Applies To NIST 800-171 R2 & CMMC L2	Applies To NIST 800-171 R3	Applies To Both 171 R2 & R3	NCP SCRP Policy	NCP SCRP Standard #	NCP CSQP Procedure #	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US DFARS Cybersecurity	US FAR 52.204-21	US FAR 52.204-25	US FAR 52.204-27	US CMMC 2.0 Level 1	US CMMC 2.0 Level 1 AOs	US CMMC 2.0 Level 2	Conformity Validation Cadence	Evidence Request List (ERL) #
R2	R3	R2 & R3	Security, Compliance & Resilience Governance	GOV-01	P-GOV-01	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.			03.15.01.a	A.03.15.01.a[01]	252.204-7012(b)	52.204-21(b)(1)						Annual	E-GOV-01 E-GOV-02
	R3	R2 & R3	Security, Compliance & Resilience Governance	GOV-01.1	P-GOV-01.1	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.			03.12.03	A.03.12.03[01]								Annual	E-GOV-03 E-PRM-06
	R3	R2 & R3	Security, Compliance & Resilience Governance	GOV-01.2	P-GOV-01.2	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).			03.12.03	A.03.12.03[01]								Annual	E-CPL-05 E-CPL-09 E-GOV-03 E-GOV-04 E-GOV-05 E-GOV-06
R2	R3	R2 & R3	Security, Compliance & Resilience Governance	GOV-02	P-GOV-02	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.		3.4.9[a] 3.9.2[a]	03.15.01.a	A.03.15.01.a[01] A.03.15.01.a[02] A.03.15.01.a[03] A.03.15.01.a[04]	252.204-7012(b)	52.204-21(b)(1)						Annual	E-GOV-08 E-GOV-09 E-GOV-11
	R3	R2 & R3	Security, Compliance & Resilience Governance	GOV-03	P-GOV-03	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.			03.15.01.b 03.15.03.d	A.03.15.01.ODP[01] A.03.15.01.b[01] A.03.15.01.b[02] A.03.15.03.d[01]								Annual	E-GOV-12
R2	R3	R2 & R3	Security, Compliance & Resilience Governance	GOV-04	P-GOV-04	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).						52.204-21(b)(1)						Annual	E-HRS-01 E-HRS-05 E-HRS-06 E-HRS-07 E-HRS-08 E-HRS-09
R2	R3	R2 & R3	Security, Compliance & Resilience Governance	GOV-04.1	P-GOV-04.1	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.						52.204-21(b)(1)						Annual	E-HRS-15
	R3	R2 & R3	Security, Compliance & Resilience Governance	GOV-05	P-GOV-05	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.			03.12.03	A.03.12.03[01]								Annual	E-GOV-13
R2	R3	R2 & R3	Security, Compliance & Resilience Governance	GOV-15	P-GOV-15	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for each Technology Asset, Application and/or Service (TAAS) under their control.			03.15.01.a 03.16.01 03.17.01.a	A.03.15.01.a[03] A.03.16.01 A.03.17.01.a[01]	252.204-7012(b)	52.204-21(b)(1)						Annual	E-GOV-19
R2	R3	R2 & R3	Security, Compliance & Resilience Governance	GOV-15.1	P-GOV-15.1	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.			03.15.01.a 03.17.01.a	A.03.15.01.a[03] A.03.17.01.a[01]	252.204-7012(b) 252.204-7012(b)(2)(i) 252.204-7012(b)(2)(ii)(A) 252.204-7012(b)(3)							Annual	
R2	R3	R2 & R3	Security, Compliance & Resilience Governance	GOV-15.2	P-GOV-15.2	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.			03.15.01.a 03.17.01.a	A.03.15.01.a[03] A.03.17.01.a[01]	252.204-7012(b)							Annual	
R2	R3	R2 & R3	Security, Compliance & Resilience Governance	GOV-15.3	P-GOV-15.3	Assess Controls	GOV-15.3	Mechanisms exist to compel data and/or process owners to assess if required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control are: (1) Implemented correctly; and (2) Operating as intended.			03.15.01.a 03.17.01.a	A.03.15.01.a[03] A.03.17.01.a[01]	252.204-7012(b)							Annual	
