Get Compliant. Stay Compliant.

STIG & CMMC Control Matrix

for Windows 10

SteelCloud

June 2020

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

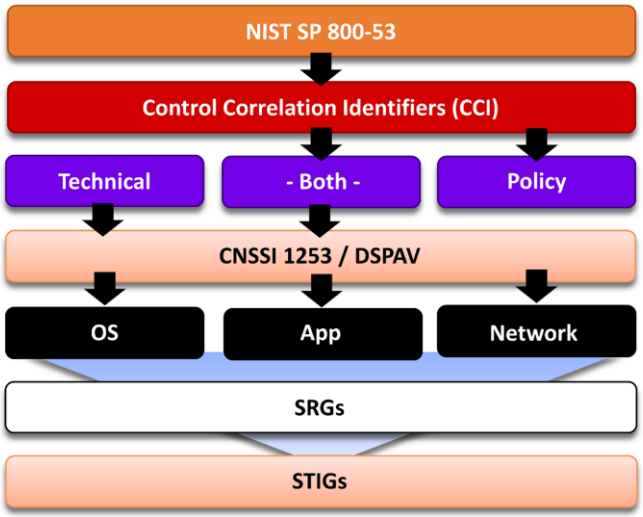
SteelCloud has spent the last decade developing patented technology to automate government policy compliance, configuration control, and cloud security. Our ConfigOS software solution was designed to reduce initial hardening time by 90% and ongoing STIG compliance effort by more than 70%. Our technology 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

I. STIG to CMMC Matrix

Windows 10

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
63319	Domain-joined systems must use Windows 10 Enterprise Edition 64-bit version.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63323	Windows 10 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			
63329	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			
63333	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			
63335	The Windows Remote Management (WinRM) client must not use Basic authentication.	MA-4 c	3.7.5		MA.2.113			
63337	Windows 10 information systems must use BitLocker to encrypt all disks to protect the confidentiality and integrity of all information at rest.	SC-28;SC-28 (1)	3.13.16			SC.3.191		
63341	The Windows Remote Management (WinRM) client must not use Digest authentication.	MA-4 c	3.7.5		MA.2.113			
63345	The operating system 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	
63347	The Windows Remote Management (WinRM) service must not use Basic authentication.	MA-4 c	3.7.5		MA.2.113			
63349	Windows 10 systems must be maintained at a supported servicing level.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63351	The Windows 10 system must use an anti-virus program.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63353	Local volumes must be formatted using NTFS.	AC-3	3.1.1 3.1.2	AC.1.001 AC.1.002				
63355	Alternate operating systems must not be permitted on the same system.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63357	Non system-created file shares on a system must limit access to groups that require it.	SC-4	3.13.4			SC.3.182		
63359	Unused accounts must be disabled or removed from the system after 35 days of inactivity.	IA-4 e	3.5.5 3.5.6			IA.3.085 IA.3.086		
63361	Only accounts responsible for the administration of a system must have Administrator rights on the system.	AC-6 (10)	3.1.7			AC.3.018		

SteelCloud

I. STIG to CMMC Matrix

Windows 10

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
63363	Only accounts responsible for the backup operations must be members of the Backup Operators group.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63365	Only authorized user accounts must be allowed to create or run virtual machines on Windows 10 systems.	CM-7 a	3.4.1		CM.2.062			
63367	Standard local user accounts must not exist on a system in a domain.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63371	Accounts must be configured to require password expiration.	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			
63373	Permissions for system files and directories must conform to minimum requirements.	AC-3 (4)	3.1.1 3.1.2	AC.1.001 AC.1.002				
63377	Internet Information System (IIS) or its subcomponents must not be installed on a workstation.	CM-7 a	3.4.1		CM.2.062			
63381	Simple Network Management Protocol (SNMP) must not be installed on the system.	CM-7 b	3.4.1		CM.2.062			
63383	Simple TCP/IP Services must not be installed on the system.	CM-7 a	3.4.1		CM.2.062			
63385	The Telnet Client must not be installed on the system.	CM-7 b	3.4.1		CM.2.062			
63389	The TFTP Client must not be installed on the system.	CM-7 b	3.4.1		CM.2.062			
63393	Software certificate installation files must be removed from Windows 10.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63399	A host-based firewall must be installed and enabled on the system.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63403	Inbound exceptions to the firewall on Windows 10 domain workstations must only allow authorized remote management hosts.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63405	Windows 10 account lockout duration must be configured to 15 minutes or greater.	AC-7 b	3.1.8		AC.2.009			
63409	The number of allowed bad logon attempts must be configured to 3 or less.	AC-7 a	3.1.8		AC.2.009			
63413	The period of time before the bad logon counter is reset must be configured to 15 minutes.	AC-7 a;AC-7 b	3.1.8		AC.2.009			

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
63415	The 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			
63419	The 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			
63421	The minimum password age must be configured to at least 1 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			
63423	Passwords must, at a minimum, be 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			
63427	The built-in Microsoft password complexity filter must be 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			
63429	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			
63431	The system 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
63435	The system 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

