Get Compliant. Stay Compliant.

STIG & CMMC Control Matrix

for Red Hat 7

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

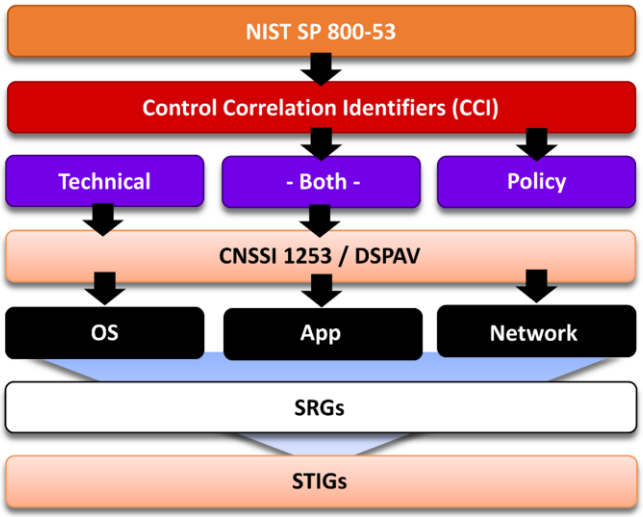
SteelCloud has spent the last decade developing patented technology to automate government policy compliance, configuration control, and cloud security. Our ConfigOS software solution was designed to reduce initial hardening time by 90% and ongoing STIG compliance effort by more than 70%. Our technology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

Red Hat 7

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
71849	The Red Hat Enterprise Linux operating system must be configured so that the file permissions, ownership, and group membership of system files and commands match the vendor values.	AC-3 (4); AC-6 (10); AU-9; AU-9 (3)	3.17 3.3.8			AC.3.017 AU.3.049		
71859	The Red Hat Enterprise Linux operating system must display the Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system via a graphical user logon.	AC-8 a	3.1.9		AC.2.005			
71861	The Red Hat Enterprise Linux operating system must display the approved Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system via a graphical user logon.	AC-8 a	3.1.9		AC.2.005			
71863	The Red Hat Enterprise Linux operating system must display the Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system via a command line user logon.	AC-8 a	3.1.9		AC.2.005			
71891	The Red Hat Enterprise Linux operating system must enable a user session lock until that user re-establishes access using established identification and authentication procedures.	AC-11 b	3.1.17		AC.2.010			
71893	The Red Hat Enterprise Linux operating system must initiate a screensaver after a 15-minute period of inactivity for graphical user interfaces.	AC-11 a	3.1.17		AC.2.010			
71897	The Red Hat Enterprise Linux operating system must have the screen package installed.	AC-11 a	3.1.17		AC.2.010			
71899	The Red Hat Enterprise Linux operating system must initiate a session lock for the screensaver after a period of inactivity for graphical user interfaces.	AC-11 a	3.1.17		AC.2.010			
71901	The Red Hat Enterprise Linux operating system must initiate a session lock for graphical user interfaces when the screensaver is activated.	AC-11 a	3.1.17		AC.2.010			
71903	The Red Hat Enterprise Linux operating system must be configured so that when passwords are changed or new passwords are established, the new password must contain at least one upper-case character.	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			

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
71905	The Red Hat Enterprise Linux operating system must be configured so that when passwords are changed or new passwords are established, the new password must contain at least one lower-case character.	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			
71907	The Red Hat Enterprise Linux operating system must be configured so that when passwords are changed or new passwords are assigned, the new password must contain at least one numeric character.	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			
71909	The Red Hat Enterprise Linux operating system must be configured so that when passwords are changed or new passwords are established, the new password must contain at least one special character.	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			
71911	The Red Hat Enterprise Linux operating system must be configured so that when passwords are changed a minimum of eight of the total number of characters must be changed.	IA-5 (1) (b)	3.5.7 3.5.8 3.5.9 3.5.10		IA.2.078 IA.2.079 IA.2.080 IA.2.081			
71913	The Red Hat Enterprise Linux operating system must be configured so that when passwords are changed a minimum of four character classes must be changed.	IA-5 (1) (b)	3.5.7 3.5.8 3.5.9 3.5.10		IA.2.078 IA.2.079 IA.2.080 IA.2.081			
71915	The Red Hat Enterprise Linux operating system must be configured so that when passwords are changed the number of repeating consecutive characters must not be more than three characters.	IA-5 (1) (b)	3.5.7 3.5.8 3.5.9 3.5.10		IA.2.078 IA.2.079 IA.2.080 IA.2.081			
71917	The Red Hat Enterprise Linux operating system must be configured so that when passwords are changed the number of repeating characters of the same character class must not be more than four characters.	IA-5 (1) (b)	3.5.7 3.5.8 3.5.9 3.5.10		IA.2.078 IA.2.079 IA.2.080 IA.2.081			

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
71919	The Red Hat Enterprise Linux operating system must be configured so that the PAM system service is configured to store only encrypted representations 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			
71921	The Red Hat Enterprise Linux operating system must be configured to use the shadow file to store only encrypted representations 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			
71923	The Red Hat Enterprise Linux operating system must be configured so that user and group account administration utilities are configured to store only encrypted representations 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			
71925	The Red Hat Enterprise Linux operating system must be configured so that passwords for new users are restricted to a 24 hours/1 day minimum lifetime.	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			
71927	The Red Hat Enterprise Linux operating system must be configured so that passwords are restricted to a 24 hours/1 day minimum lifetime.	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			
71929	The Red Hat Enterprise Linux operating system must be configured so that passwords for new users are restricted to a 60-day maximum lifetime.	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			
71931	The Red Hat Enterprise Linux operating system must be configured so that existing passwords are restricted to a 60-day maximum lifetime.	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			

