STIG & CMMC Control Matrix

for

Red Hat 8

October 2021

SteelCloud
Get Compliant. Stay Compliant.

About this Document

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

About SteelCloud

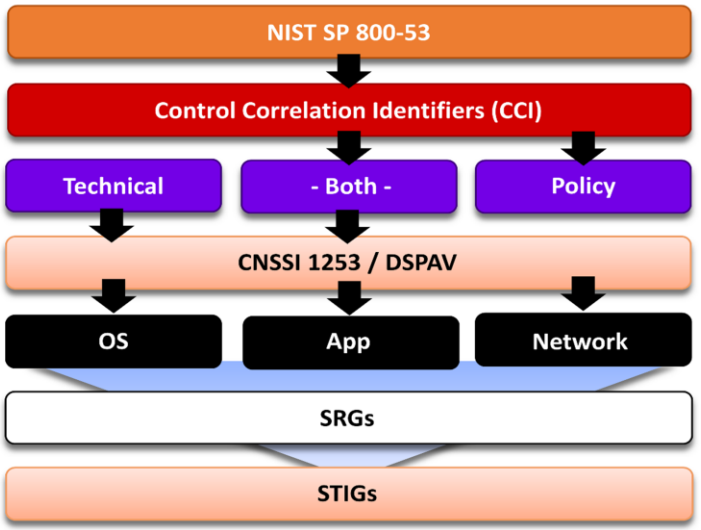
SteelCloud has spent the last decade developing patented technology to automate government policy compliance, configuration control, and cloud security. Our ConfigOS software solution was designed to reduce initial hardening time by 90% and ongoing STIG compliance effort by more than 70%. Our technology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

Links

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

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

How are STIGs Developed



Source: DISA

SteelCloud
AUTOMATING STIG & CIS COMPLIANCE

SteelCloud

I. STIG to CMMC Matrix

Red Hat 8

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
230221	RHEL 8 must be a vendor-supported release.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230222	RHEL 8 vendor packaged 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			
230223	RHEL 8 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)	3.1.1 3.1.2 3.1.13	AC.1.001 AC.1.002		AC.3.014		
230224	All RHEL 8 local disk partitions must implement cryptographic mechanisms to prevent unauthorized disclosure or modification of all information that requires at rest protection.	SC-28	3.13.16			SC.3.191		
230225	RHEL 8 must display the Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system via a ssh logon.	AC-8 a	3.1.9		AC.2.005			
230226	RHEL 8 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			
230227	RHEL 8 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			
230228	All RHEL 8 remote access methods must be monitored.	AC-17(1)	3.1.1 3.1.2 3.1.12	AC.1.001 AC.1.002	AC.2.013			
230229	RHEL 8, for PKI-based authentication, must validate certificates by constructing a certification path (which includes status information) to an accepted trust anchor.	IA-5(2) (a)	3.5.1 3.5.2	IA.1.076 IA.1.077				
230230	RHEL 8, for certificate-based authentication, must enforce authorized access to the corresponding private key.	IA-5(2)	3.5.1 3.5.2	IA.1.076 IA.1.077				
230231	RHEL 8 must encrypt all stored passwords with a FIPS 140-2 approved cryptographic hashing algorithm.	IA-5(1) (c)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	IA.1.076 IA.1.077	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
230232	RHEL 8 must employ FIPS 140-2 approved cryptographic hashing algorithms for all stored passwords.	IA-5(1) (c)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	IA.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081			
230233	The RHEL 8 password-auth file must be configured to use a sufficient number of hashing rounds.	IA-5(1) (c)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	IA.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081			
230234	RHEL 8 operating systems booted with United Extensible Firmware Interface (UEFI) must require authentication upon booting into single-user mode and maintenance.	AC-3	3.1.1 3.1.2	AC.1.001 AC.1.002				
230235	RHEL 8 operating systems booted with a 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				
230236	RHEL 8 operating systems must require authentication upon booting into rescue mode.	AC-3	3.1.1 3.1.2	AC.1.001 AC.1.002				
230237	The RHEL 8 pam_unix.so module must be configured in the password-auth file to use a FIPS 140-2 approved cryptographic hashing algorithm for system authentication.	IA-7						
230238	RHEL 8 must prevent system daemons from using Kerberos for authentication.	IA-7						
230239	The krb5-workstation package must not be installed on RHEL 8.	IA-7						
230240	RHEL 8 must use a Linux Security Module configured to enforce limits on system services.	SC-3						
230241	RHEL 8 must have policycoreutils package installed.	SC-3						
230242	All RHEL 8 public directories must be owned by root or a system account to prevent unauthorized and unintended information transferred via shared system resources.	SC-4	3.13.4			SC.3.182		
230243	A sticky bit must be set on all RHEL 8 public directories to prevent unauthorized and unintended information transferred via shared system resources.	SC-4	3.13.4			SC.3.182		

STIG V-ID	Rule Title	800-53 Rev. 4	800-171	CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5
230244	RHEL 8 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.	SC-10	3.13.0			SC.3.186		
230245	The RHEL 8 /var/log/messages file must have mode 0640 or less permissive.	SI-11 b						
230246	The RHEL 8 /var/log/messages file must be owned by root.	SI-11 b						
230247	The RHEL 8 /var/log/messages file must be group-owned by root.	SI-11 b						
230248	The RHEL 8 /var/log directory must have mode 0755 or less permissive.	SI-11 b						
230249	The RHEL 8 /var/log directory must be owned by root.	SI-11 b						
230250	The RHEL 8 /var/log directory must be group-owned by root.	SI-11 b						
230251	The RHEL 8 SSH server must be configured to use only Message Authentication Codes (MACs) employing FIPS 140-2 validated cryptographic hash algorithms.	AC-17(2)	3.1.1 3.1.2 3.1.13	AC.1.001 AC.1.002		AC.3.014		
230252	The RHEL 8 operating system must implement DoD-approved encryption to protect the confidentiality of SSH server connections.	AC-17(2)	3.1.1 3.1.2 3.1.13	AC.1.001 AC.1.002		AC.3.014		
230253	RHEL 8 must ensure the SSH server uses strong entropy.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230254	The RHEL 8 operating system must implement DoD-approved encryption in the OpenSSL package.	AC-17(2)	3.1.1 3.1.2 3.1.13	AC.1.001 AC.1.002		AC.3.014		
230255	The RHEL 8 operating system must implement DoD-approved TLS encryption in the OpenSSL package.	AC-17(2)	3.1.1 3.1.2 3.1.13	AC.1.001 AC.1.002		AC.3.014		
230256	The RHEL 8 operating system must implement DoD-approved TLS encryption in the GnuTLS package.	AC-17(2)	3.1.1 3.1.2 3.1.13	AC.1.001 AC.1.002		AC.3.014		
230257	RHEL 8 system commands must have mode 0755 or less permissive.	CM-5(6)	3.4.5			CM.3.067		
230258	RHEL 8 system commands must be owned by root.	CM-5(6)	3.4.5			CM.3.067		
230259	RHEL 8 system commands must be group-owned by root or a system account.	CM-5(6)	3.4.5			CM.3.067		
230260	RHEL 8 library files must have mode 0755 or less permissive.	CM-5(6)	3.4.5			CM.3.067		
230261	RHEL 8 library files must be owned by root.	CM-5(6)	3.4.5			CM.3.067		
230262	RHEL 8 library files must be group-owned by root or a system account.	CM-5(6)	3.4.5			CM.3.067		

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
230263	The RHEL 8 file integrity tool must notify the system administrator when changes to the baseline configuration or anomalies in the operation of any security functions are discovered within an organizationally defined frequency.	CM-3(5)	3.4.3		CM.2.065			
230264	RHEL 8 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)	3.4.5			CM.3.067		
230265	RHEL 8 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)	3.4.5			CM.3.067		
230266	RHEL 8 must prevent the loading of a new kernel for later execution.	CM-5(3)	3.4.5			CM.3.067		
230267	RHEL 8 must enable kernel parameters to enforce discretionary access control on symlinks.	AC-3(4)	3.1.1 3.1.2	AC.1.001 AC.1.002				
230268	RHEL 8 must enable kernel parameters to enforce discretionary access control on hardlinks.	AC-3(4)	3.1.1 3.1.2	AC.1.001 AC.1.002				
230269	RHEL 8 must restrict access to the kernel message buffer.	SC-4	3.13.4		SC.3.182			
230270	RHEL 8 must prevent kernel profiling by unprivileged users.	SC-4	3.13.4		SC.3.182			
230271	RHEL 8 must require users to provide a password for privilege escalation.	IA-11						
230272	RHEL 8 must require users to reauthenticate for privilege escalation.	IA-11						
230273	RHEL 8 must have the packages required for multifactor authentication installed.	IA-2(11)	3.5.1 3.5.2	IA.1.076 IA.1.077				
230274	RHEL 8 must implement certificate status checking for multifactor authentication.	IA-2(11)	3.5.1 3.5.2	IA.1.076 IA.1.077				
230275	RHEL 8 must accept Personal Identity Verification (PIV) credentials.	IA-2(12)	3.5.1 3.5.2	IA.1.076 IA.1.077				
230276	RHEL 8 must implement non-executable data to protect its memory from unauthorized code execution.	SI-16						
230277	RHEL 8 must clear the page allocator to prevent use-after-free attacks.	SC-3						
230278	RHEL 8 must disable virtual syscalls.	SC-3						