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
63445	The system must be configured to audit Account Management - Security Group Management successes.	AC-2 (4);AC-6 (9);AU-12 c	3.1.7 3.3.1 3.3.2		AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106
63447	The system must be configured to audit Account Management - User Account Management failures.	AC-2 (4);AC-6 (9);AU-12 c	3.1.7 3.3.1 3.3.2	AC.1.001 AC.1.002	AU.2.041 AU.2.042			AU.5.055 IR.5.106
63449	The system must be configured to audit Account Management - User Account Management successes.	AC-2 (4);AC-6 (9);AU-12 c	3.1.7 3.3.1 3.3.2		AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106
63451	The system must be configured to audit Detailed Tracking - PNP Activity successes.	AU-12 c	3.3.1 3.3.2		AU.2.041 AU.2.042			AU.5.055 IR.5.106
63453	The system must be configured to audit Detailed Tracking - Process Creation successes.	AU-12 c	3.3.1 3.3.2		AU.2.041 AU.2.042			AU.5.055 IR.5.106
63457	The system 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
63459	The system 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
63463	The system 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
63467	The system 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
63469	The system must be configured to audit Logon/Logoff - Special Logon successes.	AU-12 c	3.3.1 3.3.2		AC.2.013 AU.2.041 AU.2.042			AU.5.055 IR.5.106
63471	The system must be configured to audit Object Access - Removable Storage failures.	AU-12 c	3.3.1 3.3.2		AC.2.013 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
63473	The system must be configured to audit Object Access - Removable Storage successes.	AU-12 c	3.3.1 3.3.2		AC.2.013 AU.2.041 AU.2.042			AU.5.055 IR.5.106
63479	The system must be configured to audit Policy Change - Audit Policy Change successes.	AU-12 c	3.3.1 3.3.2		AC.2.013 AU.2.041 AU.2.042			AU.5.055 IR.5.106
63481	The system must be configured to audit Policy Change - Authentication Policy Change successes.	AC-6 (9);AU-12 c	3.1.7 3.3.1 3.3.2		AC.2.013 AU.2.041 AU.2.042			AU.5.055 IR.5.106
63483	The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	AC-6 (9);AU-12 c	3.1.7 3.3.1 3.3.2		AC.2.013 AU.2.041 AU.2.042			AU.5.055 IR.5.106
63487	The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	AC-6 (9);AU-12 c	3.1.7 3.3.1 3.3.2		AC.2.013 AU.2.041 AU.2.042			AU.5.055 IR.5.106
63491	The system must be configured to audit System - IPSec Driver failures.	AU-12 c	3.3.1 3.3.2		AC.2.013 AU.2.041 AU.2.042			AU.5.055 IR.5.106
63499	The system must be configured to audit System - Other System Events successes.	AU-12 c	3.3.1 3.3.2		AC.2.013 AU.2.041 AU.2.042			AU.5.055 IR.5.106
63503	The system must be configured to audit System - Other System Events failures.	AU-12 c	3.3.1 3.3.2		AC.2.013 AU.2.041 AU.2.042			AU.5.055 IR.5.106
63507	The system must be configured to audit System - Security State Change successes.	AC-6 (9);AU-12 c	3.1.7 3.3.1 3.3.2		AC.2.013 AU.2.041 AU.2.042			AU.5.055 IR.5.106
63513	The system must be configured to audit System - Security System Extension successes.	AC-6 (9);AU-12 c	3.1.7 3.3.1 3.3.2		AC.2.013 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
63515	The system must be configured to audit System - System Integrity failures.	AC-6 (9);AU-12 c	3.1.7 3.3.1 3.3.2		AC.2.013 AU.2.041 AU.2.042			AU.5.055 IR.5.106
63517	The system must be configured to audit System - System Integrity successes.	AC-6 (9);AU-12 c	3.1.7 3.3.1 3.3.2		AC.2.013 AU.2.041 AU.2.042			AU.5.055 IR.5.106
63533	Windows 10 permissions for the Application event log must prevent access by non-privileged accounts.	AU-9	3.3.8			AU.3.049		
63537	Windows 10 permissions for the Security event log must prevent access by non-privileged accounts.	AU-9	3.3.8			AU.3.049		
63541	Windows 10 permissions for the System event log must prevent access by non-privileged accounts.	AU-9	3.3.8			AU.3.049		
63545	Camera access from the lock screen must be disabled.	CM-7 a	3.4.1		CM.2.062			
63549	The display of slide shows on the lock screen must be disabled.	CM-7 a	3.4.1		CM.2.062			
63555	IPv6 source routing must be configured to highest protection.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63559	The system must be configured to prevent IP source routing.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63563	The system 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			
63569	Insecure logons to an SMB server must be disabled.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63577	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			
63581	Simultaneous connections to the Internet or a Windows domain must be limited.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63585	Connections to non-domain networks when connected to a domain authenticated network must be blocked.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63591	Wi-Fi Sense 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
63593	Default permissions for the HKEY_LOCAL_MACHINE registry hive must be maintained.	AC-6 (10)	3.1.7			AC.3.018		
63595	Virtualization Based Security must be enabled on Windows 10 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			
63599	Credential Guard must be running on Windows 10 domain-joined systems.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63601	The built-in administrator account must be disabled.	IA-2	3.5.1 3.5.2	IA.1.076 IA.1.077				
63607	Early Launch Antimalware, Boot-Start Driver Initialization Policy must prevent boot drivers.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63609	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			
63615	Downloading print driver packages over HTTP must be prevented.	CM-7 a	3.4.1		CM.2.062			
63617	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			
63619	The built-in administrator account must be renamed.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63621	Web publishing and online ordering wizards must be prevented from downloading a list of providers.	CM-7 a	3.4.1		CM.2.062			
63623	Printing over HTTP must be prevented.	CM-7 a	3.4.1		CM.2.062			
63625	The built-in guest account must be renamed.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63627	Systems must at least attempt device authentication using certificates.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63629	The network selection user interface (UI) must not be displayed on the logon screen.	CM-7 a	3.4.1		CM.2.062			
63633	Local users on domain-joined computers must not be enumerated.	CM-7 a	3.4.1		CM.2.062			
63635	Audit policy using subcategories must be enabled.	AU-12 a	3.3.1 3.3.2		AU.2.041 AU.2.042 IR.2.097			AU.5.055 IR.5.106
63639	Outgoing secure channel traffic must be encrypted or signed.	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
63643	Outgoing secure channel traffic must be encrypted when possible.	SC-8;SC-8 (1)	3.13.8			SC.3.185 SI.3.219		
63647	Outgoing secure channel traffic must be signed when possible.	SC-8;SC-8 (1)	3.13.8			SC.3.185 SI.3.219		
63651	Solicited Remote Assistance must not be allowed.	SC-4	3.13.4			SC.3.182		
63653	The computer account password must not be prevented from being reset.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63659	The setting to allow Microsoft accounts to be optional for modern style apps must be enabled.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63661	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			
63663	The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	CM-7 a	3.4.1		CM.2.062			
63665	The system must be configured to require a strong session key.	SC-8;SC-8 (1)	3.13.8			SC.3.185 SI.3.219		
63667	Autoplay must be turned off for non-volume devices.	CM-7 (2)	3.4.7			CM.3.068		
63669	The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver.	AC-11 a	3.1.10		AC.2.010			
63671	The default autorun behavior must be configured to prevent autorun commands.	CM-7 (2)	3.4.7			CM.3.068		
63673	Autoplay must be disabled for all drives.	CM-7 (2)	3.4.7			CM.3.068		
63675	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		AC.2.005			
63677	Enhanced anti-spoofing for facial recognition must be enabled on Window 10.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63681	The Windows dialog box title for the legal banner must be configured.	AC-8 a;AC-8 c 1;AC-8 c 2;AC-8 c 3	3.1.9		AC.2.005			