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
71933	The Red Hat Enterprise Linux operating system must be configured so that passwords are prohibited from reuse for a minimum of five generations.	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			
71935	The Red Hat Enterprise Linux operating system must be configured so that passwords are a minimum of 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			
71937	The Red Hat Enterprise Linux operating system must not have accounts configured with blank or null passwords.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
71939	The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon does not allow authentication using an empty password.	IA-2 (2)	3.5.3			IA.3.083		
71941	The Red Hat Enterprise Linux operating system must disable account identifiers (individuals, groups, roles, and devices) if the password expires.	IA-4 e	3.5.5 3.5.6			IA.3.085 IA.3.086		
71943	The Red Hat Enterprise Linux operating system must be configured to lock accounts for a minimum of 15 minutes after three unsuccessful logon attempts within a 15-minute timeframe.	AC-7 a; AC-7 b	3.1.8		AC.2.009			
71945	The Red Hat Enterprise Linux operating system must lock the associated account after three unsuccessful root logon attempts are made within a 15-minute period.	AC-7 b	3.1.8		AC.2.009			
71951	The Red Hat Enterprise Linux operating system must be configured so that the delay between logon prompts following a failed console logon attempt is at least four seconds.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
71953	The Red Hat Enterprise Linux operating system must not allow an unattended or automatic logon to the system via a graphical user interface.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
71955	The Red Hat Enterprise Linux operating system must not allow an unrestricted logon to the system.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
71957	The Red Hat Enterprise Linux operating system must not allow users to override SSH environment variables.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
71959	The Red Hat Enterprise Linux operating system must not allow a non-certificate trusted host SSH logon to the system.	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
71961	Red Hat Enterprise Linux operating systems prior to version 7.2 with a Basic Input/Output System (BIOS) must require authentication upon booting into single-user and maintenance modes.	AC-3	3.1.1 3.1.2	AC.1.001 AC.1.002		AC.3.018		
71963	Red Hat Enterprise Linux operating systems prior to version 7.2 using Unified Extensible Firmware Interface (UEFI) must require authentication upon booting into single-user and maintenance modes.	AC-3	3.1.1 3.1.2	AC.1.001 AC.1.002				
71965	The Red Hat Enterprise Linux operating system must uniquely identify and must authenticate organizational users (or processes acting on behalf of organizational users) using multifactor authentication.	IA-2 (2)	3.5.3			IA.3.083		
71967	The Red Hat Enterprise Linux operating system must not have the rsh-server package installed.	CM-7 a	3.4.7			CM.3068		
71969	The Red Hat Enterprise Linux operating system must not have the ypserv package installed.	CM-7 a	3.4.7			CM.3068		
71971	The Red Hat Enterprise Linux operating system must prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.	AC-3 (4); AC-6 (10)	3.1.7			AC.3.018		
71983	The Red Hat Enterprise Linux operating system must be configured to disable USB mass storage.	CM-6 b; IA-3	3.4.1 3.4.2 3.5.1 3.5.2	IA.1.076 IA.1.077	CM.2.061 CM.2.064			
71985	The Red Hat Enterprise Linux operating system must disable the file system automounter unless required.	CM-6 b; IA-3	3.4.1 3.4.2 3.5.1 3.5.2	IA.1.076 IA.1.077	CM.2.061 CM.2.064			
71993	The Red Hat Enterprise Linux operating system must be configured so that the x86 Ctrl-Alt-Delete key sequence is disabled on the command line.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
71995	The Red Hat Enterprise Linux operating system must define default permissions for all authenticated users in such a way that the user can only read and modify their own files.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
71997	The Red Hat Enterprise Linux operating system must be a vendor supported release.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
71999	The Red Hat Enterprise Linux operating system security patches and updates must be installed and up to date.	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
72001	The Red Hat Enterprise Linux operating system must not have unnecessary accounts.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72003	The Red Hat Enterprise Linux operating system must be configured so that all Group Identifiers (GIDs) referenced in the /etc/passwd file are defined in the /etc/group file.	IA-2	3.5.1 3.5.2	IA.1.076 IA.1.077				
72005	The Red Hat Enterprise Linux operating system must be configured so that the root account must be the only account having unrestricted access to the system.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72011	The Red Hat Enterprise Linux operating system must be configured so that all local interactive users have a home directory assigned in the /etc/passwd file.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72013	The Red Hat Enterprise Linux operating system must be configured so that all local interactive user accounts, upon creation, are assigned a home directory.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72015	The Red Hat Enterprise Linux operating system must be configured so that all local interactive user home directories are defined in the /etc/passwd file.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72017	The Red Hat Enterprise Linux operating system must be configured so that all local interactive user home directories have mode 0750 or less permissive.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72019	The Red Hat Enterprise Linux operating system must be configured so that all local interactive user home directories are owned by their respective users.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72021	The Red Hat Enterprise Linux operating system must be configured so that all local interactive user home directories are group-owned by the home directory owners primary group.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72023	The Red Hat Enterprise Linux operating system must be configured so that all files and directories contained in local interactive user home directories are owned by the owner of the home directory.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72025	The Red Hat Enterprise Linux operating system must be configured so that all files and directories contained in local interactive user home directories are group-owned by a group of which the home directory owner is a member.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72027	The Red Hat Enterprise Linux operating system must be configured so that all files and directories contained in local interactive user home directories have a mode of 0750 or less permissive.	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
72029	The Red Hat Enterprise Linux operating system must be configured so that all local initialization files for interactive users are owned by the home directory user or root.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72031	The Red Hat Enterprise Linux operating system must be configured so that all local initialization files for local interactive users are be group-owned by the users primary group or root.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72033	The Red Hat Enterprise Linux operating system must be configured so that all local initialization files have mode 0740 or less permissive.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72035	The Red Hat Enterprise Linux operating system must be configured so that all local interactive user initialization files executable search paths contain only paths that resolve to the users home directory.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72037	The Red Hat Enterprise Linux operating system must be configured so that local initialization files do not execute world-writable programs.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72039	The Red Hat Enterprise Linux operating system must be configured so that all system device files are correctly labeled to prevent unauthorized modification.	CM-3 f; CM-5 (1); CM-6 c; CM-11 (2)	3.4.3 3.4.1 3.4.2		CM.2.065 CM.2.061 CM.2.064			
72041	The Red Hat Enterprise Linux operating system must be configured so that file systems containing user home directories are mounted to prevent files with the setuid and setgid bit set from being executed.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72043	The Red Hat Enterprise Linux operating system must prevent files with the setuid and setgid bit set from being executed on file systems that are used with removable media.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72045	The Red Hat Enterprise Linux operating system must prevent files with the setuid and setgid bit set from being executed on file systems that are being imported via Network File System (NFS).	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72047	The Red Hat Enterprise Linux operating system must be configured so that all world-writable directories are group-owned by root, sys, bin, or an application group.	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
72049	The Red Hat Enterprise Linux operating system must set the umask value to 077 for all local interactive user accounts.	CM-3 f; CM-5 (1); CM-6 c; CM-11 (2)	3.4.3 3.4.1 3.4.2		CM.2.065 CM.2.061 CM.2.064			
72051	The Red Hat Enterprise Linux operating system must have cron logging implemented.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72053	The Red Hat Enterprise Linux operating system must be configured so that the cron.allow file, if it exists, is owned by root.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72055	The Red Hat Enterprise Linux operating system must be configured so that the cron.allow file, if it exists, is group-owned by root.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72057	The Red Hat Enterprise Linux operating system must disable Kernel core dumps unless needed.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72059	The Red Hat Enterprise Linux operating system must be configured so that a separate file system is used for user home directories (such as /home or an equivalent).	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72061	The Red Hat Enterprise Linux operating system must use a separate file system for /var.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72063	The Red Hat Enterprise Linux operating system must use a separate file system for the system audit data path.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72065	The Red Hat Enterprise Linux operating system must use a separate file system for /tmp (or equivalent).	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72067	The Red Hat Enterprise Linux operating system must implement NIST FIPS-validated cryptography for the following: to provision digital signatures, to generate cryptographic hashes, and to protect data requiring data-at-rest protections in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	AC-17 (2); SC-13; SC-28; SC-28 (1)	3.13.11 3.13.16			SC.3.177 SC.3.191		
72069	The Red Hat Enterprise Linux operating system must be configured so that the file integrity tool is configured to verify Access Control Lists (ACLs).	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72071	The Red Hat Enterprise Linux operating system must be configured so that the file integrity tool is configured to verify extended attributes.	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
72073	The Red Hat Enterprise Linux operating system must use a file integrity tool that is configured to use FIPS 140-2 approved cryptographic hashes for validating file contents and directories.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72075	The Red Hat Enterprise Linux operating system must not allow removable media to be used as the boot loader unless approved.	CM-3 f; CM-5 (1); CM-6 c; CM-11 (2)	3.4.3 3.4.1 3.4.2		CM.2.065 CM.2.061 CM.2.064			
72077	The Red Hat Enterprise Linux operating system must not have the telnet-server package installed.	CM-7 a	3.4.6		CM.2.062			
72079	The Red Hat Enterprise Linux operating system must be configured so that auditing is configured to produce records containing information to establish what type of events occurred, where the events occurred, the source of the events, and the outcome of the events. These audit records must also identify individual identities of group account users.	AU-2 d; AU-3	3.3.2 3.3.3		AU.2.041 AU.2.042			
72081	The Red Hat Enterprise Linux operating system must shut down upon audit processing failure, unless availability is an overriding concern. If availability is a concern, the system must alert the designated staff (System Administrator [SA] and Information System Security Officer [ISSO] at a minimum) in the event of an audit processing failure.	AU-5 a	3.3.4			AU.3.046		
72095	The Red Hat Enterprise Linux operating system must audit all executions of privileged functions.	AC-6 (9)	3.1.7			AC.3.018		
72097	The Red Hat Enterprise Linux operating system must audit all uses of the chown syscall.	AU-2 d; AU-12 c	3.3.2 3.3.3		AU.2.041 AU.2.042			
72099	The Red Hat Enterprise Linux operating system must audit all uses of the fchown syscall.	AU-2 d; AU-12 c	3.3.2 3.3.3		AU.2.041 AU.2.042			
72101	The Red Hat Enterprise Linux operating system must audit all uses of the lchown syscall.	AU-2 d; AU-12 c	3.3.2 3.3.3		AU.2.041 AU.2.042			
72103	The Red Hat Enterprise Linux operating system must audit all uses of the fchownat syscall.	AU-2 d; AU-12 c	3.3.2 3.3.3		AU.2.041 AU.2.042			
72105	The Red Hat Enterprise Linux operating system must audit all uses of the chmod syscall.	AU-12 c	3.3.2 3.3.3		AU.2.041 AU.2.042			