STIG V-ID	Rule Title	800-53 Rev. 4	800-171	CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5
230279	RHEL 8 must clear SLUB/SLAB objects to prevent use-after-free attacks.	SC-3						
230280	RHEL 8 must implement address space layout randomization (ASLR) to protect its memory from unauthorized code execution.	SI-16						
230281	YUM must remove all software components after updated versions have been installed on RHEL 8.	SI-2(6)	3.14.1	SI.1.210				
230282	RHEL 8 must enable the SELinux targeted policy.	SI-6 a						
230283	There must be no shosts.equiv files on the RHEL 8 operating system.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230284	There must be no .shosts files on the RHEL 8 operating system.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230285	RHEL 8 must enable the hardware random number generator entropy gatherer service.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230286	The RHEL 8 SSH public host key files must have mode 0644 or less permissive.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230287	The RHEL 8 SSH private host key files must have mode 0600 or less permissive.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230288	The RHEL 8 SSH daemon must perform strict mode checking of home directory configuration files.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230289	The RHEL 8 SSH daemon must not allow compression or must only allow compression after successful authentication.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230290	The RHEL 8 SSH daemon must not allow authentication using known host's authentication.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230291	The RHEL 8 SSH daemon must not allow Kerberos authentication, except to fulfill documented and validated mission requirements.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230292	RHEL 8 must use a separate file system for /var.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230293	RHEL 8 must use a separate file system for /var/log.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230294	RHEL 8 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			
230295	A separate RHEL 8 filesystem must be used for the /tmp directory.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230296	RHEL 8 must not permit direct logons to the root account using remote access via SSH.	IA-2(5)	3.5.1 3.5.2	IA.1.076 IA.1.077				
230297	The auditd service must be running in RHEL 8.	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
230298	The rsyslog service must be running in RHEL 8.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230299	RHEL 8 must prevent files with the setuid and setgid bit set from being executed on file systems that contain user home directories.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230300	RHEL 8 must prevent files with the setuid and setgid bit set from being executed on the /boot directory.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230301	RHEL 8 must prevent special devices on non-root local partitions.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230302	RHEL 8 must prevent code from being executed on file systems that contain user home directories.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230303	RHEL 8 must prevent special devices on file systems that are used with removable media.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230304	RHEL 8 must prevent code 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			
230305	RHEL 8 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			
230306	RHEL 8 must prevent code from being executed on file systems that are imported via Network File System (NFS).	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230307	RHEL 8 must prevent special devices on file systems that are imported via Network File System (NFS).	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230308	RHEL 8 must prevent files with the setuid and setgid bit set from being executed on file systems that are imported via Network File System (NFS).	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230309	Local RHEL 8 initialization files must not execute world-writable programs.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230310	RHEL 8 must disable kernel dumps unless needed.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230311	RHEL 8 must disable the kernel.core_pattern.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230312	RHEL 8 must disable acquiring, saving, and processing core dumps.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230313	RHEL 8 must disable core dumps for all users.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230314	RHEL 8 must disable storing core dumps.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230315	RHEL 8 must disable core dump backtraces.	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
230316	For RHEL 8 systems using Domain Name Servers (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			
230317	Executable search paths within the initialization files of all local interactive RHEL 8 users must only contain paths that resolve to the system default or the users home directory.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230318	All RHEL 8 world-writable directories must be owned by root, sys, bin, or an application user.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230319	All RHEL 8 world-writable directories must be 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			
230320	All RHEL 8 local interactive users must 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			
230321	All RHEL 8 local interactive user home directories must have mode 0750 or less permissive.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230322	All RHEL 8 local interactive user home directories must be group-owned by the home directory owner's primary group.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230323	All RHEL 8 local interactive user home directories defined in the /etc/passwd file must exist.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230324	All RHEL 8 local interactive user accounts must be assigned a home directory upon creation.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230325	All RHEL 8 local initialization files must have mode 0740 or less permissive.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230326	All RHEL 8 local files and directories must have a valid owner.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230327	All RHEL 8 local files and directories must have a valid group owner.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230328	A separate RHEL 8 filesystem must be 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			
230329	Unattended or automatic logon via the RHEL 8 graphical user interface must not be allowed.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230330	RHEL 8 must not allow users to override SSH environment variables.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230331	RHEL 8 temporary user accounts must be provisioned with an expiration time of 72 hours or less.	AC-2(2)	3.1.1 3.1.2	AC.1.001 AC.1.002				
230332	RHEL 8 must automatically lock an account when three unsuccessful logon attempts occur.	AC-7 a	3.1.8		AC.2.009			
230333	RHEL 8 must automatically lock an account when three unsuccessful logon attempts occur.	AC-7 a	3.1.8		AC.2.009			

STIG V-ID	Rule Title	800-53 Rev. 4	800-171	CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5
230334	RHEL 8 must automatically lock an account when three unsuccessful logon attempts occur during a 15-minute time period.	AC-7 a	3.1.8		AC.2.009			
230335	RHEL 8 must automatically lock an account when three unsuccessful logon attempts occur during a 15-minute time period.	AC-7 a	3.1.8		AC.2.009			
230336	RHEL 8 must automatically lock an account until the locked account is released by an administrator when three unsuccessful logon attempts occur during a 15-minute time period.	AC-7 a	3.1.8		AC.2.009			
230337	RHEL 8 must automatically lock an account until the locked account is released by an administrator when three unsuccessful logon attempts occur during a 15-minute time period.	AC-7 a	3.1.8		AC.2.009			
230338	RHEL 8 must ensure account lockouts persist.	AC-7 a	3.1.8		AC.2.009			
230339	RHEL 8 must ensure account lockouts persist.	AC-7 a	3.1.8		AC.2.009			
230340	RHEL 8 must prevent system messages from being presented when three unsuccessful logon attempts occur.	AC-7 a	3.1.8		AC.2.009			
230341	RHEL 8 must prevent system messages from being presented when three unsuccessful logon attempts occur.	AC-7 a	3.1.8		AC.2.009			
230342	RHEL 8 must log user name information when unsuccessful logon attempts occur.	AC-7 a	3.1.8		AC.2.009			
230343	RHEL 8 must log user name information when unsuccessful logon attempts occur.	AC-7 a	3.1.8		AC.2.009			
230344	RHEL 8 must include root when automatically locking an account until the locked account is released by an administrator when three unsuccessful logon attempts occur during a 15-minute time period.	AC-7 a	3.1.8		AC.2.009			
230345	RHEL 8 must include root when automatically locking an account until the locked account is released by an administrator when three unsuccessful logon attempts occur during a 15-minute time period.	AC-7 a	3.1.8		AC.2.009			
230346	RHEL 8 must limit the number of concurrent sessions to ten for all accounts and/or account types.	AC-10						
230347	RHEL 8 must enable a user session lock until that user re-establishes access using established identification and authentication procedures for graphical user sessions.	AC-11 b	3.1.10		AC.2.010			
230348	RHEL 8 must enable a user session lock until that user re-establishes access using established identification and authentication procedures for command line sessions.	AC-11 b	3.1.10		AC.2.010			
230349	RHEL 8 must ensure session control is automatically started at shell initialization.	AC-11 b	3.1.10		AC.2.010			
230350	RHEL 8 must prevent users from disabling session control mechanisms.	AC-11 b	3.1.10		AC.2.010			