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
63683	Windows Telemetry must not be configured to Full.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63685	The Windows Defender SmartScreen for Explorer must be enabled.	CM-7 a	3.4.1		CM.2.062			
63687	Caching of logon credentials must be limited.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63695	File Explorer shell protocol must run in protected mode.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63697	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			
63699	Users must not be allowed to ignore Windows Defender SmartScreen filter warnings for malicious websites in Microsoft Edge.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63701	Users must not be allowed to ignore Windows Defender SmartScreen filter warnings for unverified files in Microsoft Edge.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63703	The Windows SMB client must be configured to always perform SMB packet signing.	SC-8;SC-8 (1)	3.13.8			SC.3.185 SI.3.219		
63709	The password manager function in the Edge browser must be disabled.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63711	Unencrypted passwords must not be sent to third-party 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			
63713	The Windows Defender SmartScreen filter for Microsoft Edge must be enabled.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63717	The use of a hardware security device with Windows Hello for Business must be enabled.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63719	The Windows SMB server must be configured to always perform SMB packet signing.	SC-8;SC-8 (1)	3.13.8			SC.3.185 SI.3.219		
63721	Windows 10 must be configured to require a minimum pin length of six characters or greater.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63731	Local drives must be prevented from sharing with Remote Desktop Session Hosts.	SC-4	3.13.4			SC.3.182		

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
63737	The Remote Desktop Session Host must require secure RPC communications.	AC-17 (2)	AC.3.014			3.1.13		
63739	Anonymous SID/Name translation must not be allowed.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63741	Remote Desktop Services must be configured with the client connection encryption set to the required level.	AC-17 (2);MA-4 (6)	AC.3.014			3.1.13		
63743	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			
63745	Anonymous enumeration of SAM accounts must not be allowed.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63747	Basic authentication for RSS feeds over HTTP must not be used.	CM-7 a	3.4.1		CM.2.062			
63749	Anonymous enumeration of shares must be restricted.	SC-4	3.13.4			SC.3.182		
63751	Indexing of encrypted files must be turned off.	CM-7 a	3.4.1		CM.2.062			
63755	The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63759	Anonymous access to Named Pipes and Shares must be restricted.	SC-4	3.13.4			SC.3.182		
63765	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			
63767	PKU2U authentication using online identities must be prevented.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63797	The system 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			
63801	The LanMan 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			
63803	The system must be configured to the required LDAP client signing level.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63805	The system must be configured to meet the minimum session security requirement for NTLM SSP based clients.	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
63807	The system must be configured to meet the minimum session security requirement for NTLM SSP based servers.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63811	The system must be configured to use FIPS-compliant algorithms for encryption, hashing, and signing.	SC-13	3.13.11			SC.3.177		
63815	The default permissions of global system objects must be increased.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63839	Toast notifications to the lock screen must be turned off.	CM-7 a	3.4.1		CM.2.062			
63841	Zone information must be preserved when saving attachments.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
63843	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		
63845	The Access this computer from the network user right must only be assigned to the Administrators and Remote Desktop Users groups.	AC-3	3.1.1 3.1.2	AC.1.001 AC.1.002				
63847	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		
63851	The Allow log on locally user right must only be assigned to the Administrators and Users groups.	AC-3	3.1.1 3.1.2	AC.1.001 AC.1.002				
63853	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		
63855	The Change the system time user right must only be assigned to Administrators and Local Service and NT SERVICE\autotimesvc.	AC-6 (10)	3.1.7			AC.3.018		
63857	The Create a pagefile user right must only be assigned to the Administrators group.	AC-6 (10)	3.1.7			AC.3.018		
63859	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		
63861	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		
63863	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		
63865	The Create symbolic links user right must only be assigned to the Administrators group.	AC-6 (10)	3.1.7			AC.3.018		
63869	The Debug programs 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
63871	The Deny access to this computer from the network user right on workstations must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems and unauthenticated access on all systems.	AC-3	3.1.1 3.1.2	AC.1.001 AC.1.002				
63873	The Deny log on as a batch job user right on domain-joined workstations must be configured to prevent access from highly privileged domain accounts.	AC-3	3.1.1 3.1.2	AC.1.001 AC.1.002				
63875	The Deny log on as a service user right on Windows 10 domain-joined workstations must be configured to prevent access from highly privileged domain accounts.	AC-3	3.1.1 3.1.2	AC.1.001 AC.1.002				
63877	The Deny log on locally user right on workstations must be configured to prevent access from highly privileged domain accounts on domain systems and unauthenticated access on all systems.	AC-3	3.1.1 3.1.2	AC.1.001 AC.1.002				
63879	The Deny log on through Remote Desktop Services user right on Windows 10 workstations must at a minimum be configured to prevent access from highly privileged domain accounts and local accounts on domain systems and unauthenticated access on all systems.	AC-3;AC-17 (1)	3.1.12		AC.2.013			
63881	The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts.	AC-6 (10)	3.1.7			AC.3.018		
63883	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		
63889	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		
63917	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		
63925	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		
63927	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	AU.3.049		AU.5.055 IR.5.106
63931	The Modify firmware environment values 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
63933	The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	AC-6 (10)	3.1.7			AC.3.018		
63935	The Profile single process user right must only be assigned to the Administrators group.	AC-6 (10)	3.1.7			AC.3.018		
63939	The Restore files and directories user right must only be assigned to the Administrators group.	AC-6 (10)	3.1.7			AC.3.018		
63941	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		
65681	Windows Update must not obtain updates from other PCs on the Internet.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
70637	The Windows PowerShell 2.0 feature must be disabled on the system.	CM-7 a	3.4.1		CM.2.062			
70639	The Server Message Block (SMB) v1 protocol must be disabled on the system.	CM-7 a	3.4.1		CM.2.062			
71759	The system must be configured to audit Logon/Logoff - Account Lockout failures.	AU-12 c	3.3.1 3.3.2		AU.2.041 AU.2.042			AU.5.055 IR.5.106
71761	The system must be configured to audit Policy Change - Authorization Policy Change successes.	AU-12 c	3.3.1 3.3.2		AU.2.041 AU.2.042			AU.5.055 IR.5.106
71763	WDigest Authentication must be disabled.	CM-7 a	3.4.1		CM.2.062			
71765	Internet connection sharing must be disabled.	CM-7 a	3.4.1		CM.2.062			
71769	Remote calls to the Security Account Manager (SAM) must be restricted to Administrators.	AC-6 (10)	3.1.7			AC.3.018		
71771	Microsoft consumer experiences must be turned off.	CM-7 a	3.4.1		CM.2.062			
72329	Run as different user must be removed from context menus.	CM-7 a	3.4.1		CM.2.062			
72765	Bluetooth must be turned off unless approved by the organization.	CM-7 a	3.4.1		CM.2.062			
72767	Bluetooth must be turned off when not in use.	CM-7 a	3.4.1		CM.2.062			
72769	The system must notify the user when a Bluetooth device attempts to connect.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
74409	Windows 10 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
74411	Windows 10 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
74417	Windows 10 must be configured to disable Windows Game Recording and Broadcasting.	CM-7 a	3.4.1		CM.2.062			