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
72107	The Red Hat Enterprise Linux operating system must audit all uses of the fchmod syscall.	AU-12 c	3.3.2 3.3.3		AU.2.041 AU.2.042			
72109	The Red Hat Enterprise Linux operating system must audit all uses of the fchmodat syscall.	AU-12 c	3.3.2 3.3.3		AU.2.041 AU.2.042			
72111	The Red Hat Enterprise Linux operating system must audit all uses of the setxattr syscall.	AU-12 c	3.3.2 3.3.3		AU.2.041 AU.2.042			
72113	The Red Hat Enterprise Linux operating system must audit all uses of the fsetxattr syscall.	AU-12 c	3.3.2 3.3.3		AU.2.041 AU.2.042			
72115	The Red Hat Enterprise Linux operating system must audit all uses of the lsetxattr syscall.	AU-12 c	3.3.2 3.3.3		AU.2.041 AU.2.042			
72117	The Red Hat Enterprise Linux operating system must audit all uses of the removexattr syscall.	AU-12 c	3.3.2 3.3.3		AU.2.041 AU.2.042			
72119	The Red Hat Enterprise Linux operating system must audit all uses of the fremovexattr syscall.	AU-12 c	3.3.2 3.3.3		AU.2.041 AU.2.042			
72121	The Red Hat Enterprise Linux operating system must audit all uses of the lremovexattr syscall.	AU-12 c	3.3.2 3.3.3		AU.2.041 AU.2.042			
72123	The Red Hat Enterprise Linux operating system must audit all uses of the creat syscall.	AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3		AU.2.041 AU.2.042			
72125	The Red Hat Enterprise Linux operating system must audit all uses of the open syscall.	AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3		AU.2.041 AU.2.042			
72127	The Red Hat Enterprise Linux operating system must audit all uses of the openat syscall.	AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3		AU.2.041 AU.2.042			
72129	The Red Hat Enterprise Linux operating system must audit all uses of the open_by_handle_at syscall.	AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3		AU.2.041 AU.2.042			
72131	The Red Hat Enterprise Linux operating system must audit all uses of the truncate syscall.	AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3		AU.2.041 AU.2.042			

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
72133	The Red Hat Enterprise Linux operating system must audit all uses of the ftruncate syscall.	AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3		AU.2.041 AU.2.042			
72135	The Red Hat Enterprise Linux operating system must audit all uses of the semanage command.	AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3		AU.2.041 AU.2.042			
72137	The Red Hat Enterprise Linux operating system must audit all uses of the setsebool command.	AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3		AU.2.041 AU.2.042			
72139	The Red Hat Enterprise Linux operating system must audit all uses of the chcon command.	AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3		AU.2.041 AU.2.042			
72141	The Red Hat Enterprise Linux operating system must audit all uses of the setfiles command.	AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3		AU.2.041 AU.2.042			
72145	The Red Hat Enterprise Linux operating system must generate audit records for all unsuccessful account access events.	AU-2 d; AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3		AU.2.041 AU.2.042			
72147	The Red Hat Enterprise Linux operating system must generate audit records for all successful account access events.	AU-2 d; AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3		AU.2.041 AU.2.042			
72149	The Red Hat Enterprise Linux operating system must audit all uses of the passwd command.	AU-3 (1); AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3		AU.2.041 AU.2.042			
72151	The Red Hat Enterprise Linux operating system must audit all uses of the unix_chkpwd command.	AU-3 (1); AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3		AU.2.041 AU.2.042			

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
72153	The Red Hat Enterprise Linux operating system must audit all uses of the gpasswd command.	AU-3 (1); AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3		AU.2.041 AU.2.042			
72155	The Red Hat Enterprise Linux operating system must audit all uses of the chage command.	AU-3 (1); AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3		AU.2.041 AU.2.042			
72157	The Red Hat Enterprise Linux operating system must audit all uses of the userhelper command.	AU-3 (1); AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3		AU.2.041 AU.2.042			
72159	The Red Hat Enterprise Linux operating system must audit all uses of the su command.	AU-3; AU-3 (1); AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3		AU.2.041 AU.2.042			
72161	The Red Hat Enterprise Linux operating system must audit all uses of the sudo command.	AU-3; AU-3 (1); AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3		AU.2.041 AU.2.042			
72163	The Red Hat Enterprise Linux operating system must audit all uses of the sudoers file and all files in the /etc/sudoers.d/ directory.	AU-3; AU-3 (1); AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3		AU.2.041 AU.2.042			
72165	The Red Hat Enterprise Linux operating system must audit all uses of the newgrp command.	AU-3; AU-3 (1); AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3		AU.2.041 AU.2.042			