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
230351	RHEL 8 must be able to initiate directly a session lock for all connection types using smartcard when the smartcard is removed.	AC-11 b	3.1.10		AC.2.010			
230352	RHEL 8 must automatically lock graphical user sessions after 15 minutes of inactivity.	AC-11 a	3.1.10		AC.2.010			
230353	RHEL 8 must automatically lock command line user sessions after 15 minutes of inactivity.	AC-11 a	3.1.10		AC.2.010			
230354	RHEL 8 must prevent a user from overriding the session lock-delay setting for the graphical user interface.	AC-11 a	3.1.10		AC.2.010			
230355	RHEL 8 must map the authenticated identity to the user or group account for PKI-based authentication.	IA-5(2) (c)	3.5.1 3.5.2	IA.1.076 IA.1.077				
230356	RHEL 8 must ensure a password complexity module is enabled.	IA-5(1) (a)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	IA.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081			
230357	RHEL 8 must enforce password complexity by requiring that at least one uppercase character be used.	IA-5(1) (a)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	IA.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081			
230358	RHEL 8 must enforce password complexity by requiring that at least one lower-case character be used.	IA-5(1) (a)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	IA.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081			
230359	RHEL 8 must enforce password complexity by requiring that at least one lower-case character be used.	IA-5(1) (a)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	IA.1.076 IA.1.077	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
230360	RHEL 8 must require the maximum number of repeating characters of the same character class be limited to four when passwords are changed.	IA-5(1) (b)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	IA.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081			
230361	RHEL 8 must require the maximum number of repeating characters be limited to three when passwords are changed.	IA-5(1) (b)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	IA.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081			
230362	RHEL 8 must require the change of at least four character classes when passwords are changed.	IA-5(1) (b)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	IA.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081			
230363	RHEL 8 must require the change of at least 8 characters when passwords are changed.	IA-5(1) (b)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	IA.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081			
230364	RHEL 8 passwords must have a 24 hours/1 day minimum password lifetime restriction in /etc/shadow.	IA-5(1) (d)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	IA.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081			
230365	RHEL 8 passwords for new users or password changes must have a 24 hours/1 day minimum password lifetime restriction in /etc/logins.def.	IA-5(1) (d)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	IA.1.076 IA.1.077	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
230366	RHEL 8 user account passwords must have a 60-day maximum password lifetime restriction.	IA-5(1) (d)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	IA.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081			
230367	RHEL 8 user account passwords must be configured so that existing passwords are restricted to a 60-day maximum lifetime.	IA-5(1) (d)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	IA.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081			
230368	RHEL 8 passwords must be prohibited from reuse for a minimum of five generations.	IA-5(1) (e)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	IA.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081			
230369	RHEL 8 passwords must have a minimum of 15 characters.	IA-5(1) (a)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	IA.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081			
230370	RHEL 8 passwords for new users must have a minimum of 15 characters.	IA-5(1) (a)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	IA.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081			
230371	RHEL 8 duplicate User IDs (UIDs) must not exist for interactive users.	IA-2	3.5.1 3.5.2	IA.1.076 IA.1.077				
230372	RHEL 8 must implement smart card logon for multifactor authentication for access to interactive accounts.	IA-2(1)	3.5.1 3.5.2 3.5.3	IA.1.076 IA.1.077		IA.3.083		
230373	RHEL 8 account identifiers (individuals, groups, roles, and devices) must be disabled after 35 days of inactivity.	IA-4 e	3.5.5 3.5.6			IA.3.085 IA.3.086		

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
230374	RHEL 8 emergency accounts must be automatically removed or disabled after the crisis is resolved or within 72 hours.	AC-2(2)	3.1.1 3.1.2	AC.1.001 AC.1.002				
230375	All RHEL 8 passwords must contain at least one special character.	IA-5(1) (a)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	IA.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081			
230376	RHEL 8 must prohibit the use of cached authentications after one day.	IA-5(13)	3.5.1 3.5.2	IA.1.076 IA.1.077				
230377	RHEL 8 must prevent the use of dictionary words for passwords.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230378	RHEL 8 must enforce a delay of at least four seconds between logon prompts following a failed logon attempt.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230379	RHEL 8 must not have unnecessary accounts.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230380	RHEL 8 must not allow accounts configured with blank or null passwords.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230381	RHEL 8 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			
230382	RHEL 8 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			
230383	RHEL 8 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			
230384	RHEL 8 must set the umask value to 077 for all local interactive user accounts.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230385	RHEL 8 must define default permissions for logon and non-logon shells.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230386	The RHEL 8 audit system must be configured to audit the execution of privileged functions and prevent all software from executing at higher privilege levels than users executing the software.	AC-6(8)	3.1.5		AC.2.007			
230387	Cron logging must be implemented in RHEL 8.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230388	The RHEL 8 System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) must be alerted of an audit processing failure event.	AU-5 a	3.3.4			AU.3.046		

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
230389	The RHEL 8 Information System Security Officer (ISSO) and System Administrator (SA) (at a minimum) must have mail aliases to be notified of an audit processing failure.	AU-5 a	3.3.4			AU.3.046		
230390	The RHEL 8 System must take appropriate action when an audit processing failure occurs.	AU-5 b	3.3.4			AU.3.046		
230391	The RHEL 8 System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) must be alerted when the audit storage volume is full.	AU-5 b	3.3.4			AU.3.046		
230392	The RHEL 8 audit system must take appropriate action when the audit storage volume is full.	AU-5 b	3.3.4			AU.3.046		
230393	The RHEL 8 audit system must audit local events.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230394	RHEL 8 must label all off-loaded audit logs before sending them to the central log server.	AU-4(1)						
230395	RHEL 8 must resolve audit information before writing to disk.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230396	RHEL 8 audit logs must have a mode of 0600 or less permissive to prevent unauthorized read access.	AU-9	3.3.8			AU.3.049		
230397	RHEL 8 audit logs must be owned by root to prevent unauthorized read access.	AU-9	3.3.8			AU.3.049		
230398	RHEL 8 audit logs must be group-owned by root to prevent unauthorized read access.	AU-9	3.3.8			AU.3.049		
230399	RHEL 8 audit log directory must be owned by root to prevent unauthorized read access.	AU-9	3.3.8			AU.3.049		
230400	RHEL 8 audit log directory must be group-owned by root to prevent unauthorized read access.	AU-9	3.3.8			AU.3.049		
230401	RHEL 8 audit log directory must have a mode of 0700 or less permissive to prevent unauthorized read access.	AU-9	3.3.8			AU.3.049		
230402	RHEL 8 audit system must protect auditing rules from unauthorized change.	AU-9	3.3.8			AU.3.049		
230403	RHEL 8 audit system must protect logon UIDs from unauthorized change.	AU-9	3.3.8			AU.3.049		
230404	RHEL 8 must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/shadow.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230405	RHEL 8 must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/security/opasswd.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106

STIG V-ID	Rule Title	800-53 Rev. 4	800-171	CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5
230406	RHEL 8 must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230407	RHEL 8 must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/gshadow.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230408	RHEL 8 must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/group.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230409	RHEL 8 must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/sudoers.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230410	RHEL 8 must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/sudoers.d/.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230411	The RHEL 8 audit package must be installed.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230412	Successful/unsuccessful uses of the su command in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230413	The RHEL 8 audit system must be configured to audit any usage of the lremovexattr system call.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230414	The RHEL 8 audit system must be configured to audit any usage of the removexattr system call.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230415	The RHEL 8 audit system must be configured to audit any usage of the lsetxattr system call.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230416	The RHEL 8 audit system must be configured to audit any usage of the fsetxattr system call.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230417	The RHEL 8 audit system must be configured to audit any usage of the fremovexattr system call.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230418	Successful/unsuccessful uses of the chage command in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230419	Successful/unsuccessful uses of the chcon command in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230420	The RHEL 8 audit system must be configured to audit any usage of the setxattr system call.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230421	Successful/unsuccessful uses of the ssh-agent in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106

STIG V-ID	Rule Title	800-53 Rev. 4	800-171	CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5
230422	Successful/unsuccessful uses of the passwd command in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230423	Successful/unsuccessful uses of the mount command in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230424	Successful/unsuccessful uses of the umount command in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230425	Successful/unsuccessful uses of the mount syscall in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230426	Successful/unsuccessful uses of the unix_update in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230427	Successful/unsuccessful uses of postdrop in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230428	Successful/unsuccessful uses of postqueue in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230429	Successful/unsuccessful uses of semanage in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230430	Successful/unsuccessful uses of setfiles in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230431	Successful/unsuccessful uses of userhelper in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230432	Successful/unsuccessful uses of setsebool in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230433	Successful/unsuccessful uses of unix_chkpwd in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230434	Successful/unsuccessful uses of the ssh-keysign in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230435	Successful/unsuccessful uses of the setfacl command in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230436	Successful/unsuccessful uses of the pam_timestamp_check command in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230437	Successful/unsuccessful uses of the newgrp command in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230438	Successful/unsuccessful uses of the init_module command in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230439	Successful/unsuccessful uses of the rename command in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230440	Successful/unsuccessful uses of the renameat command in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106

