portable storage devices when such devices have no identifiable owner.			X		
C024 Sanitize media	MP.1.118	3.8.3		MP-6	Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.	X				

SteelCloud

III. CMMC Control MATRIX

Capability	CMMC Control #	NIST 800-171 R1	NIST 800-171 B	NIST 800-53 R4	Control	Maturity Level				
						ML 1	ML 2	ML 3	ML 4	ML 5
C025 Protect media during transport	MP.3.124	3.8.5		MP-5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.			X		
	MP.3.125	3.8.6		MP-5(4)	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.			X		
PERSONNEL SECURITY (SP)										
C026 Screen personnel	PS.2.127	3.9.1		PS-3	Screen individuals prior to authorizing access to organizational systems containing CUI.		X			
C027 Protect CUI during personnel actions	PS.2.128	3.9.2		PS-4; PS-5	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.		X			
PHYSICAL PROTECTION (PE)										
C028 Limit physical access	PE.1.131	3.10.1		PE-2	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	X				
	PE.1.132	3.10.3		PE-3	Escort visitors and monitor visitor activity.	X				
	PE.1.133	3.10.4		PE-3	Maintain audit logs of physical access.	X				
	PE.1.134	3.10.5		PE-3	Control and manage physical access devices.	X				
	PE.2.135	3.10.2		PE-6	Protect and monitor the physical facility and support infrastructure for organizational systems.		X			
	PE.3.136	3.10.6		PE-17	Enforce safeguarding measures for CUI at alternate work sites.			X		
RECOVERY (RE)										
C029 Manage backups	RE.2.137			CP-9	Regularly perform and test data backups.		X			
	RE.2.138	3.8.9		CP-9	Protect the confidentiality of backup CUI at storage locations.		X			
	RE.3.139			CP-9; CP-9(3)	Regularly perform complete, comprehensive, and resilient data backups as organizationally defined.			X		
C030 Manage information security continuity	RE.5.140			CP-10	Ensure information processing facilities meet organizationally defined information security continuity, redundancy, and availability requirements.					X
RISK MANAGEMENT (RM)										

SteelCloud

III. CMMC Control MATRIX

Capability	CMMC Control #	NIST 800-171 R1	NIST 800-171 B	NIST 800-53 R4	Control	Maturity Level				
						ML 1	ML 2	ML 3	ML 4	ML 5
C031 Identify and evaluate risk	RM.2.141	3.11.1		RA-3	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.		X			
	RM.2.142	3.11.2		RA-5	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.		X			
	RM.3.144			RA-3	Periodically perform risk assessments to identify and prioritize risks according to the defined risk categories, risk sources, and risk measurement criteria.			X		
	RM.4.149				Catalog and periodically update threat profiles and adversary TTPs.				X	
	RM.4.150		3.11.1e		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.				X	
	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.				X	
C032 Manage risk	RM.2.143	3.11.3		RA-5	Remediate vulnerabilities in accordance with risk assessments.		X			
	RM.3.146			PM-9	Develop and implement risk mitigation plans.			X		
	RM.3.147			SA-22(1)	Manage non-vendor supported products (e.g., end of life) separately and restrict as necessary to reduce risk.			X		
	RM.5.152				Utilize an exception process for non-whitelisted software that includes mitigation techniques.					X
	RM.5.155		3.11.5e		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.					X
C033 Manage supply chain risk	RM.4.148		3.11.7e	SA-12	Develop and update as required, a plan for managing supply chain risks associated with the IT supply chain.				X	

SteelCloud

III. CMMC Control MATRIX

Capability	CMMC Control #	NIST 800-171 R1	NIST 800-171 B	NIST 800-53 R4	Control	Maturity Level				
						ML 1	ML 2	ML 3	ML 4	ML 5
SECURITY ASSESSMENT (CA)										
C034 Develop and manage a system security plan	CA.2.157	3.12.4		PL-2	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.		X			
	CA.4.163			PL-1	Create, maintain, and leverage a security strategy and roadmap for organizational cybersecurity improvement.				X	
C035 Define and manage controls	CA.2.158	3.12.1		CA-2	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.		X			
	CA.2.159	3.12.2		CA-5	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.		X			
	CA.3.161	3.12.3		CA-7	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.			X		
	CA.4.164		3.12.1e	CA-8	Conduct penetration testing periodically, leveraging automated scanning tools and ad hoc tests using human experts.				X	
	CA.4.227			CA-8(2)	Periodically perform red teaming against organizational assets in order to validate defensive capabilities.				X	
C036 Perform code reviews	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.			X		
SITUATIONAL AWARENESS (SA)										
C037 Implement threat monitoring	SA.3.169			PM-16	Receive and respond to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders.			X		
	SA.4.171		3.11.2e	PM-16	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.				X	
	SA.4.173			SI-4(24)	Design network and system security capabilities to leverage, integrate, and share indicators of compromise.				X	
SYSTEM AND COMMUNICATIONS PROTECTION (SC)										