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
72167	The Red Hat Enterprise Linux operating system must audit all uses of the chsh command.	AU-3; AU-3 (1); AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3		AU.2.041 AU.2.042			
72171	The Red Hat Enterprise Linux operating system must audit all uses of the mount command and syscall.	AU-3 (1); MA-4 (1) (a)	3.3.2 3.3.3		AU.2.041 AU.2.042			
72173	The Red Hat Enterprise Linux operating system must audit all uses of the umount command.	AU-3 (1); MA-4 (1) (a)	3.3.2 3.3.3		AU.2.041 AU.2.042			
72175	The Red Hat Enterprise Linux operating system must audit all uses of the postdrop command.	AU-3 (1); MA-4 (1) (a)	3.3.2 3.3.3		AU.2.041 AU.2.042			
72177	The Red Hat Enterprise Linux operating system must audit all uses of the postqueue command.	AU-3 (1); MA-4 (1) (a)	3.3.2 3.3.3		AU.2.041 AU.2.042			
72179	The Red Hat Enterprise Linux operating system must audit all uses of the ssh-keysign command.	AU-3 (1); AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3		AU.2.041 AU.2.042			
72183	The Red Hat Enterprise Linux operating system must audit all uses of the crontab command.	AU-3 (1); AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3		AU.2.041 AU.2.042			
72185	The Red Hat Enterprise Linux operating system must audit all uses of the pam_timestamp_check command.	AU-12 c	3.3.2 3.3.3		AU.2.041 AU.2.042			
72187	The Red Hat Enterprise Linux operating system must audit all uses of the init_module syscall.	AU-12 c	3.3.2 3.3.3		AU.2.041 AU.2.042			
72189	The Red Hat Enterprise Linux operating system must audit all uses of the delete_module syscall.	AU-12 c	3.3.2 3.3.3		AU.2.041 AU.2.042			

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
72191	The Red Hat Enterprise Linux operating system must audit all uses of the kmod command.	AU-12 c	3.3.2 3.3.3		AU.2.041 AU.2.042			
72197	The Red Hat Enterprise Linux operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd.	AU-12 c	3.1.1 3.1.2 3.3.1 3.3.2		AU 2.042 AU 2.041			
72197	The Red Hat Enterprise Linux operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd.	AC-2 (4); AU-12 c	3.3.2 3.3.3		AU.2.041 AU.2.042			
72199	The Red Hat Enterprise Linux operating system must audit all uses of the rename syscall.	AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3		AU.2.041 AU.2.042			
72201	The Red Hat Enterprise Linux operating system must audit all uses of the renameat syscall.	AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3		AU.2.041 AU.2.042			
72203	The Red Hat Enterprise Linux operating system must audit all uses of the rmdir syscall.	AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3		AU.2.041 AU.2.042			
72205	The Red Hat Enterprise Linux operating system must audit all uses of the unlink syscall.	AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3		AU.2.041 AU.2.042			
72207	The Red Hat Enterprise Linux operating system must audit all uses of the unlinkat syscall.	AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3		AU.2.041 AU.2.042			
72209	The Red Hat Enterprise Linux operating system must send rsyslog output to a log aggregation server.	CM-6 b	3.4.1 3.4.2		AU.2.041 AU.2.042			
72211	The Red Hat Enterprise Linux operating system must be configured so that the rsyslog daemon does not accept log messages from other servers unless the server is being used for log aggregation.	CM-3 f; CM-5 (1); CM-6 c; CM-11 (2)	3.4.3 3.4.1 3.4.2		CM.2.065 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
72219	The Red Hat Enterprise Linux operating system must be configured to prohibit or restrict the use of functions, ports, protocols, and/or services, as defined in the Ports, Protocols, and Services Management Component Local Service Assessment (PPSM CLSA) and vulnerability assessments.	AC-17 (1); CM-7 b	3.1.12 3.4.6		CM.2.062 AC.2.013			
72221	The Red Hat Enterprise Linux operating system must use a FIPS 140-2 approved cryptographic algorithm for SSH communications.	AC-17 (2); CM-6 b; IA-7	3.1.13 3.4.1 3.4.2		CM.2.061 CM.2.062	AC.3.014		
72223	The Red Hat Enterprise Linux operating system must be configured so that all network connections associated with a communication session are terminated at the end of the session or after 10 minutes of inactivity from the user at a command prompt, except to fulfill documented and validated mission requirements.	AC-12; SC-10	3.1.11 3.13.9			AC.3.019 SC.3.186		
72225	The Red Hat Enterprise Linux operating system must display the Standard Mandatory DoD Notice and Consent Banner immediately prior to, or as part of, remote access logon prompts.	AC-8 a; AC-8 b; AC-8 c 1; AC-8 c 2; AC-8 c 3	3.1.9		AC.2.005			
72227	The Red Hat Enterprise Linux operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) authentication communications.	AC-17 (2)	3.1.13			AC.3.014		
72229	The Red Hat Enterprise Linux operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) communications.	AC-17 (2)	3.1.13			AC.3.014		
72231	The Red Hat Enterprise Linux operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) communications.	AC-17 (2)	3.1.13			AC.3.014		
72233	The Red Hat Enterprise Linux operating system must be configured so that all networked systems have SSH installed.	SC-8; SC-8 (1); SC-8 (2)	3.13.9			SC.3.186		
72235	The Red Hat Enterprise Linux operating system must be configured so that all networked systems use SSH for confidentiality and integrity of transmitted and received information as well as information during preparation for transmission.	SC-8; SC-8 (1); SC-8 (2)	3.13.9			SC.3.186		