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
74699	Windows 10 must be configured to enable Remote host allows delegation of non-exportable credentials.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
74719	The Secondary Logon service must be disabled on Windows 10.	CM-7 a	3.4.1		CM.2.062			
74721	Windows 10 must be configured to audit Object Access - File Share successes.	AU-12 c	3.3.1 3.3.2		AU.2.041 AU.2.042			AU.5.055 IR.5.106
74723	The Server Message Block (SMB) v1 protocol must be disabled on the SMB server.	CM-7 a	3.4.1		CM.2.062			
74725	The Server Message Block (SMB) v1 protocol must be disabled on the SMB client.	CM-7 a	3.4.1		CM.2.062			
75027	Windows 10 must be configured to audit Object Access - File Share failures.	AU-12 c	3.3.1 3.3.2		AU.2.041 AU.2.042			AU.5.055 IR.5.106
76505	Orphaned security identifiers (SIDs) must be removed from user rights on Windows 10.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
77083	Windows 10 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			
77085	Secure Boot must be enabled on Windows 10 systems.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
77091	Windows 10 Exploit Protection system-level mitigation, Data Execution Prevention (DEP), must be on.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
77097	Windows 10 Exploit Protection system-level mitigation, Control flow guard (CFG), must be on.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
77101	Windows 10 Exploit Protection system-level mitigation, Validate exception chains (SEHOP), must be on.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
77103	Windows 10 Exploit Protection system-level mitigation, Validate heap integrity, must be on.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
77189	Exploit Protection mitigations in Windows 10 must be configured for Acrobat.exe.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
77191	Exploit Protection mitigations in Windows 10 must be configured for AcroRd32.exe.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
77195	Exploit Protection mitigations in Windows 10 must be configured for chrome.exe.	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
77201	Exploit Protection mitigations in Windows 10 must be configured for EXCEL.EXE.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
77205	Exploit Protection mitigations in Windows 10 must be configured for firefox.exe.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
77209	Exploit Protection mitigations in Windows 10 must be configured for FLTLDR.EXE.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
77213	Exploit Protection mitigations in Windows 10 must be configured for GROOVE.EXE.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
77217	Exploit Protection mitigations in Windows 10 must be configured for iexplore.exe.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
77221	Exploit Protection mitigations in Windows 10 must be configured for INFOPATH.EXE.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
77223	Exploit Protection mitigations in Windows 10 must be configured for java.exe, javaw.exe, and javaws.exe.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
77227	Exploit Protection mitigations in Windows 10 must be configured for lync.exe.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
77231	Exploit Protection mitigations in Windows 10 must be configured for MSACCESS.EXE.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
77233	Exploit Protection mitigations in Windows 10 must be configured for MSPUB.EXE.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
77235	Exploit Protection mitigations in Windows 10 must be configured for OneDrive.exe.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
77239	Exploit Protection mitigations in Windows 10 must be configured for OIS.EXE.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
77243	Exploit Protection mitigations in Windows 10 must be configured for OUTLOOK.EXE.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
77245	Exploit Protection mitigations in Windows 10 must be configured for plugin-container.exe.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
77247	Exploit Protection mitigations in Windows 10 must be configured for POWERPNT.EXE.	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
77249	Exploit Protection mitigations in Windows 10 must be configured for PPTVIEW.EXE.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
77255	Exploit Protection mitigations in Windows 10 must be configured for VISIO.EXE.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
77259	Exploit Protection mitigations in Windows 10 must be configured for VPREVIEW.EXE.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
77263	Exploit Protection mitigations in Windows 10 must be configured for WINWORD.EXE.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
77267	Exploit Protection mitigations in Windows 10 must be configured for wmplayer.exe.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
77269	Exploit Protection mitigations in Windows 10 must be configured for wordpad.exe.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
78129	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			
82137	The use of personal accounts for OneDrive synchronization must be disabled.	CM-7 a	3.4.1		CM.2.062			
82139	Windows 10 must be configured to prevent certificate error overrides in Microsoft Edge.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
82145	If Enhanced diagnostic data is enabled it must be limited to the minimum required to support Windows Analytics.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
88203	OneDrive must only allow synchronizing of accounts for DoD organization instances.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
94719	Windows 10 must be configured to prevent Windows apps from being activated by voice while the system is locked.	AC-11 b	3.1.10		AC.2.010			
94859	Windows 10 systems must use a BitLocker PIN for pre-boot authentication.	SC-28;SC-28 (1)	3.13.16			SC.3.191		
94861	Windows 10 systems must use a BitLocker PIN with a minimum length of 6 digits for pre-boot authentication.	SC-28;SC-28 (1)	3.13.16			SC.3.191		