STIG V-ID	Rule Title	800-53 Rev. 4	800-171	CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5
230441	Successful/unsuccessful uses of the rmdir command in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230442	Successful/unsuccessful uses of the unlink command in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230443	Successful/unsuccessful uses of the unlinkat command in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230444	Successful/unsuccessful uses of the gpasswd command in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230445	Successful/unsuccessful uses of the finit_module command in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230446	Successful/unsuccessful uses of the delete_module command in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230447	Successful/unsuccessful uses of the crontab command in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230448	Successful/unsuccessful uses of the chsh command in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230449	Successful/unsuccessful uses of the truncate command in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230450	Successful/unsuccessful uses of the openat system call in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230451	Successful/unsuccessful uses of the open system call in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230452	Successful/unsuccessful uses of the open_by_handle_at system call in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230453	Successful/unsuccessful uses of the ftruncate command in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230454	Successful/unsuccessful uses of the creat system call in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230455	Successful/unsuccessful uses of the chown command in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230456	Successful/unsuccessful uses of the chmod command in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230457	Successful/unsuccessful uses of the lchown system call in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230458	Successful/unsuccessful uses of the fchownat system call in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230459	Successful/unsuccessful uses of the fchown system call in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106

STIG V-ID	Rule Title	800-53 Rev. 4	800-171	CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5
230460	Successful/unsuccessful uses of the fchmodat system call in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230461	Successful/unsuccessful uses of the fchmod system call in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230462	Successful/unsuccessful uses of the sudo command in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230463	Successful/unsuccessful uses of the usermod command in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230464	Successful/unsuccessful uses of the chacl command in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230465	Successful/unsuccessful uses of the kmod command in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230466	Successful/unsuccessful modifications to the faillock log file in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230467	Successful/unsuccessful modifications to the lastlog file in RHEL 8 must generate an audit record.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230468	RHEL 8 must enable auditing of processes that start prior to the audit daemon.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230469	RHEL 8 must allocate an audit_backlog_limit of sufficient size to capture processes that start prior to the audit daemon.	AU-4						
230470	RHEL 8 must enable Linux audit logging for the USBGuard daemon.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230471	RHEL 8 must allow only the Information System Security Manager (ISSM) (or individuals or roles appointed by the ISSM) to select which auditable events are to be audited.	AU-12 b	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
230472	RHEL 8 audit tools must have a mode of 0755 or less permissive.	AU-9	3.3.8			AU.3.049		
230473	RHEL 8 audit tools must be owned by root.	AU-9	3.3.8			AU.3.049		
230474	RHEL 8 audit tools must be group-owned by root.	AU-9	3.3.8			AU.3.049		
230475	RHEL 8 must use cryptographic mechanisms to protect the integrity of audit tools.	AU-9(3)	3.3.8			AU.3.049		
230476	RHEL 8 must allocate audit record storage capacity to store at least one week of audit records, when audit records are not immediately sent to a central audit record storage facility.	AU-4						
230477	RHEL 8 must have the packages required for offloading audit logs installed.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230478	RHEL 8 must have the packages required for encrypting offloaded audit logs installed.	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
230479	The RHEL 8 audit records must be off-loaded onto a different system or storage media from the system being audited.	AU-4(1)						
230480	RHEL 8 must take appropriate action when the internal event queue is full.	AU-4(1)						
230481	RHEL 8 must encrypt the transfer of audit records off-loaded onto a different system or media from the system being audited.	AU-4(1)						
230482	RHEL 8 must authenticate the remote logging server for off-loading audit logs.	AU-4(1)						
230483	RHEL 8 must take action when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity.	AU-5(1)	3.3.4			AU.3.046		
230484	RHEL 8 must securely compare internal information system clocks at least every 24 hours with a server synchronized to an authoritative time source, such as the United States Naval Observatory (USNO) time servers, or a time server designated for the appropriate DoD network (NIPRNet/SIPRNet), and/or the Global Positioning System (GPS).	AU-8(1) (a)	3.3.7		AU.2.043			
230485	RHEL 8 must disable the chrony daemon from acting as a server.	CM-7 a	3.4.6		CM.2.062			
230486	RHEL 8 must disable network management of the chrony daemon.	CM-7 a	3.4.6		CM.2.062			
230487	RHEL 8 must not have the telnet-server package installed.	CM-7 a	3.4.6		CM.2.062			
230488	RHEL 8 must not have any automated bug reporting tools installed.	CM-7 a	3.4.6		CM.2.062			
230489	RHEL 8 must not have the sendmail package installed.	CM-7 a	3.4.6		CM.2.062			
230491	RHEL 8 must enable mitigations against processor-based vulnerabilities.	CM-7 a	3.4.6		CM.2.062			
230492	RHEL 8 must not have the rsh-server package installed.	CM-7 a	3.4.6		CM.2.062			
230493	RHEL 8 must cover or disable the built-in or attached camera when not in use.	CM-7 a	3.4.6		CM.2.062			
230494	RHEL 8 must disable the asynchronous transfer mode (ATM) protocol.	CM-7 a	3.4.6		CM.2.062			
230495	RHEL 8 must disable the controller area network (CAN) protocol.	CM-7 a	3.4.6		CM.2.062			
230496	RHEL 8 must disable the stream control transmission protocol (SCTP).	CM-7 a	3.4.6		CM.2.062			
230497	RHEL 8 must disable the transparent inter-process communication (TIPC) protocol.	CM-7 a	3.4.6		CM.2.062			
230498	RHEL 8 must disable mounting of cramfs.	CM-7 a	3.4.6		CM.2.062			
230499	RHEL 8 must disable IEEE 1394 (FireWire) Support.	CM-7 a	3.4.6		CM.2.062			

STIG V-ID	Rule Title	800-53 Rev. 4	800-171	CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5
230500	RHEL 8 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 (PPSM) Category Assignments List (CAL) and vulnerability assessments.	CM-7 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230502	The RHEL 8 file system automounter must be disabled unless required.	IA-3	3.5.1 3.5.2	IA.1.076 IA.1.077				
230503	RHEL 8 must be configured to disable USB mass storage.	IA-3	3.5.1 3.5.2	IA.1.076 IA.1.077				
230504	A RHEL 8 firewall must employ a deny-all, allow-by-exception policy for allowing connections to other systems.	AC-17(1)	3.1.1 3.1.2 3.1.12	AC.1.001 AC.1.002	AC.2.013			
230505	A firewall must be installed on RHEL 8.	AC-17(1)	3.1.1 3.1.2 3.1.12	AC.1.001 AC.1.002	AC.2.013			
230506	RHEL 8 wireless network adapters must be disabled.	AC-18(1)	3.1.16 3.1.17		AC.2.011	AC.3.012		
230507	RHEL 8 Bluetooth must be disabled.	AC-18(1)	3.1.16 3.1.17		AC.2.011	AC.3.012		
230508	RHEL 8 must mount /dev/shm with the nodev option.	CM-7(2)	3.4.6 3.4.7		CM.2.062	CM.3.068		
230509	RHEL 8 must mount /dev/shm with the nosuid option.	CM-7(2)	3.4.6 3.4.7		CM.2.062	CM.3.068		
230510	RHEL 8 must mount /dev/shm with the noexec option.	CM-7(2)	3.4.6 3.4.7		CM.2.062	CM.3.068		
230511	RHEL 8 must mount /tmp with the nodev option.	CM-7(2)	3.4.6 3.4.7		CM.2.062	CM.3.068		
230512	RHEL 8 must mount /tmp with the nosuid option.	CM-7(2)	3.4.6 3.4.7		CM.2.062	CM.3.068		
230513	RHEL 8 must mount /tmp with the noexec option.	CM-7(2)	3.4.6 3.4.7		CM.2.062	CM.3.068		
230514	RHEL 8 must mount /var/log with the nodev option.	CM-7(2)	3.4.6 3.4.7		CM.2.062	CM.3.068		
230515	RHEL 8 must mount /var/log with the nosuid option.	CM-7(2)	3.4.6 3.4.7		CM.2.062	CM.3.068		
230516	RHEL 8 must mount /var/log with the noexec option.	CM-7(2)	3.4.6 3.4.7		CM.2.062	CM.3.068		
230517	RHEL 8 must mount /var/log/audit with the nodev option.	CM-7(2)	3.4.6 3.4.7		CM.2.062	CM.3.068		