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
72237	The Red Hat Enterprise Linux operating system must be configured so that all network connections associated with SSH traffic are terminated at the end of the session or after 10 minutes of inactivity, except to fulfill documented and validated mission requirements.	AC-12; SC-10	3.1.11 3.13.9			AC.3.019 SC.3.186		
72239	The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon does not allow authentication using RSA rhosts authentication.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72241	The Red Hat Enterprise Linux operating system must be configured so that all network connections associated with SSH traffic terminate after a period of inactivity.	AC-12; SC-10	3.1.11 3.13.9			AC.3.019 SC.3.186		
72243	The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon does not allow authentication using rhosts authentication.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72245	The Red Hat Enterprise Linux operating system must display the date and time of the last successful account logon upon an SSH logon.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72247	The Red Hat Enterprise Linux operating system must not permit direct logons to the root account using remote access via SSH.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72249	The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon does not allow authentication using known hosts authentication.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72253	The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon is configured to only use Message Authentication Codes (MACs) employing FIPS 140-2 approved cryptographic hash algorithms.	AC-17 (2)	3.1.13			AC.3.014		
72255	The Red Hat Enterprise Linux operating system must be configured so that the SSH public host key files have mode 0644 or less permissive.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72257	The Red Hat Enterprise Linux operating system must be configured so that the SSH private host key files have mode 0640 or less permissive.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72259	The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon does not permit Generic Security Service Application Program Interface (GSSAPI) authentication unless needed.	CM-3 f; CM-5 (1); CM-6 c; CM-11 (2)	3.4.3 3.4.1 3.4.2		CM.2.065 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
72261	The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon does not permit Kerberos authentication unless needed.	CM-3 f; CM-5 (1); CM-6 c; CM-11 (2)	3.4.3 3.4.1 3.4.2		CM.2.065 CM.2.061 CM.2.064			
72263	The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon performs strict mode checking of home directory configuration files.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72265	The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon uses privilege separation.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72267	The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon does not allow compression or only allows compression after successful authentication.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72269	The Red Hat Enterprise Linux operating system must, for networked systems, synchronize clocks with a server that is synchronized to one of the redundant United States Naval Observatory (USNO) time servers, a time server designated for the appropriate DoD network (NIPRNet/SIPRNet), and/or the Global Positioning System (GPS).	AU-8 (1) (a); AU-8 (1) (b)	3.3.7		AU.2.043			
72273	The Red Hat Enterprise Linux operating system must enable an application firewall, if available.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72275	The Red Hat Enterprise Linux operating system must display the date and time of the last successful account logon upon logon.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72277	The Red Hat Enterprise Linux operating system must not contain .shosts files.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72279	The Red Hat Enterprise Linux operating system must not contain shosts.equiv files.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72281	For Red Hat Enterprise Linux operating systems using DNS resolution, at least two name servers must be configured.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72283	The Red Hat Enterprise Linux operating system must not forward Internet Protocol version 4 (IPv4) source-routed packets.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72285	The Red Hat Enterprise Linux operating system must not forward Internet Protocol version 4 (IPv4) source-routed packets by default.	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
72287	The Red Hat Enterprise Linux operating system must not respond to Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) echoes sent to a broadcast address.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72289	The Red Hat Enterprise Linux operating system must prevent Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirect messages from being accepted.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72291	The Red Hat Enterprise Linux operating system must not allow interfaces to perform Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirects by default.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72293	The Red Hat Enterprise Linux operating system must not send Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirects.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72295	Network interfaces configured on the Red Hat Enterprise Linux operating system must not be in promiscuous mode.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72297	The Red Hat Enterprise Linux operating system must be configured to prevent unrestricted mail relaying.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72299	The Red Hat Enterprise Linux operating system must not have a File Transfer Protocol (FTP) server package installed unless needed.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72301	The Red Hat Enterprise Linux operating system must not have the Trivial File Transfer Protocol (TFTP) server package installed if not required for operational support.	CM-3 f; CM-5 (1); CM-6 c; CM-11 (2)	3.4.3 3.4.1 3.4.2		CM.2.065 CM.2.061 CM.2.064			
72303	The Red Hat Enterprise Linux operating system must be configured so that remote X connections for interactive users are encrypted.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72305	The Red Hat Enterprise Linux operating system must be configured so that if the Trivial File Transfer Protocol (TFTP) server is required, the TFTP daemon is configured to operate in secure mode.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72307	The Red Hat Enterprise Linux operating system must not have an X Windows display manager installed unless approved.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72309	The Red Hat Enterprise Linux operating system must not be performing packet forwarding unless the system is a router.	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
72311	The Red Hat Enterprise Linux operating system must be configured so that the Network File System (NFS) is configured to use RPCSEC_GSS.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72313	SNMP community strings on the Red Hat Enterprise Linux operating system must be changed from the default.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72315	The Red Hat Enterprise Linux operating system access control program must be configured to grant or deny system access to specific hosts and services.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72317	The Red Hat Enterprise Linux operating system must not have unauthorized IP tunnels configured.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
72319	The Red Hat Enterprise Linux operating system must not forward IPv6 source-routed packets.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
73155	The Red Hat Enterprise Linux operating system must prevent a user from overriding the screensaver lock-delay setting for the graphical user interface.	AC-11 a	3.1.10		AC.2.010			
73157	The Red Hat Enterprise Linux operating system must prevent a user from overriding the session idle-delay setting for the graphical user interface.	AC-11 a	3.1.10		AC.2.010			
73159	The Red Hat Enterprise Linux operating system must be configured so that when passwords are changed or new passwords are established, pwquality must be used.	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			
73161	The Red Hat Enterprise Linux operating system must prevent binary files from being executed on file systems that are being imported via Network File System (NFS).	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
73165	The Red Hat Enterprise Linux operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/group.	AU-12 c	3.3.1 3.3.2		AU 2.042 AU 2.041			
73167	The Red Hat Enterprise Linux operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/gshadow.	AU-12 c	3.1.1 3.1.2 3.3.1 3.3.2		AU 2.042 AU 2.041			
73167	The Red Hat Enterprise Linux operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/gshadow.	AU-12 c	3.3.1 3.3.2		AU 2.042 AU 2.041			

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
73171	The Red Hat Enterprise Linux operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/shadow.	AU-12 c	3.1.1 3.1.2 3.3.1 3.3.2		AU 2.042 AU 2.041			
73173	The Red Hat Enterprise Linux operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/opasswd.	AU-12 c	3.1.1 3.1.2 3.3.1 3.3.2		AU 2.042 AU 2.041			
73173	The Red Hat Enterprise Linux operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/opasswd.	AC-2 (4); AU-12 c	3.3.1 3.3.2		AU 2.042 AU 2.041			
73175	The Red Hat Enterprise Linux operating system must ignore Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirect messages.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
73177	The Red Hat Enterprise Linux operating system must be configured so that all wireless network adapters are disabled.	AC-18 (1); SC-8	3.1.17			AC.3.012		
77821	The Red Hat Enterprise Linux operating system must be configured so that the Datagram Congestion Control Protocol (DCCP) kernel module is disabled unless required.	IA-3	3.5.1 3.5.2	IA.1.076 IA.1.077				
77823	The Red Hat Enterprise Linux operating system must require authentication upon booting into single-user and maintenance modes.	AC-3	3.1.1 3.1.2	AC.1.001 AC.1.002				
77825	The Red Hat Enterprise Linux operating system must implement virtual address space randomization.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
78995	The Red Hat Enterprise Linux operating system must prevent a user from overriding the screensaver lock-enabled setting for the graphical user interface.	AC-11 a	3.1.10		AC.2.010			
78997	The Red Hat Enterprise Linux operating system must prevent a user from overriding the screensaver idle-activation-enabled setting for the graphical user interface.	AC-11 a	3.1.10		AC.2.010			
78999	The Red Hat Enterprise Linux operating system must audit all uses of the create_module syscall.	AU-12 c	3.3.1 3.3.2		AU 2.042 AU 2.041			
79001	The Red Hat Enterprise Linux operating system must audit all uses of the finit_module syscall.	AU-12 c	3.3.1 3.3.2		AU 2.042 AU 2.041			