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
99555	Passwords for enabled local Administrator accounts 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			
99557	Windows 10 Kernel (Direct Memory Access) DMA Protection must be enabled.	SC-4	3.13.4			SC.3.182		
99559	The convenience PIN for Windows 10 must be disabled.	CM-7 a	3.4.1		CM.2.062			
99561	Windows Ink Workspace configured but disallow access above the lock.	CM-7 a	3.4.1		CM.2.062			
99563	Windows 10 should be configured to prevent users from receiving suggestions for third-party or additional applications.	CM-7 a	3.4.1		CM.2.062			
100093	Windows 10 must cover or disable the built-in or attached camera when not in use.	CM-7 a	3.4.1		CM.2.062			
102611	Windows 10 non-persistent VM sessions should not exceed 24 hours.	SC-28	3.13.16			SC.3.191		
102617	The Windows Explorer Preview pane must be disabled for Windows 10.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
102627	Windows 10 must use multifactor authentication for local and network access to privileged and non-privileged accounts.	IA-2 (1);IA-2 (2);IA-2 (3);IA-2 (4)	3.5.3			IA.3.083		
63321	Users must be prevented from changing installation options.	CM-11 (2)						
63325	The Windows Installer Always install with elevated privileges must be disabled.	CM-11 (2)						
63339	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	MA-4 (6)						
63343	Windows 10 must employ automated mechanisms to determine the state of system components with regard to flaw remediation using the following frequency: continuously, where 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)						
63369	The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	MA-4 (6)						
63375	The Windows Remote Management (WinRM) service must not store RunAs credentials.	IA-11						

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
63519	The Application event log size must be configured to 32768 KB or greater.	AU-4						
63523	The Security event log size must be configured to 1024000 KB or greater.	AU-4						
63527	The System event log size must be configured to 32768 KB or greater.	AU-4						
63567	The system must be configured to ignore NetBIOS name release requests except from WINS servers.	SC-5						
63579	The DoD Root CA certificates must be installed in the Trusted Root Store.	IA-5 (2) (a);SC-23 (5)						
63583	The External Root CA certificates must be installed in the Trusted Root Store on unclassified systems.	IA-5 (2) (a)						
63587	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)						
63589	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)						
63597	Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	SC-3						
63611	The built-in guest account must be disabled.	IA-8						
63645	Users must be prompted for a password on resume from sleep (on battery).	IA-11						
63649	The user must be prompted for a password on resume from sleep (plugged in).	IA-11						
63657	Unauthenticated RPC clients must be restricted from connecting to the RPC server.	IA-3 (1)						
63679	Administrator accounts must not be enumerated during elevation.	SC-3						
63689	Explorer Data Execution Prevention must be enabled.	SI-16						
63691	Turning off File Explorer heap termination on corruption must be disabled.	SC-5						
63729	Passwords must not be saved in the Remote Desktop Client.	IA-11						

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
63733	Remote Desktop Services must always prompt a client for passwords upon connection.	IA-11						
63795	Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.	IA-7						
63817	User Account Control approval mode for the built-in Administrator must be enabled.	IA-11						
63819	User Account Control must, at minimum, prompt administrators for consent on the secure desktop.	SC-3						
63821	User Account Control must automatically deny elevation requests for standard users.	IA-11						
63825	User Account Control must be configured to detect application installations and prompt for elevation.	SC-3						
63827	User Account Control must only elevate UIAccess applications that are installed in secure locations.	SC-3						
63829	User Account Control must run all administrators in Admin Approval Mode, enabling UAC.	IA-11						
63831	User Account Control must virtualize file and registry write failures to per-user locations.	SC-3						
68817	Command line data must be included in process creation events.	AU-3 (1)						
68819	PowerShell script block logging must be enabled on Windows 10.	AU-3 (1)						
68845	Data Execution Prevention (DEP) must be configured to at least OptOut.	SI-16						
68849	Structured Exception Handling Overwrite Protection (SEHOP) must be enabled.	SI-16						
74413	Windows 10 must be configured to prioritize ECC Curves with longer key lengths first.	IA-7						
77095	Windows 10 Exploit Protection system-level mitigation, Randomize memory allocations (Bottom-Up ASLR), must be on.	SI-16						
99541	Windows 10 must be configured to audit other Logon/Logoff Events Failures.	AU-3						
99543	Windows 10 must be configured to audit other Logon/Logoff Events Successes.	AU-3						
99545	Windows 10 must be configured to audit Detailed File Share Failures.	AU-3						
99547	Windows 10 must be configured to audit MPSSVC Rule-Level Policy Change Successes.	AU-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
99549	Windows 10 must be configured to audit MPSSVC Rule-Level Policy Change Failures.	AU-3						
99551	Windows 10 must be configured to audit Other Policy Change Events Successes.	AU-3						
99553	Windows 10 must be configured to audit Other Policy Change Events Failures.	AU-3						