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
230518	RHEL 8 must mount /var/log/audit with the nosuid option.	CM-7(2)	3.4.6 3.4.7		CM.2.062	CM.3.068		
230519	RHEL 8 must mount /var/log/audit with the noexec option.	CM-7(2)	3.4.6 3.4.7		CM.2.062	CM.3.068		
230520	RHEL 8 must mount /var/tmp with the nodev option.	CM-7(2)	3.4.6 3.4.7		CM.2.062	CM.3.068		
230521	RHEL 8 must mount /var/tmp with the nosuid option.	CM-7(2)	3.4.6 3.4.7		CM.2.062	CM.3.068		
230522	RHEL 8 must mount /var/tmp with the noexec option.	CM-7(2)	3.4.6 3.4.7		CM.2.062	CM.3.068		
230523	The RHEL 8 fapolicy module must be installed.	CM-7(2)	3.4.6 3.4.7		CM.2.062	CM.3.068		
230524	RHEL 8 must block unauthorized peripherals before establishing a connection.	IA-3	3.5.1 3.5.2	IA.1.076 IA.1.077				
230525	A firewall must be able to protect against or limit the effects of Denial of Service (DoS) attacks by ensuring RHEL 8 can implement rate-limiting measures on impacted network interfaces.	SC-5						
230526	All RHEL 8 networked systems must have and implement SSH to protect the confidentiality and integrity of transmitted and received information, as well as information during preparation for transmission.	SC-8				SI.3.219		
230527	RHEL 8 must force a frequent session key renegotiation for SSH connections to the server.	AC-17(2)	3.1.1 3.1.2 3.1.13	AC.1.001 AC.1.002		AC.3.014		
230529	The x86 Ctrl-Alt-Delete key sequence must be disabled on RHEL 8.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230530	The x86 Ctrl-Alt-Delete key sequence in RHEL 8 must be disabled if a graphical user interface is installed.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230531	The systemd Ctrl-Alt-Delete burst key sequence in RHEL 8 must be disabled.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230532	The debug-shell systemd service must be disabled on RHEL 8.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230533	The Trivial File Transfer Protocol (TFTP) server package must not be installed if not required for RHEL 8 operational support.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230534	The root account must be the only account having unrestricted access to the RHEL 8 system.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230535	RHEL 8 must prevent IPv6 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			

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
230536	RHEL 8 must not send Internet Control Message Protocol (ICMP) redirects.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230537	RHEL 8 must not respond to 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			
230538	RHEL 8 must not forward IPv6 source-routed packets.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230539	RHEL 8 must not forward IPv6 source-routed packets by default.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230540	RHEL 8 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			
230541	RHEL 8 must not accept router advertisements on all IPv6 interfaces.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230542	RHEL 8 must not accept router advertisements on all IPv6 interfaces by default.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230543	RHEL 8 must not allow interfaces to perform Internet Control Message Protocol (ICMP) redirects by default.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230544	RHEL 8 must ignore IPv6 Internet Control Message Protocol (ICMP) redirect messages.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230545	RHEL 8 must disable access to network bpf syscall from unprivileged processes.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230546	RHEL 8 must restrict usage of ptrace to descendant processes.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230547	RHEL 8 must restrict exposed kernel pointer addresses access.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230548	RHEL 8 must disable the use of user namespaces.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230549	RHEL 8 must use reverse path filtering on all IPv4 interfaces.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230550	RHEL 8 must be configured to prevent unrestricted mail relaying.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230551	The RHEL 8 file integrity tool must be configured to verify extended attributes.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230552	The RHEL 8 file integrity tool must be configured to verify Access Control Lists (ACLs).	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230553	The graphical display manager must not be installed on RHEL 8 unless approved.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230554	RHEL 8 network interfaces must not be in promiscuous mode.	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
230555	RHEL 8 remote X connections for interactive users must be disabled unless to fulfill documented and validated mission requirements.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230556	The RHEL 8 SSH daemon must prevent remote hosts from connecting to the proxy display.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230557	If the Trivial File Transfer Protocol (TFTP) server is required, the RHEL 8 TFTP daemon must be configured to operate in secure mode.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230558	A File Transfer Protocol (FTP) server package must not be installed unless mission essential on RHEL 8.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230559	The gssproxy package must not be installed unless mission essential on RHEL 8.	CM-7 a	3.4.6		CM.2.062			
230560	The iprutils package must not be installed unless mission essential on RHEL 8.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
230561	The tuned package must not be installed unless mission essential on RHEL 8.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
237640	The krb5-server package must not be installed on RHEL 8.	IA-7						
237641	RHEL 8 must restrict privilege elevation to authorized personnel.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
237642	RHEL 8 must use the invoking user's password for privilege escalation when using "sudo".	AC-6(5)	3.1.5		AC.2.007			
237643	RHEL 8 must require re-authentication when using the "sudo" command.	IA-11						
244519	RHEL 8 must display a banner before granting local or remote access to the system via a graphical user logon.	AC-8 a	3.1.9		AC.2.005			
244520	The RHEL 8 system-auth file must be configured to use a sufficient number of hashing rounds.	IA-5(1) (c)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	IA.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081			
244521	RHEL 8 operating systems booted with United Extensible Firmware Interface (UEFI) must require a unique superusers name upon booting into single-user mode and maintenance.	AC-3	3.1.1 3.1.2	AC.1.001 AC.1.002				
244522	RHEL 8 operating systems booted with a BIOS must require a unique superusers name upon booting into single-user and maintenance modes.	AC-3	3.1.1 3.1.2	AC.1.001 AC.1.002				
244523	RHEL 8 operating systems must require authentication upon booting into emergency mode.	AC-3	3.1.1 3.1.2	AC.1.001 AC.1.002				

STIG V-ID	Rule Title	800-53 Rev. 4	800-171	CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5
244524	The RHEL 8 pam_unix.so module must be configured in the system-auth file to use a FIPS 140-2 approved cryptographic hashing algorithm for system authentication.	IA-7						
244525	The RHEL 8 SSH daemon must be configured with a timeout interval.	SC-10	3.13.9			SC.3.186		
244526	The RHEL 8 SSH daemon must be configured to use system-wide crypto policies.	AC-17(2)	3.1.1 3.1.2 3.1.13	AC.1.001 AC.1.002		AC.3.014		
244527	RHEL 8 must have the packages required to use the hardware random number generator entropy gatherer service.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
244528	The RHEL 8 SSH daemon must not allow GSSAPI authentication, except to fulfill documented and validated mission requirements.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
244529	RHEL 8 must use a separate file system for /var/tmp.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
244530	RHEL 8 must prevent files with the setuid and setgid bit set from being executed on the /boot/efi directory.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
244531	All RHEL 8 local interactive user home directory files must have mode 0750 or less permissive.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
244532	RHEL 8 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			
244533	RHEL 8 must configure the use of the pam_faillock.so module in the /etc/pam.d/system-auth file.	AC-7 a	3.1.8		AC.2.009			
244534	RHEL 8 must configure the use of the pam_faillock.so module in the /etc/pam.d/password-auth file.	AC-7 a	3.1.8		AC.2.009			
244535	RHEL 8 must initiate a session lock for graphical user interfaces when the screensaver is activated.	AC-11 a	3.1.10		AC.2.010			
244536	RHEL 8 must disable the user list at logon for graphical user interfaces.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
244537	RHEL 8 must have the tmux package installed.	AC-11 b	3.1.10		AC.2.010			
244538	RHEL 8 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			
244539	RHEL 8 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			
244540	RHEL 8 must not allow blank or null passwords in the system-auth file.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
244541	RHEL 8 must not allow blank or null passwords in the password-auth file.	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
244542	RHEL 8 audit records must contain information to establish what type of events occurred, the source of events, where events occurred, and the outcome of events.	AU-12 a	3.3.2 3.3.1		AU.2.041 AU.2.042			AU.5.055 AU.5.106
244543	RHEL 8 must notify the System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) when allocated audit record storage volume 75 percent utilization.	AU-5(1)	3.3.4			AU.3.046		
244544	A firewall must be active on RHEL 8.	AC-17(1)	3.1.1 3.1.2 3.1.12	AC.1.001 AC.1.002	AC.2.013			
244545	The RHEL 8 fapolicy module must be enabled.	CM-7(2)	3.4.6 3.4.7		CM.2.062	CM.3.068		
244546	The RHEL 8 fapolicy module must be configured to employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs.	CM-7(2)	3.4.6 3.4.7		CM.2.062	CM.3.068		
244547	RHEL 8 must have the USBGuard installed.	IA-3	3.5.1 3.5.2	IA.1.076 IA.1.077				
244548	RHEL 8 must enable the USBGuard.	IA-3	3.5.1 3.5.2	IA.1.076 IA.1.077				
244549	All RHEL 8 networked systems must have SSH installed.	SC-8				SI.3.219		
244550	RHEL 8 must prevent 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			
244551	RHEL 8 must not forward IPv4 source-routed packets.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
244552	RHEL 8 must not forward IPv4 source-routed packets by default.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
244553	RHEL 8 must ignore IPv4 Internet Control Message Protocol (ICMP) redirect messages.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
244554	RHEL 8 must enable hardening for the Berkeley Packet Filter Just-in-time compiler.	CM-6 b	3.4.1 3.4.2		CM.2.061 CM.2.064			
245540	The RHEL 8 operating system must implement the Endpoint Security for Linux Threat Prevention tool.	SI-2(2)	3.14.1	SI.1.210				