III. CMMC Control MATRIX

Capability	CMMC Control #	NIST 800-171 R1	NIST 800-171 B	NIST 800-53 R4	Control	Maturity Level				
						ML 1	ML 2	ML 3	ML 4	ML 5
C038 Define security requirements for systems and communications	SC.2.178	3.13.12		SC-15	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.		X			
	SC.2.179				Use encrypted sessions for the management of network devices.		X			
	SC.3.177	3.13.11		SC-13	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.			X		
	SC.3.180	3.13.2		SA-8	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.			X		
	SC.3.181	3.13.3		SC-2	Separate user functionality from system management functionality.			X		
	SC.3.182	3.13.4		SC-4	Prevent unauthorized and unintended information transfer via shared system resources.			X		
	SC.3.183	3.13.6		SC-7(5)	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).			X		
	SC.3.184	3.13.7		SC-7(7)	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).			X		
	SC.3.185	3.13.8		SC-8(1)	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.			X		
	SC.3.186	3.13.9		SC-10	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.			X		
	SC.3.187	3.13.10		SC-12	Establish and manage cryptographic keys for cryptography employed in organizational systems.			X		
	SC.3.188	3.13.13		SC-18	Control and monitor the use of mobile code.			X		
	SC.3.189	3.13.14		SC-19	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.			X		
	SC.3.190	3.13.15		SC-23	Protect the authenticity of communications sessions.			X		
	SC.3.191	3.13.16		SC-28	Protect the confidentiality of CUI at rest.			X		
	SC.4.197		3.13.4e	AC-5	Employ physical and logical isolation techniques in the system and security architecture and/or where deemed appropriate by the organization.				X	

III. CMMC Control MATRIX

Capability	CMMC Control #	NIST 800-171 R1	NIST 800-171 B	NIST 800-53 R4	Control	Maturity Level				
						ML 1	ML 2	ML 3	ML 4	ML 5
	SC.4.228	3.13.2		SA-8	Isolate administration of organizationally defined high-value critical network infrastructure components and servers.				X	
	SC.5.198				Configure monitoring systems to record packets passing through the organization's Internet network boundaries and other organizationally defined boundaries.					X
	SC.5.230			SC-7(17)	Enforce port and protocol compliance.					X
C039 Control communications at system boundaries	SC.1.175	3.13.1		SC-7	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.	X				
	SC.1.176	3.13.5		SC-7	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	X				
	SC.3.192			SC-20	Implement Domain Name System (DNS) filtering services.			X		
	SC.3.193				Implement a policy restricting the publication of CUI on externally owned, publicly accessible websites (e.g., forums, LinkedIn, Facebook, Twitter).			X		
	SC.4.199				Utilize threat intelligence to proactively block DNS requests from reaching malicious domains.				X	
	SC.4.202			SC-44	Employ mechanisms to analyze executable code and scripts (e.g., sandbox) traversing Internet network boundaries or other organizationally defined boundaries.				X	
	SC.4.229				Utilize a URL categorization service and implement techniques to enforce URL filtering of websites that are not approved by the organization.				X	
	SC.5.208				Employ organizationally defined and tailored boundary protections in addition to commercially available solutions.					X
SYSTEM AND INFORMATION SECURITY (SI)										
C040 Identify and manage information system flaws	SI.1.210	3.14.1		SI-2	Identify, report, and correct information and information system flaws in a timely manner.	X				
	SI.2.214	3.14.3		SI-5	Monitor system security alerts and advisories and take action in response.		X			

SteelCloud

III. CMMC Control MATRIX

Capability	CMMC Control #	NIST 800-171 R1	NIST 800-171 B	NIST 800-53 R4	Control	Maturity Level				
						ML 1	ML 2	ML 3	ML 4	ML 5
	SI.4.221		3.14.6e		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.				X	
C041 Identify malicious content	SI.1.211	3.14.2		SI-3	Provide protection from malicious code at appropriate locations within organizational information systems.	X				
	SI.1.212	3.14.4		SI-3	Update malicious code protection mechanisms when new releases are available.	X				
	SI.1.213	3.14.5		SI-3	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	X				
	SI.5.222				Analyze system behavior to detect and mitigate execution of normal system commands and scripts that indicate malicious actions.					X
C042 Perform network and system monitoring	SI.2.216	3.14.6		SI-4	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.		X			
	SI.2.217	3.14.7		SI-4	Identify unauthorized use of organizational systems.		X			
	SI.3.218			SI-8	Employ spam protection mechanisms at information system access entry and exit points.			X		
	SI.5.223		3.14.2e	SI-4	Monitor individuals and system components on an ongoing basis for anomalous or suspicious behavior.					X
C043 Implement advanced	SI.3.219			SC-8	Implement email forgery protections.			X		
	SI.3.220			SC-44	Utilize sandboxing to detect or block potentially malicious email.			X		