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	AU.2.041 AU.2.042			AU.5.055 IR.5.106	AC-2 (4);AC-6 (9);AU-12 c	3.1.7 3.3.1 3.3.2	**63447**
AC.1.001 AC.1.002					AC-3	3.1.1 3.1.2	**63353**
AC.1.001 AC.1.002					AC-3 (4)	3.1.1 3.1.2	**63373**
AC.1.001 AC.1.002					AC-3	3.1.1 3.1.2	**63845**
AC.1.001 AC.1.002					AC-3	3.1.1 3.1.2	**63851**
AC.1.001 AC.1.002					AC-3	3.1.1 3.1.2	**63871**
AC.1.001 AC.1.002					AC-3	3.1.1 3.1.2	**63873**
AC.1.001 AC.1.002					AC-3	3.1.1 3.1.2	**63875**
AC.1.001 AC.1.002					AC-3	3.1.1 3.1.2	**63877**
IA.1.076 IA.1.077					IA-2	3.5.1 3.5.2	**63601**
	AC.2.005				AC-8 a;AC-8 b;AC-8 c 1;AC-8 c 2;AC-8 c 3	3.1.9	**63675**
	AC.2.005				AC-8 a;AC-8 c 1;AC-8 c 2;AC-8 c 3	3.1.9	**63681**
	AC.2.009				AC-7 b	3.1.8	**63405**
	AC.2.009				AC-7 a	3.1.8	**63409**
	AC.2.009				AC-7 a;AC-7 b	3.1.8	**63413**
	AC.2.010				AC-11 a	3.1.10	**63669**

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.2.010				AC-11 b	3.1.10	**94719**
	AC.2.013				AC-3;AC-17 (1)	3.1.12	**63879**
	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	**63459**
	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	**63463**
	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	**63467**
	AC.2.013 AU.2.041 AU.2.042			AU.5.055 IR.5.106	AU-12 c	3.3.1 3.3.2	**63469**
	AC.2.013 AU.2.041 AU.2.042			AU.5.055 IR.5.106	AU-12 c	3.3.1 3.3.2	**63471**
	AC.2.013 AU.2.041 AU.2.042			AU.5.055 IR.5.106	AU-12 c	3.3.1 3.3.2	**63473**
	AC.2.013 AU.2.041 AU.2.042			AU.5.055 IR.5.106	AU-12 c	3.3.1 3.3.2	**63479**
	AC.2.013 AU.2.041 AU.2.042			AU.5.055 IR.5.106	AC-6 (9);AU-12 c	3.1.7 3.3.1 3.3.2	**63481**
	AC.2.013 AU.2.041 AU.2.042			AU.5.055 IR.5.106	AC-6 (9);AU-12 c	3.1.7 3.3.1 3.3.2	**63483**

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.2.013 AU.2.041 AU.2.042			AU.5.055 IR.5.106	AC-6 (9);AU-12 c	3.1.7 3.3.1 3.3.2	**63487**
	AC.2.013 AU.2.041 AU.2.042			AU.5.055 IR.5.106	AU-12 c	3.3.1 3.3.2	**63491**
	AC.2.013 AU.2.041 AU.2.042			AU.5.055 IR.5.106	AU-12 c	3.3.1 3.3.2	**63499**
	AC.2.013 AU.2.041 AU.2.042			AU.5.055 IR.5.106	AU-12 c	3.3.1 3.3.2	**63503**
	AC.2.013 AU.2.041 AU.2.042			AU.5.055 IR.5.106	AC-6 (9);AU-12 c	3.1.7 3.3.1 3.3.2	**63507**
	AC.2.013 AU.2.041 AU.2.042			AU.5.055 IR.5.106	AC-6 (9);AU-12 c	3.1.7 3.3.1 3.3.2	**63513**
	AC.2.013 AU.2.041 AU.2.042			AU.5.055 IR.5.106	AC-6 (9);AU-12 c	3.1.7 3.3.1 3.3.2	**63515**
	AC.2.013 AU.2.041 AU.2.042			AU.5.055 IR.5.106	AC-6 (9);AU-12 c	3.1.7 3.3.1 3.3.2	**63517**
	AU.2.041 AU.2.042	AU.3.049		AU.5.055 IR.5.106	AU-9;AU-12 b;AU-12 (3)	3.3.1 3.3.2 3.3.8	**63927**
	AU.2.041 AU.2.042	AC.3.018		AU.5.055 IR.5.106	AC-2 (4);AC-6 (9);AU-12 c	3.1.7 3.3.1 3.3.2	**63445**

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-2 (4);AC-6 (9);AU-12 c	3.1.7 3.3.1 3.3.2	**63449**
	AU.2.041 AU.2.042			AU.5.055 IR.5.106	AU-12 c	3.3.1 3.3.2	**63451**
	AU.2.041 AU.2.042			AU.5.055 IR.5.106	AU-12 c	3.3.1 3.3.2	**63453**
	AU.2.041 AU.2.042			AU.5.055 IR.5.106	AU-12 c	3.3.1 3.3.2	**63457**
	AU.2.041 AU.2.042			AU.5.055 IR.5.106	AU-12 c	3.3.1 3.3.2	**71759**
	AU.2.041 AU.2.042			AU.5.055 IR.5.106	AU-12 c	3.3.1 3.3.2	**71761**
	AU.2.041 AU.2.042			AU.5.055 IR.5.106	AU-12 c	3.3.1 3.3.2	**74409**
	AU.2.041 AU.2.042			AU.5.055 IR.5.106	AU-12 c	3.3.1 3.3.2	**74411**
	AU.2.041 AU.2.042			AU.5.055 IR.5.106	AU-12 c	3.3.1 3.3.2	**74721**
	AU.2.041 AU.2.042			AU.5.055 IR.5.106	AU-12 c	3.3.1 3.3.2	**75027**
	AU.2.041 AU.2.042			AU.5.055 IR.5.106	AU-12 c	3.3.1 3.3.2	**63431**
	AU.2.041 AU.2.042			AU.5.055 IR.5.106	AU-12 c	3.3.1 3.3.2	**63435**
	AU.2.041 AU.2.042 IR.2.097			AU.5.055 IR.5.106	AU-12 a	3.3.1 3.3.2	**63635**