II. CMMC to STIG Matrix

Red Hat 8

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	**230221**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230222**
AC.1.001 AC.1.002		AC.3.014			AC-17(2)	3.1.1 3.1.2 3.1.13	**230223**
		SC.3.191			SC-28	3.13.16	**230224**
	AC.2.005				AC-8 a	3.1.9	**230225**
	AC.2.005				AC-8 a	3.1.9	**230226**
	AC.2.005				AC-8 a	3.1.9	**230227**
AC.1.001 AC.1.002	AC.2.013				AC-17(1)	3.1.1 3.1.2 3.1.12	**230228**
IA.1.076 IA.1.077					IA-5(2) (a)	3.5.1 3.5.2	**230229**
IA.1.076 IA.1.077					IA-5(2)	3.5.1 3.5.2	**230230**
IA.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5(1) (c)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	**230231**

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.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5(1) (c)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	**230232**
IA.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5(1) (c)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	**230233**
AC.1.001 AC.1.002					AC-3	3.1.1 3.1.2	**230234**
AC.1.001 AC.1.002					AC-3	3.1.1 3.1.2	**230235**
AC.1.001 AC.1.002					AC-3	3.1.1 3.1.2	**230236**
					IA-7		**230237**
					IA-7		**230238**
					IA-7		**230239**
					SC-3		**230240**
					SC-3		**230241**
		SC.3.182			SC-4	3.13.4	**230242**
		SC.3.182			SC-4	3.13.4	**230243**
		SC.3.186			SC-10	3.13.0	**230244**
					SI-11 b		**230245**
					SI-11 b		**230246**
					SI-11 b		**230247**

CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5	800-53 Rev. 4	800-171	STIG V-ID
					SI-11 b		**230248**
					SI-11 b		**230249**
					SI-11 b		**230250**
AC.1.001 AC.1.002		AC.3.014			AC-17(2)	3.1.1 3.1.2 3.1.13	**230251**
AC.1.001 AC.1.002		AC.3.014			AC-17(2)	3.1.1 3.1.2 3.1.13	**230252**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230253**
AC.1.001 AC.1.002		AC.3.014			AC-17(2)	3.1.1 3.1.2 3.1.13	**230254**
AC.1.001 AC.1.002		AC.3.014			AC-17(2)	3.1.1 3.1.2 3.1.13	**230255**
AC.1.001 AC.1.002		AC.3.014			AC-17(2)	3.1.1 3.1.2 3.1.13	**230256**
		CM.3.067			CM-5(6)	3.4.5	**230257**
		CM.3.067			CM-5(6)	3.4.5	**230258**
		CM.3.067			CM-5(6)	3.4.5	**230259**
		CM.3.067			CM-5(6)	3.4.5	**230260**
		CM.3.067			CM-5(6)	3.4.5	**230261**
		CM.3.067			CM-5(6)	3.4.5	**230262**
	CM.2.065				CM-3(5)	3.4.3	**230263**
		CM.3.067			CM-5(3)	3.4.5	**230264**
		CM.3.067			CM-5(3)	3.4.5	**230265**

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.3.067			CM-5(3)	3.4.5	**230266**
AC.1.001 AC.1.002					AC-3(4)	3.1.1 3.1.2	**230267**
AC.1.001 AC.1.002					AC-3(4)	3.1.1 3.1.2	**230268**
	SC.3.182				SC-4	3.13.4	**230269**
	SC.3.182				SC-4	3.13.4	**230270**
					IA-11		**230271**
					IA-11		**230272**
IA.1.076 IA.1.077					IA-2(11)	3.5.1 3.5.2	**230273**
IA.1.076 IA.1.077					IA-2(11)	3.5.1 3.5.2	**230274**
IA.1.076 IA.1.077					IA-2(12)	3.5.1 3.5.2	**230275**
					SI-16		**230276**
					SC-3		**230277**
					SC-3		**230278**
					SC-3		**230279**
					SI-16		**230280**
SI.1.210					SI-2(6)	3.14.1	**230281**
					SI-6 a		**230282**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230283**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230284**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230285**

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	**230286**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230287**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230288**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230289**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230290**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230291**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230292**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230293**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230294**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230295**
IA.1.076 IA.1.077					IA-2(5)	3.5.1 3.5.2	**230296**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230297**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230298**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230299**

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	**230300**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230301**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230302**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230303**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230304**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230305**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230306**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230307**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230308**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230309**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230310**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230311**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230312**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230313**

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	**230314**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230315**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230316**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230317**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230318**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230319**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230320**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230321**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230322**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230323**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230324**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230325**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230326**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230327**

II. CMMC to STIG Matrix

Red Hat 8

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	**230328**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230329**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230330**
AC.1.001 AC.1.002					AC-2(2)	3.1.1 3.1.2	**230331**
	AC.2.009				AC-7 a	3.1.8	**230332**
	AC.2.009				AC-7 a	3.1.8	**230333**
	AC.2.009				AC-7 a	3.1.8	**230334**
	AC.2.009				AC-7 a	3.1.8	**230335**
	AC.2.009				AC-7 a	3.1.8	**230336**
	AC.2.009				AC-7 a	3.1.8	**230337**
	AC.2.009				AC-7 a	3.1.8	**230338**
	AC.2.009				AC-7 a	3.1.8	**230339**
	AC.2.009				AC-7 a	3.1.8	**230340**
	AC.2.009				AC-7 a	3.1.8	**230341**
	AC.2.009				AC-7 a	3.1.8	**230342**
	AC.2.009				AC-7 a	3.1.8	**230343**
	AC.2.009				AC-7 a	3.1.8	**230344**
	AC.2.009				AC-7 a	3.1.8	**230345**
					AC-10		**230346**
	AC.2.010				AC-11 b	3.1.10	**230347**
	AC.2.010				AC-11 b	3.1.10	**230348**
	AC.2.010				AC-11 b	3.1.10	**230349**
	AC.2.010				AC-11 b	3.1.10	**230350**
	AC.2.010				AC-11 b	3.1.10	**230351**
	AC.2.010				AC-11 a	3.1.10	**230352**

CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5	800-53 Rev. 4	800-171	STIG V-ID
	AC.2.010				AC-11 a	3.1.10	**230353**
	AC.2.010				AC-11 a	3.1.10	**230354**
IA.1.076 IA.1.077					IA-5(2) (c)	3.5.1 3.5.2	**230355**
IA.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5(1) (a)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	**230356**
IA.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5(1) (a)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	**230357**
IA.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5(1) (a)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	**230358**
IA.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5(1) (a)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	**230359**

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.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5(1) (b)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	**230360**
IA.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5(1) (b)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	**230361**
IA.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5(1) (b)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	**230362**
IA.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5(1) (b)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	**230363**

II. CMMC to STIG Matrix

Red Hat 8

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.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5(1) (d)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	**230364**
IA.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5(1) (d)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	**230365**
IA.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5(1) (d)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	**230366**
IA.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5(1) (d)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	**230367**