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
81003	The Red Hat Enterprise Linux operating system must be configured so that /etc/pam.d/passwd implements /etc/pam.d/system-auth when changing passwords.	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				
81005	Red Hat Enterprise Linux operating systems version 7.2 or newer with a Basic Input/Output System (BIOS) must require authentication upon booting into single-user and maintenance modes.	AC-3	3.1.1 3.1.2	AC.1.001 AC.1.002				
81007	Red Hat Enterprise Linux operating systems version 7.2 or newer using Unified Extensible Firmware Interface (UEFI) must require authentication upon booting into single-user and maintenance modes.	AC-3	3.1.1 3.1.2	AC.1.001 AC.1.002				
81009	The Red Hat Enterprise Linux operating system must mount /dev/shm with the nodev option.	CM-7 (2)	3.4.7			CM.3.068		
81011	The Red Hat Enterprise Linux operating system must mount /dev/shm with the nosuid option.	CM-7 (2)	3.4.7			CM.3.068		
81013	The Red Hat Enterprise Linux operating system must mount /dev/shm with the noexec option.	CM-7 (2)	3.4.7			CM.3.068		
92251	The Red Hat Enterprise Linux operating system must use a reverse-path filter for IPv4 network traffic when possible on all interfaces.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
92253	The Red Hat Enterprise Linux operating system must use a reverse-path filter for IPv4 network traffic when possible by default.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
94843	The Red Hat Enterprise Linux operating system must be configured so that the x86 Ctrl-Alt-Delete key sequence is disabled in the Graphical User Interface.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
100023	The Red Hat Enterprise Linux operating system must disable the graphical user interface automounter unless required.	CM-6 b; IA-3	3.4.1 3.4.2 3.5.1 3.5.2	IA.1.076 IA.1.077	CM.2.061 CM.2.064			
71855	The Red Hat Enterprise Linux operating system must be configured so that the cryptographic hash of system files and commands matches vendor values.	CM-5 (3)						
71947	The Red Hat Enterprise Linux operating system must be configured so that users must provide a password for privilege escalation.	IA-11						
71949	The Red Hat Enterprise Linux operating system must be configured so that users must re-authenticate for privilege escalation.	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
71973	The Red Hat Enterprise Linux operating system must be configured so that a file integrity tool verifies the baseline operating system configuration at least weekly.	CM-3 (5)						
71975	The Red Hat Enterprise Linux operating system must be configured so that designated personnel are notified if baseline configurations are changed in an unauthorized manner.	CM-3 (5)						
71977	The Red Hat Enterprise Linux operating system must prevent the installation of software, patches, service packs, device drivers, or operating system components from a repository without verification they have been digitally signed using a certificate that is issued by a Certificate Authority (CA) that is recognized and approved by the organization.	CM-5 (3)						
71979	The Red Hat Enterprise Linux operating system must prevent the installation of software, patches, service packs, device drivers, or operating system components of local packages without verification they have been digitally signed using a certificate that is issued by a Certificate Authority (CA) that is recognized and approved by the organization.	CM-5 (3)						
71987	The Red Hat Enterprise Linux operating system must remove all software components after updated versions have been installed.	SI-2 (6)						
71989	The Red Hat Enterprise Linux operating system must enable SELinux.	AC-3 (4); SI-6 a						
71991	The Red Hat Enterprise Linux operating system must enable the SELinux targeted policy.	AC-3 (4); SI-6 a						
72007	The Red Hat Enterprise Linux operating system must be configured so that all files and directories have a valid owner.	AC-3 (4)						
72009	The Red Hat Enterprise Linux operating system must be configured so that all files and directories have a valid group owner.	AC-3 (4)						
72083	The Red Hat Enterprise Linux operating system must off-load audit records onto a different system or media from the system being audited.	AU-4 (1)						
72085	The Red Hat Enterprise Linux operating system must encrypt the transfer of audit records off-loaded onto a different system or media from 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
72087	The Red Hat Enterprise Linux operating system must be configured so that the audit system takes appropriate action when the audit storage volume is full.	AU-4 (1)						
72089	The Red Hat Enterprise Linux operating system must initiate an action to notify the System Administrator (SA) and Information System Security Officer ISSO, at a minimum, when allocated audit record storage volume reaches 75% of the repository maximum audit record storage capacity.	AU-5 (1)						
72091	The Red Hat Enterprise Linux operating system must immediately notify the System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) via email when the threshold for the repository maximum audit record storage capacity is reached.	AU-5 (1)						
72093	The Red Hat Enterprise Linux operating system must immediately notify the System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) when the threshold for the repository maximum audit record storage capacity is reached.	AU-5 (1)						
72213	The Red Hat Enterprise Linux operating system must use a virus scan program.							
72217	The Red Hat Enterprise Linux operating system must limit the number of concurrent sessions to 10 for all accounts and/or account types.	AC-10						
72251	The Red Hat Enterprise Linux operating system must be configured so that the SSH daemon is configured to only use the SSHv2 protocol.	CM-6 b; IA-5 (1) (c)						
72417	The Red Hat Enterprise Linux operating system must have the required packages for multifactor authentication installed.	IA-2 (11); IA-2 (12)						
72427	The Red Hat Enterprise Linux operating system must implement multifactor authentication for access to privileged accounts via pluggable authentication modules (PAM).	IA-2 (11); IA-2 (12)						
72433	The Red Hat Enterprise Linux operating system must implement certificate status checking for PKI authentication.	IA-2 (11); IA-2 (12)						
73163	The Red Hat Enterprise Linux operating system must be configured so that the audit system takes appropriate action when there is an error sending audit records to a remote system.	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
77819	The Red Hat Enterprise Linux operating system must uniquely identify and must authenticate users using multifactor authentication via a graphical user logon.	IA-2 (11); IA-2 (12)						
81015	The Red Hat Enterprise Linux operating system must be configured to use the au-remote plugin.	AU-4 (1)						
81017	The Red Hat Enterprise Linux operating system must configure the au-remote plugin to off-load audit logs using the audisp-remote daemon.	AU-4 (1)						
81019	The Red Hat Enterprise Linux operating system must take appropriate action when the audisp-remote buffer is full.	AU-4 (1)						
81021	The Red Hat Enterprise Linux operating system must label all off-loaded audit logs before sending them to the central log server.	AU-4 (1)						
92255	The Red Hat Enterprise Linux operating system must have a host-based intrusion detection tool installed.							