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	**63319**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63323**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63329**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63333**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63349**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63351**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63355**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63363**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63367**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63393**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63399**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63403**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63555**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63559**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63563**

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	**63569**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63577**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63581**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63585**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63591**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63595**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63599**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63607**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63609**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63617**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63619**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63625**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63627**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63653**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63659**

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	**63661**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63677**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63683**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63687**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63695**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63697**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63699**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63701**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63709**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63713**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63717**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63721**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63739**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63743**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63745**

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	**63755**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63765**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63767**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63801**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63803**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63805**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63807**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63815**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**63841**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**65681**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72769**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**74699**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**76505**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**77083**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**77085**

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	**77091**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**77097**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**77101**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**77103**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**77189**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**77191**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**77195**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**77201**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**77205**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**77209**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**77213**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**77217**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**77221**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**77223**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**77227**

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	**77231**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**77233**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**77235**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**77239**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**77243**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**77245**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**77247**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**77249**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**77255**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**77259**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**77263**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**77267**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**77269**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**78129**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**82139**

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	**82145**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**88203**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**102617**
	CM.2.062				CM-7 a	3.4.1	**63365**
	CM.2.062				CM-7 a	3.4.1	**63377**
	CM.2.062				CM-7 b	3.4.1	**63381**
	CM.2.062				CM-7 a	3.4.1	**63383**
	CM.2.062				CM-7 b	3.4.1	**63385**
	CM.2.062				CM-7 b	3.4.1	**63389**
	CM.2.062				CM-7 a	3.4.1	**63545**
	CM.2.062				CM-7 a	3.4.1	**63549**
	CM.2.062				CM-7 a	3.4.1	**63615**
	CM.2.062				CM-7 a	3.4.1	**63621**
	CM.2.062				CM-7 a	3.4.1	**63623**
	CM.2.062				CM-7 a	3.4.1	**63629**
	CM.2.062				CM-7 a	3.4.1	**63633**
	CM.2.062				CM-7 a	3.4.1	**63663**
	CM.2.062				CM-7 a	3.4.1	**63685**
	CM.2.062				CM-7 a	3.4.1	**63747**
	CM.2.062				CM-7 a	3.4.1	**63751**
	CM.2.062				CM-7 a	3.4.1	**63839**
	CM.2.062				CM-7 a	3.4.1	**70637**
	CM.2.062				CM-7 a	3.4.1	**70639**
	CM.2.062				CM-7 a	3.4.1	**71763**
	CM.2.062				CM-7 a	3.4.1	**71765**
	CM.2.062				CM-7 a	3.4.1	**71771**
	CM.2.062				CM-7 a	3.4.1	**72329**
	CM.2.062				CM-7 a	3.4.1	**72765**

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.2.062				CM-7 a	3.4.1	**72767**
	CM.2.062				CM-7 a	3.4.1	**74417**
	CM.2.062				CM-7 a	3.4.1	**74719**
	CM.2.062				CM-7 a	3.4.1	**74723**
	CM.2.062				CM-7 a	3.4.1	**74725**
	CM.2.062				CM-7 a	3.4.1	**82137**
	CM.2.062				CM-7 a	3.4.1	**99559**
	CM.2.062				CM-7 a	3.4.1	**99561**
	CM.2.062				CM-7 a	3.4.1	**99563**
	CM.2.062				CM-7 a	3.4.1	**100093**
	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	**63371**
	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	**63415**
	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	**63419**
	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	**63421**
	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	**63423**

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-5 (1) (a)	3.5.7	**63427**
	IA.2.079					3.5.8	
	IA.2.080					3.5.9	
	IA.2.081					3.5.10	
	IA.2.078				IA-5 (1) (c)	3.5.7	**63429**
	IA.2.079					3.5.8	
	IA.2.080					3.5.9	
	IA.2.081					3.5.10	
	IA.2.078				IA-5 (1) (c)	3.5.7	**63711**
	IA.2.079					3.5.8	
	IA.2.080					3.5.9	
	IA.2.081					3.5.10	
	IA.2.078				IA-5 (1) (c)	3.5.7	**63797**
	IA.2.079					3.5.8	
	IA.2.080					3.5.9	
	IA.2.081					3.5.10	
	IA.2.078				IA-5 (1) (d)	3.5.7	**99555**
	IA.2.079					3.5.8	
	IA.2.080					3.5.9	
	IA.2.081					3.5.10	
	MA.2.113				MA-4 c	3.7.5	**63335**
	MA.2.113				MA-4 c	3.7.5	**63341**
	MA.2.113				MA-4 c	3.7.5	**63347**
		AC.3.018			AC-6 (10)	3.1.7	**63361**
		AC.3.018			AC-6 (10)	3.1.7	**63593**
		AC.3.018			AC-6 (10)	3.1.7	**63843**
		AC.3.018			AC-6 (10)	3.1.7	**63847**
		AC.3.018			AC-6 (10)	3.1.7	**63853**
		AC.3.018			AC-6 (10)	3.1.7	**63855**
		AC.3.018			AC-6 (10)	3.1.7	**63857**
		AC.3.018			AC-6 (10)	3.1.7	**63859**