II. CMMC to STIG Matrix

Red Hat 8

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.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5(1) (e)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	**230368**
IA.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5(1) (a)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	**230369**
IA.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5(1) (a)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	**230370**
IA.1.076 IA.1.077					IA-2	3.5.1 3.5.2	**230371**
IA.1.076 IA.1.077		IA.3.083			IA-2(1)	3.5.1 3.5.2 3.5.3	**230372**
		IA.3.085 IA.3.086			IA-4 e	3.5.5 3.5.6	**230373**
AC.1.001 AC.1.002					AC-2(2)	3.1.1 3.1.2	**230374**

II. CMMC to STIG Matrix

Red Hat 8

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.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5(1) (a)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	**230375**
IA.1.076 IA.1.077					IA-5(13)	3.5.1 3.5.2	**230376**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230377**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230378**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230379**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230380**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230381**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230382**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230383**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230384**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230385**
	AC.2.007				AC-6(8)	3.1.5	**230386**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230387**

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.3.046			AU-5 a	3.3.4	**230388**
		AU.3.046			AU-5 a	3.3.4	**230389**
		AU.3.046			AU-5 b	3.3.4	**230390**
		AU.3.046			AU-5 b	3.3.4	**230391**
		AU.3.046			AU-5 b	3.3.4	**230392**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230393**
					AU-4(1)		**230394**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230395**
		AU.3.049			AU-9	3.3.8	**230396**
		AU.3.049			AU-9	3.3.8	**230397**
		AU.3.049			AU-9	3.3.8	**230398**
		AU.3.049			AU-9	3.3.8	**230399**
		AU.3.049			AU-9	3.3.8	**230400**
		AU.3.049			AU-9	3.3.8	**230401**
		AU.3.049			AU-9	3.3.8	**230402**
		AU.3.049			AU-9	3.3.8	**230403**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230404**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230405**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230406**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230407**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230408**

CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5	800-53 Rev. 4	800-171	STIG V-ID
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230409**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230410**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230411**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230412**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230413**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230414**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230415**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230416**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230417**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230418**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230419**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230420**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230421**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230422**

CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5	800-53 Rev. 4	800-171	STIG V-ID
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230423**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230424**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230425**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230426**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230427**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230428**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230429**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230430**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230431**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230432**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230433**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230434**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230435**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230436**

CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5	800-53 Rev. 4	800-171	STIG V-ID
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230437**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230438**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230439**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230440**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230441**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230442**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230443**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230444**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230445**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230446**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230447**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230448**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230449**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230450**

CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5	800-53 Rev. 4	800-171	STIG V-ID
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230451**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230452**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230453**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230454**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230455**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230456**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230457**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230458**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230459**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230460**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230461**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230462**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230463**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230464**

CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5	800-53 Rev. 4	800-171	STIG V-ID
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230465**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230466**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230467**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230468**
					AU-4		**230469**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**230470**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 b	3.3.2 3.3.1	**230471**
		AU.3.049			AU-9	3.3.8	**230472**
		AU.3.049			AU-9	3.3.8	**230473**
		AU.3.049			AU-9	3.3.8	**230474**
		AU.3.049			AU-9(3)	3.3.8	**230475**
					AU-4		**230476**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230477**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230478**
					AU-4(1)		**230479**
					AU-4(1)		**230480**
					AU-4(1)		**230481**
					AU-4(1)		**230482**
		AU.3.046			AU-5(1)	3.3.4	**230483**
	AU.2.043				AU-8(1) (a)	3.3.7	**230484**
	CM.2.062				CM-7 a	3.4.6	**230485**

II. CMMC to STIG Matrix

Red Hat 8

CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5	800-53 Rev. 4	800-171	STIG V-ID
	CM.2.062				CM-7 a	3.4.6	**230486**
	CM.2.062				CM-7 a	3.4.6	**230487**
	CM.2.062				CM-7 a	3.4.6	**230488**
	CM.2.062				CM-7 a	3.4.6	**230489**
	CM.2.062				CM-7 a	3.4.6	**230491**
	CM.2.062				CM-7 a	3.4.6	**230492**
	CM.2.062				CM-7 a	3.4.6	**230493**
	CM.2.062				CM-7 a	3.4.6	**230494**
	CM.2.062				CM-7 a	3.4.6	**230495**
	CM.2.062				CM-7 a	3.4.6	**230496**
	CM.2.062				CM-7 a	3.4.6	**230497**
	CM.2.062				CM-7 a	3.4.6	**230498**
	CM.2.062				CM-7 a	3.4.6	**230499**
	CM.2.061 CM.2.064				CM-7 b	3.4.1 3.4.2	**230500**
IA.1.076 IA.1.077					IA-3	3.5.1 3.5.2	**230502**
IA.1.076 IA.1.077					IA-3	3.5.1 3.5.2	**230503**
AC.1.001 AC.1.002	AC.2.013				AC-17(1)	3.1.1 3.1.2 3.1.12	**230504**
AC.1.001 AC.1.002	AC.2.013				AC-17(1)	3.1.1 3.1.2 3.1.12	**230505**
	AC.2.011	AC.3.012			AC-18(1)	3.1.16 3.1.17	**230506**
	AC.2.011	AC.3.012			AC-18(1)	3.1.16 3.1.17	**230507**

CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5	800-53 Rev. 4	800-171	STIG V-ID
	CM.2.062	CM.3.068			CM-7(2)	3.4.6 3.4.7	**230508**
	CM.2.062	CM.3.068			CM-7(2)	3.4.6 3.4.7	**230509**
	CM.2.062	CM.3.068			CM-7(2)	3.4.6 3.4.7	**230510**
	CM.2.062	CM.3.068			CM-7(2)	3.4.6 3.4.7	**230511**
	CM.2.062	CM.3.068			CM-7(2)	3.4.6 3.4.7	**230512**
	CM.2.062	CM.3.068			CM-7(2)	3.4.6 3.4.7	**230513**
	CM.2.062	CM.3.068			CM-7(2)	3.4.6 3.4.7	**230514**
	CM.2.062	CM.3.068			CM-7(2)	3.4.6 3.4.7	**230515**
	CM.2.062	CM.3.068			CM-7(2)	3.4.6 3.4.7	**230516**
	CM.2.062	CM.3.068			CM-7(2)	3.4.6 3.4.7	**230517**
	CM.2.062	CM.3.068			CM-7(2)	3.4.6 3.4.7	**230518**
	CM.2.062	CM.3.068			CM-7(2)	3.4.6 3.4.7	**230519**
	CM.2.062	CM.3.068			CM-7(2)	3.4.6 3.4.7	**230520**
	CM.2.062	CM.3.068			CM-7(2)	3.4.6 3.4.7	**230521**

II. CMMC to STIG Matrix

Red Hat 8

CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5	800-53 Rev. 4	800-171	STIG V-ID
	CM.2.062	CM.3.068			CM-7(2)	3.4.6 3.4.7	**230522**
	CM.2.062	CM.3.068			CM-7(2)	3.4.6 3.4.7	**230523**
IA.1.076 IA.1.077					IA-3	3.5.1 3.5.2	**230524**
					SC-5		**230525**
		SI.3.219			SC-8		**230526**
AC.1.001 AC.1.002		AC.3.014			AC-17(2)	3.1.1 3.1.2 3.1.13	**230527**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230529**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230530**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230531**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230532**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230533**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230534**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230535**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230536**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230537**

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	**230538**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230539**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230540**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230541**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230542**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230543**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230544**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230545**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230546**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230547**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230548**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230549**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230550**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230551**

II. CMMC to STIG Matrix

Red Hat 8

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	**230552**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230553**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230554**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230555**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230556**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230557**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230558**
	CM.2.062				CM-7 a	3.4.6	**230559**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230560**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**230561**
					IA-7		**237640**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**237641**
	AC.2.007				AC-6(5)	3.1.5	**237642**
					IA-11		**237643**
	AC.2.005				AC-8 a	3.1.9	**244519**

II. CMMC to STIG Matrix

Red Hat 8

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.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081				IA-5(1) (c)	3.5.1 3.5.2 3.5.7 3.5.8 3.5.9 3.5.10	**244520**
AC.1.001 AC.1.002					AC-3	3.1.1 3.1.2	**244521**
AC.1.001 AC.1.002					AC-3	3.1.1 3.1.2	**244522**
AC.1.001 AC.1.002					AC-3	3.1.1 3.1.2	**244523**
					IA-7		**244524**
		SC.3.186			SC-10	3.13.9	**244525**
AC.1.001 AC.1.002		AC.3.014			AC-17(2)	3.1.1 3.1.2 3.1.13	**244526**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**244527**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**244528**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**244529**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**244530**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**244531**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**244532**