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-12 c	3.1.1 3.1.2 3.3.1 3.3.2	**72197**
	AU.2.041 AU.2.042				AU-12 c	3.1.1 3.1.2 3.3.1 3.3.2	**73165**
	AU.2.041 AU.2.042				AU-12 c	3.1.1 3.1.2 3.3.1 3.3.2	**73167**
	AU.2.041 AU.2.042				AU-12 c	3.1.1 3.1.2 3.3.1 3.3.2	**73171**
	AU.2.041 AU.2.042				AU-12 c	3.1.1 3.1.2 3.3.1 3.3.2	**73173**
AC.1.001 AC.1.002		AC.3.018			AC-3	3.1.1 3.1.2	**71961**
AC.1.001 AC.1.002					AC-3	3.1.1 3.1.2	**71963**
AC.1.001 AC.1.002					AC-3	3.1.1 3.1.2	**77823**
AC.1.001 AC.1.002					AC-3	3.1.1 3.1.2	**81005**
AC.1.001 AC.1.002					AC-3	3.1.1 3.1.2	**81007**
IA.1.076 IA.1.077	CM.2.061 CM.2.064				CM-6 b; IA-3	3.4.1 3.4.2 3.5.1 3.5.2	**71983**
IA.1.076 IA.1.077	CM.2.061 CM.2.064				CM-6 b; IA-3	3.4.1 3.4.2 3.5.1 3.5.2	**71985**
IA.1.076 IA.1.077					IA-2	3.5.1 3.5.2	**72003**
IA.1.076 IA.1.077					IA-3	3.5.1 3.5.2	**77821**
IA.1.076 IA.1.077	CM.2.061 CM.2.064				CM-6 b; IA-3	3.4.1 3.4.2 3.5.1 3.5.2	**100023**

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) (a)	3.5.7 3.5.8 3.5.9 3.5.10	**81003**
	AC.2.005				AC-8 a	3.1.9	**71859**
	AC.2.005				AC-8 a	3.1.9	**71861**
	AC.2.005				AC-8 a	3.1.9	**71863**
	AC.2.005				AC-8 a; AC-8 b; AC-8 c 1; AC-8 c 2; AC-8 c 3	3.1.9	**72225**
	AC.2.009				AC-7 a; AC-7 b	3.1.8	**71943**
	AC.2.009				AC-7 b	3.1.8	**71945**
	AC.2.010				AC-11 b	3.1.17	**71891**
	AC.2.010				AC-11 a	3.1.17	**71893**
	AC.2.010				AC-11 a	3.1.17	**71897**
	AC.2.010				AC-11 a	3.1.17	**71899**
	AC.2.010				AC-11 a	3.1.17	**71901**
	AC.2.010				AC-11 a	3.1.10	**73155**
	AC.2.010				AC-11 a	3.1.10	**73157**
	AC.2.010				AC-11 a	3.1.10	**78995**
	AC.2.010				AC-11 a	3.1.10	**78997**
	AU.2.041 AU.2.042				AC-2 (4); AU-12 c	3.3.1 3.3.2	**73165**
	AU.2.041 AU.2.042				AC-2 (4); AU-12 c	3.3.1 3.3.2	**73167**
	AU.2.041 AU.2.042				AC-2 (4); AU-12 c	3.3.1 3.3.2	**73171**
	AU.2.041 AU.2.042				AC-2 (4); AU-12 c	3.3.1 3.3.2	**73173**
	AU.2.041 AU.2.042				AU-12 c	3.3.1 3.3.2	**78999**
	AU.2.041 AU.2.042				AU-12 c	3.3.1 3.3.2	**79001**

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-2 d; AU-3	3.3.2 3.3.3	**72079**
	AU.2.041 AU.2.042				AU-2 d; AU-12 c	3.3.2 3.3.3	**72097**
	AU.2.041 AU.2.042				AU-2 d; AU-12 c	3.3.2 3.3.3	**72099**
	AU.2.041 AU.2.042				AU-2 d; AU-12 c	3.3.2 3.3.3	**72101**
	AU.2.041 AU.2.042				AU-2 d; AU-12 c	3.3.2 3.3.3	**72103**
	AU.2.041 AU.2.042				AU-12 c	3.3.2 3.3.3	**72105**
	AU.2.041 AU.2.042				AU-12 c	3.3.2 3.3.3	**72107**
	AU.2.041 AU.2.042				AU-12 c	3.3.2 3.3.3	**72109**
	AU.2.041 AU.2.042				AU-12 c	3.3.2 3.3.3	**72111**
	AU.2.041 AU.2.042				AU-12 c	3.3.2 3.3.3	**72113**
	AU.2.041 AU.2.042				AU-12 c	3.3.2 3.3.3	**72115**
	AU.2.041 AU.2.042				AU-12 c	3.3.2 3.3.3	**72117**
	AU.2.041 AU.2.042				AU-12 c	3.3.2 3.3.3	**72119**
	AU.2.041 AU.2.042				AU-12 c	3.3.2 3.3.3	**72121**
	AU.2.041 AU.2.042				AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3	**72123**

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-12 c; MA-4 (1) (a)	3.3.2 3.3.3	**72125**
	AU.2.041 AU.2.042				AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3	**72127**
	AU.2.041 AU.2.042				AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3	**72129**
	AU.2.041 AU.2.042				AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3	**72131**
	AU.2.041 AU.2.042				AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3	**72133**
	AU.2.041 AU.2.042				AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3	**72135**
	AU.2.041 AU.2.042				AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3	**72137**
	AU.2.041 AU.2.042				AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3	**72139**
	AU.2.041 AU.2.042				AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3	**72141**
	AU.2.041 AU.2.042				AU-2 d; AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3	**72145**
	AU.2.041 AU.2.042				AU-2 d; AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3	**72147**
	AU.2.041 AU.2.042				AU-3 (1); AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3	**72149**
	AU.2.041 AU.2.042				AU-3 (1); AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3	**72151**
	AU.2.041 AU.2.042				AU-3 (1); AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3	**72153**
	AU.2.041 AU.2.042				AU-3 (1); AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3	**72155**

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-3 (1); AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3	**72157**
	AU.2.041 AU.2.042				AU-3; AU-3 (1); AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3	**72159**
	AU.2.041 AU.2.042				AU-3; AU-3 (1); AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3	**72161**
	AU.2.041 AU.2.042				AU-3; AU-3 (1); AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3	**72163**
	AU.2.041 AU.2.042				AU-3; AU-3 (1); AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3	**72165**
	AU.2.041 AU.2.042				AU-3; AU-3 (1); AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3	**72167**
	AU.2.041 AU.2.042				AU-3 (1); MA-4 (1) (a)	3.3.2 3.3.3	**72171**
	AU.2.041 AU.2.042				AU-3 (1); MA-4 (1) (a)	3.3.2 3.3.3	**72173**
	AU.2.041 AU.2.042				AU-3 (1); MA-4 (1) (a)	3.3.2 3.3.3	**72175**
	AU.2.041 AU.2.042				AU-3 (1); MA-4 (1) (a)	3.3.2 3.3.3	**72177**
	AU.2.041 AU.2.042				AU-3 (1); AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3	**72179**
	AU.2.041 AU.2.042				AU-3 (1); AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3	**72183**
	AU.2.041 AU.2.042				AU-12 c	3.3.2 3.3.3	**72185**