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	**63861**
		AC.3.018			AC-6 (10)	3.1.7	**63863**
		AC.3.018			AC-6 (10)	3.1.7	**63865**
		AC.3.018			AC-6 (10)	3.1.7	**63869**
		AC.3.018			AC-6 (10)	3.1.7	**63881**
		AC.3.018			AC-6 (10)	3.1.7	**63883**
		AC.3.018			AC-6 (10)	3.1.7	**63889**
		AC.3.018			AC-6 (10)	3.1.7	**63917**
		AC.3.018			AC-6 (10)	3.1.7	**63925**
		AC.3.018			AC-6 (10)	3.1.7	**63931**
		AC.3.018			AC-6 (10)	3.1.7	**63933**
		AC.3.018			AC-6 (10)	3.1.7	**63935**
		AC.3.018			AC-6 (10)	3.1.7	**63939**
		AC.3.018			AC-6 (10)	3.1.7	**63941**
		AC.3.018			AC-6 (10)	3.1.7	**71769**
		AC.3.014			AC-17 (2)	AC.3.014	**63737**
		AC.3.014			AC-17 (2);MA-4 (6)	AC.3.014	**63741**
		AU.3.049			AU-9	3.3.8	**63533**
		AU.3.049			AU-9	3.3.8	**63537**
		AU.3.049			AU-9	3.3.8	**63541**
		CM.3.068			CM-7 (2)	3.4.7	**63667**
		CM.3.068			CM-7 (2)	3.4.7	**63671**
		CM.3.068			CM-7 (2)	3.4.7	**63673**
		CM.3.069	CM.4.073		CM-7 (5) (b)	3.4.8	**63345**
		IA.3.083			IA-2 (1);IA-2 (2);IA-2 (3);IA-2 (4)	3.5.3	**102627**
		IA.3.085 IA.3.086			IA-4 e	3.5.5 3.5.6	**63359**

CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5	800-53 Rev 4	800-171	STIG V-ID
		SC.3.177			SC-13	3.13.11	**63811**
		SC.3.182			SC-4	3.13.4	**63357**
		SC.3.182			SC-4	3.13.4	**63651**
		SC.3.182			SC-4	3.13.4	**63731**
		SC.3.182			SC-4	3.13.4	**63749**
		SC.3.182			SC-4	3.13.4	**63759**
		SC.3.182			SC-4	3.13.4	**99557**
		SC.3.185 SI.3.219			SC-8;SC-8 (1)	3.13.8	**63639**
		SC.3.185 SI.3.219			SC-8;SC-8 (1)	3.13.8	**63643**
		SC.3.185 SI.3.219			SC-8;SC-8 (1)	3.13.8	**63647**
		SC.3.185 SI.3.219			SC-8;SC-8 (1)	3.13.8	**63665**
		SC.3.185 SI.3.219			SC-8;SC-8 (1)	3.13.8	**63703**
		SC.3.185 SI.3.219			SC-8;SC-8 (1)	3.13.8	**63719**
		SC.3.191			SC-28;SC-28 (1)	3.13.16	**63337**
		SC.3.191			SC-28;SC-28 (1)	3.13.16	**94859**
		SC.3.191			SC-28;SC-28 (1)	3.13.16	**94861**
		SC.3.191			SC-28	3.13.16	**102611**
					CM-11 (2)		**63321**
					CM-11 (2)		**63325**
					MA-4 (6)		**63339**
					SI-2 (2)		**63343**
					MA-4 (6)		**63369**
					IA-11		**63375**
					AU-4		**63519**
					AU-4		**63523**

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-4		**63527**
					SC-5		**63567**
					IA-5 (2) (a);SC-23 (5)		**63579**
					IA-5 (2) (a)		**63583**
					IA-5 (2) (a);SC-23 (5)		**63587**
					IA-5 (2) (a);SC-23 (5)		**63589**
					SC-3		**63597**
					IA-8		**63611**
					IA-11		**63645**
					IA-11		**63649**
					IA-3 (1)		**63657**
					SC-3		**63679**
					SI-16		**63689**
					SC-5		**63691**
					IA-11		**63729**
					IA-11		**63733**
					IA-7		**63795**
					IA-11		**63817**
					SC-3		**63819**
					IA-11		**63821**
					SC-3		**63825**
					SC-3		**63827**
					IA-11		**63829**
					SC-3		**63831**
					AU-3 (1)		**68817**
					AU-3 (1)		**68819**
					SI-16		**68845**
					SI-16		**68849**

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-7		**74413**
					SI-16		**77095**
					AU-3		**99541**
					AU-3		**99543**
					AU-3		**99545**
					AU-3		**99547**
					AU-3		**99549**
					AU-3		**99551**
					AU-3		**99553**

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.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		
	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		

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
	AC.4.023		CMMC mod of Draft NIST SP 800-171B 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.4.032				Restrict remote network access based on organizationally defined risk factors such as time of day, location, network connection, and measured properties of the current user and role.				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			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.1.016	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		CMMC mod of Draft NIST SP 800-171B 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			
	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

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
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, mod, 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				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		CMMC mod of Draft NIST SP 800-171B 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	
C012 Conduct training	AT.2.057	3.2.2		4 AT-2, AT-3	Ensure that personnel are trained to carry out their assigned information security related duties and responsibilities.		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
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	CMMC mod of NIST SP 800-171 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		CMMC mod of Draft NIST SP 800-171B 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
IDENTIFICATION AND AUTHENTICATION (IA)										
C015 Grant access to	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				

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
authenticated entities	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		

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
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 predefined procedures.		X			
	IR.3.098			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		CMMC mod of Draft NIST SP 800-171B 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		CMMC mod of NIST 800-171B 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

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
MAINTENANCE (MA)										
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.3.122	3.8.4		MP-3	Mark media with necessary CUI markings and distribution limitations.			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

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
RISK MANAGEMENT (RM)										
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			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		CMMC mod of Draft NIST SP 800-171B 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

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
C033 Manage supply chain risk			CMMC mod of Draft NIST SP 800-171B 3.11.7e	SA-12	Develop and update as required, a plan for managing supply chain risks associated with the IT supply chain.				X	
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.4.1.64		CMMC mod of Draft NIST SP 800-171B 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	

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
	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)										
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		

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
	SC.4.197		CMMC mod of Draft NIST SP 800-171B 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	
	SC.4.228	CMMC mod of NIST SP 800-171 Rev 1 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

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
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			
	SI.4.221		Draft NIST SP 800-171B 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	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		