II. CMMC to STIG Matrix

Red Hat 8

CMMC Level 1	CMMC Level 2	CMMC Level 3	CMMC Level 4	CMMC Level 5	800-53 Rev. 4	800-171	STIG V-ID
	AC.2.009				AC-7 a	3.1.8	**244533**
	AC.2.009				AC-7 a	3.1.8	**244534**
	AC.2.010				AC-11 a	3.1.10	**244535**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**244536**
	AC.2.010				AC-11 b	3.1.10	**244537**
	AC.2.010				AC-11 a	3.1.10	**244538**
	AC.2.010				AC-11 a	3.1.10	**244539**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**244540**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**244541**
	AU.2.041 AU.2.042			AU.5.055 AU.5.106	AU-12 a	3.3.2 3.3.1	**244542**
		AU.3.046			AU-5(1)	3.3.4	**244543**
AC.1.001 AC.1.002	AC.2.013				AC-17(1)	3.1.1 3.1.2 3.1.12	**244544**
	CM.2.062	CM.3.068			CM-7(2)	3.4.6 3.4.7	**244545**
	CM.2.062	CM.3.068			CM-7(2)	3.4.6 3.4.7	**244546**
IA.1.076 IA.1.077					IA-3	3.5.1 3.5.2	**244547**
IA.1.076 IA.1.077					IA-3	3.5.1 3.5.2	**244548**
		SI.3.219			SC-8		**244549**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**244550**

II. CMMC to STIG Matrix

Red Hat 8

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	**244551**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**244552**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**244553**
	CM.2.061 CM.2.064				CM-6 b	3.4.1 3.4.2	**244554**
SI.1.210					SI-2(2)	3.14.1	**245540**

SteelCloud

III. CMMC Control MATRIX

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

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.3.018	3.1.7		AC-6(9) AC-6(10)	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.			X		
	AC.3.019	3.1.11		AC-12	Terminate (automatically) user sessions after a defined condition.			X		
	AC.3.012	3.1.17		AC-18(1)	Protect wireless access using authentication and encryption.			X		
	AC.3.020	3.1.18		AC-19	Control Connection of mobile devices.			X		
	AC.4.023		3.1.3e	AC-4 AC-4(1) AC-4(6) AC-4(8) AC-4(12) AC-4(13) AC-4(15) AC-4(20)	Control information flows between security domains on connected systems.				X	
	AC.4.025				Periodically review and update CUI program access permissions.				X	
	AC.5.024			SI-4(14)	Identify and mitigate risk associated with unidentified wireless access points connected to the network.					X
C003 Control remote system access	AC.2.013	3.1.12		AC-17(1)	Monitor and control remote access sessions.		X			
	AC.2.015	3.1.14		AC-17(3)	Route remote access via managed access control points.		X			
	AC.3.014	3.1.13		AC-17(2)	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.			X		
	AC.3.021	3.1.15		AC-17(4)	Authorize remote execution of privileged commands and remote access to security-relevant information.			X		
	AC.4.032				Restrict remote network access based on organizationally defined risk factors such as time of day, location of access, physical location, network connection state, and measured properties of the current user and role.				X	

SteelCloud

III. CMMC Control MATRIX

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

III. CMMC Control MATRIX

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

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
C012 Conduct training	AT.2.057	3.2.2		AT-2 AT-3	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.		X			
CONFIGURATION MANAGEMENT (CM)										
C013 Establish configuration baselines	CM.2.061	3.4.1		CM-2 CM-6 CM-8 CM-8(1)	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.		X			
	CM.2.062	3.4.6		CM-7	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.		X			
	CM.2.063	3.4.9		CM-11	Control and monitor user-installed software.		X			
C014 Perform configuration and change management	CM.2.064	3.4.2		CM-2 CM-6 CM-8 CM-8(1)	Establish and enforce security configuration settings for information technology products employed in organizational systems.		X			
	CM.2.065	3.4.3		CM-3	Track, review, approve, or disapprove, and log changes to organizational systems.		X			
	CM.2.066	3.4.4		CM-4	Analyze the security impact of changes prior to implementation.		X			
	CM.3.067	3.4.5		CM-5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.			X		
	CM.3.068	3.4.7		CM-7(1) CM-7(2)	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.			X		
	CM.3.069	3.4.8		CM-7(4) CM-7(5)	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.			X		
	CM.4.073	3.4.8		CM-7(4) CM-7(5)	Employ application whitelisting and an application vetting process for systems identified by the organization.				X	
	CM.5.074		3.14.1e	SI-7(6) SI-7(9) SI-7(10) SA-17	Verify the integrity and correctness of security critical or essential software as defined by the organization (e.g., roots of trust, formal verification, or cryptographic signatures).					X

SteelCloud

III. CMMC Control MATRIX

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

SteelCloud

III. CMMC Control MATRIX

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

SteelCloud

III. CMMC Control MATRIX

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

SteelCloud

III. CMMC Control MATRIX

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

SteelCloud

III. CMMC Control MATRIX

Capability	CMMC Control #	NIST 800-171 R1	NIST 800-171 B	NIST 800-53 R4	Control	Maturity Level				
						ML 1	ML 2	ML 3	ML 4	ML 5
C031 Identify and evaluate risk	RM.2.141	3.11.1		RA-3	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.		X			
	RM.2.142	3.11.2		RA-5	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.		X			
	RM.3.144			RA-3	Periodically perform risk assessments to identify and prioritize risks according to the defined risk categories, risk sources, and risk measurement criteria.			X		
	RM.4.149				Catalog and periodically update threat profiles and adversary TTPs.				X	
	RM.4.150		3.11.1e		Employ threat intelligence to inform the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, and response and recovery activities.				X	
	RM.4.151				Perform scans for unauthorized ports available across perimeter network boundaries over the organization's Internet network boundaries and other organizationally defined boundaries.				X	
C032 Manage risk	RM.2.143	3.11.3		RA-5	Remediate vulnerabilities in accordance with risk assessments.		X			
	RM.3.146			PM-9	Develop and implement risk mitigation plans.			X		
	RM.3.147			SA-22(1)	Manage non-vendor supported products (e.g., end of life) separately and restrict as necessary to reduce risk.			X		
	RM.5.152				Utilize an exception process for non-whitelisted software that includes mitigation techniques.					X
	RM.5.155		3.11.5e		Analyze the effectiveness of security solutions at least annually to address anticipated risk to the system and the organization based on current and accumulated threat intelligence.					X
C033 Manage supply chain risk	RM.4.148		3.11.7e	SA-12	Develop and update as required, a plan for managing supply chain risks associated with the IT supply chain.				X	

SteelCloud

III. CMMC Control MATRIX

Capability	CMMC Control #	NIST 800-171 R1	NIST 800-171 B	NIST 800-53 R4	Control	Maturity Level				
						ML 1	ML 2	ML 3	ML 4	ML 5
SECURITY ASSESSMENT (CA)										
C034 Develop and manage a system security plan	CA.2.157	3.12.4		PL-2	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.		X			
	CA.4.163			PL-1	Create, maintain, and leverage a security strategy and roadmap for organizational cybersecurity improvement.				X	
C035 Define and manage controls	CA.2.158	3.12.1		CA-2	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.		X			
	CA.2.159	3.12.2		CA-5	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.		X			
	CA.3.161	3.12.3		CA-7	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.			X		
	CA.4.164		3.12.1e	CA-8	Conduct penetration testing periodically, leveraging automated scanning tools and ad hoc tests using human experts.				X	
	CA.4.227			CA-8(2)	Periodically perform red teaming against organizational assets in order to validate defensive capabilities.				X	
C036 Perform code reviews	CA.3.162				Employ a security assessment of enterprise software that has been developed internally, for internal use, and that has been organizationally defined as an area of risk.			X		
SITUATIONAL AWARENESS (SA)										
C037 Implement threat monitoring	SA.3.169			PM-16	Receive and respond to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders.			X		
	SA.4.171		3.11.2e	PM-16	Establish and maintain a cyber threat hunting capability to search for indicators of compromise in organizational systems and detect, track, and disrupt threats that evade existing controls.				X	
	SA.4.173			SI-4(24)	Design network and system security capabilities to leverage, integrate, and share indicators of compromise.				X	
SYSTEM AND COMMUNICATIONS PROTECTION (SC)										

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

III. CMMC Control MATRIX

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

SteelCloud

III. CMMC Control MATRIX

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