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-12 c	3.3.2 3.3.3	**72187**
	AU.2.041 AU.2.042				AU-12 c	3.3.2 3.3.3	**72189**
	AU.2.041 AU.2.042				AU-12 c	3.3.2 3.3.3	**72191**
	AU.2.041 AU.2.042				AC-2 (4); AU-12 c	3.3.2 3.3.3	**72197**
	AU.2.041 AU.2.042				AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3	**72199**
	AU.2.041 AU.2.042				AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3	**72201**
	AU.2.041 AU.2.042				AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3	**72203**
	AU.2.041 AU.2.042				AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3	**72205**
	AU.2.041 AU.2.042				AU-12 c; MA-4 (1) (a)	3.3.2 3.3.3	**72207**
	AU.2.043				AU-8 (1) (a); AU-8 (1) (b)	3.3.7	**72269**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**71937**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**71951**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**71953**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**71955**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**71957**

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	**71959**
	CM.2.061 CM.2.062	AC.3.014			AC-17 (2); CM-6 b; IA-7	3.1.13 3.4.1 3.4.2	**72221**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**71993**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**71995**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**71997**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**71999**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72001**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72005**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72011**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72013**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72015**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72017**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72019**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72021**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72023**

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	**72025**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72027**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72029**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72031**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72033**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72035**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72037**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72041**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72043**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72045**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72047**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72051**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72053**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72055**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72057**

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	**72059**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72061**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72063**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72065**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72069**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72071**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72073**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72209**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72239**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72243**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72245**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72247**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72249**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72255**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72257**

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	**72263**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72265**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72267**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72273**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72275**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72277**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72279**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72281**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72283**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72285**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72287**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72289**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72291**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72293**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72295**

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	**72297**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72299**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72303**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72305**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72307**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72309**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72311**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72313**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72315**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72317**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**72319**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**73161**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**73175**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**77825**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**92251**

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	**92253**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**94843**
	CM.2.062				CM-7 a	3.4.6	**72077**
	CM.2.062 AC.2.013				AC-17 (1); CM-7 b	3.1.12 3.4.6	**72219**
	CM.2.065 CM.2.061 CM.2.064				CM-3 f; CM-5 (1); CM-6 c; CM-11 (2)	3.4.3 3.4.1 3.4.2	**72039**
	CM.2.065 CM.2.061 CM.2.064				CM-3 f; CM-5 (1); CM-6 c; CM-11 (2)	3.4.3 3.4.1 3.4.2	**72049**
	CM.2.065 CM.2.061 CM.2.064				CM-3 f; CM-5 (1); CM-6 c; CM-11 (2)	3.4.3 3.4.1 3.4.2	**72075**
	CM.2.065 CM.2.061 CM.2.064				CM-3 f; CM-5 (1); CM-6 c; CM-11 (2)	3.4.3 3.4.1 3.4.2	**72211**
	CM.2.065 CM.2.061 CM.2.064				CM-3 f; CM-5 (1); CM-6 c; CM-11 (2)	3.4.3 3.4.1 3.4.2	**72259**
	CM.2.065 CM.2.061 CM.2.064				CM-3 f; CM-5 (1); CM-6 c; CM-11 (2)	3.4.3 3.4.1 3.4.2	**72261**
	CM.2.065 CM.2.061 CM.2.064				CM-3 f; CM-5 (1); CM-6 c; CM-11 (2)	3.4.3 3.4.1 3.4.2	**72301**
	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	**71903**

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) (a)	3.5.7 3.5.8 3.5.9 3.5.10	**71905**
	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	**71907**
	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	**71909**
	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5 (1) (b)	3.5.7 3.5.8 3.5.9 3.5.10	**71911**
	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5 (1) (b)	3.5.7 3.5.8 3.5.9 3.5.10	**71913**
	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5 (1) (b)	3.5.7 3.5.8 3.5.9 3.5.10	**71915**
	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5 (1) (b)	3.5.7 3.5.8 3.5.9 3.5.10	**71917**
	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	**71919**
	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	**71921**
	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	**71923**
	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	**71925**

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	**71927**
	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	**71929**
	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	**71931**
	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	**71933**
	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	**71935**
	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	**73159**
		AC.3.012			AC-18 (1); SC-8	3.1.17	**73177**
		AC.3.014			AC-17 (2)	3.1.13	**72227**
		AC.3.014			AC-17 (2)	3.1.13	**72229**
		AC.3.014			AC-17 (2)	3.1.13	**72231**
		AC.3.014			AC-17 (2)	3.1.13	**72253**
		AC.3.017 AU.3.049			AC-3 (4); AC-6 (10); AU-9; AU-9 (3)	3.17 3.3.8	**71849**
		AC.3.018			AC-3 (4); AC-6 (10)	3.1.7	**71971**
		AC.3.018			AC-6 (9)	3.1.7	**72095**
		AC.3.019 SC.3.186			AC-12; SC-10	3.1.11 3.13.9	**72223**
		AC.3.019 SC.3.186			AC-12; SC-10	3.1.11 3.13.9	**72237**

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.3.019 SC.3.186			AC-12; SC-10	3.1.11 3.13.9	**72241**
		AU.3.046			AU-5 a	3.3.4	**72081**
		CM.3.068			CM-7 (2)	3.4.7	**81009**
		CM.3.068			CM-7 (2)	3.4.7	**81011**
		CM.3.068			CM-7 (2)	3.4.7	**81013**
		CM.3068			CM-7 a	3.4.7	**71967**
		CM.3068			CM-7 a	3.4.7	**71969**
		IA.3.083			IA-2 (2)	3.5.3	**71939**
		IA.3.083			IA-2 (2)	3.5.3	**71965**
		IA.3.085 IA.3.086			IA-4 e	3.5.5 3.5.6	**71941**
		SC.3.177 SC.3.191			AC-17 (2); SC-13; SC-28; SC-28 (1)	3.13.11 3.13.16	**72067**
		SC.3.186			SC-8; SC-8 (1); SC-8 (2)	3.13.9	**72233**
		SC.3.186			SC-8; SC-8 (1); SC-8 (2)	3.13.9	**72235**
					CM-5 (3)		**71855**
					IA-11		**71947**
					IA-11		**71949**
					CM-3 (5)		**71973**
					CM-3 (5)		**71975**
					CM-5 (3)		**71977**
					CM-5 (3)		**71979**
					SI-2 (6)		**71987**
					AC-3 (4); SI-6 a		**71989**
					AC-3 (4); SI-6 a		**71991**
					AC-3 (4)		**72007**
					AC-3 (4)		**72009**
					AU-4 (1)		**72083**

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 (1)		**72085**
					AU-4 (1)		**72087**
					AU-5 (1)		**72089**
					AU-5 (1)		**72091**
					AU-5 (1)		**72093**
							72213
					AC-10		**72217**
					CM-6 b; IA-5 (1) (c)		**72251**
					IA-2 (11); IA-2 (12)		**72417**
					IA-2 (11); IA-2 (12)		**72427**
					IA-2 (11); IA-2 (12)		**72433**
					AU-4 (1)		**73163**
					IA-2 (11); IA-2 (12)		**77819**
					AU-4 (1)		**81015**
					AU-4 (1)		**81017**
					AU-4 (1)		**81019**
					AU-4 (1)		**81021**
							92255

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		

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		