R2	R3	R2 & R3	Security, Compliance & Resilience Governance	GOV-15.4	P-GOV-15.4	Authorize Technology Assets, Applications and/or Services (TAAS)	GOV-15.4	Mechanisms exist to compel data and/or process owners to obtain authorization for the production use of each Technology Asset, Application and/or Service (TAAS) under their control.			03.15.01.a 03.17.01.a	A.03.15.01.a[03] A.03.17.01.a[01]	252.204-7012(b)							Annual	
R2	R3	R2 & R3	Security, Compliance & Resilience Governance	GOV-15.5	P-GOV-15.5	Monitor Controls	GOV-15.5	Mechanisms exist to compel data and/or process owners to monitor Technology Assets, Applications, Services and/or Data (TAASD) under their control on an ongoing basis for applicable threats and risks, as well as to ensure security, compliance and resilience controls are operating as intended.			03.15.01.a 03.17.01.a	A.03.15.01.a[03] A.03.17.01.a[01]	252.204-7012(b)							Annual	
R2	R3	R2 & R3	Security, Compliance & Resilience Governance	GOV-17	P-GOV-17	Security, Compliance & Resilience Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.					252.204-7012(b)(2)(ii)(B)		52.204-25(d)(2)(i) 52.204-25(d)(2)(ii) 52.204-25(d)					Semi-Annual	E-GOV-17
R2	R3	R2 & R3	Asset Management	AST-01	P-AST-01	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	3.4.1 3.8.3		03.01.03 03.01.18.a 03.04.11.a 03.07.04.a	A.03.01.03[01] A.03.01.03[02] A.03.01.18.a[01] A.03.04.11.a[02] A.03.07.04.a[01]		52.204-21(b)(1)(vii)			MP.L1-B.1.VII		CML2.-3.4.1 MPL2.-3.8.3	Annual	E-AST-01
	R3	R2 & R3	Asset Management	AST-01.1	P-AST-01.1	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS) that support more than one critical business function.			03.01.03	A.03.01.03[02]								Annual	E-BCM-09
	R3	R2 & R3	Asset Management	AST-01.4	P-AST-01.4	Approved Technologies	AST-01.4	Mechanisms exist to maintain a current list of approved technologies (hardware and software).			03.04.08.c	A.03.04.08.c								Annual	
R2	R3	R2 & R3	Asset Management	AST-02	P-AST-02	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting;	3.4.1	3.4.1[d] 3.4.1[e] 3.4.1[f]	03.04.08.a 03.04.08.c 03.04.10.a 03.04.10.b 03.04.11.a	A.03.04.08.a A.03.04.08.c A.03.04.10.ODP[01] A.03.04.10.a A.03.04.10.b[01] A.03.04.10.b[02]						CML2.-3.4.1	Annual	E-AST-04 E-AST-05 E-AST-07 E-AST-28
R2	R3	R2 & R3	Asset Management	AST-02.1	P-AST-02.1	Updates During Installations / Removals	AST-02.1	Mechanisms exist to update asset inventories as part of component installations, removals and asset upgrades.		3.4.1[f]	03.04.10.a 03.04.10.b 03.04.10.c	A.03.04.10.a A.03.04.10.b[02] A.03.04.10.c[01] A.03.04.10.c[02] A.03.04.10.c[03]								Annual	
R2		R2 & R3	Asset Management	AST-02.3	P-AST-02.3	Component Duplication Avoidance	AST-02.3	Mechanisms exist to establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components that prevents assets from being duplicated in other asset inventories.	NFO - CM-8(5)											Annual	
	R3	R2 & R3	Asset Management	AST-02.4	P-AST-02.4	Approved Baseline Deviations	AST-02.4	Mechanisms exist to document and govern instances of approved deviations from established baseline configurations.			03.04.02.b 03.04.06.a	A.03.04.02.a[02] A.03.04.06.a								Annual	E-AST-33 E-RSK-03 E-TDA-14

Applies To NIST 800-171 R2 & CMMC L2	Applies To NIST 800-171 R3	Applies To Both 171 R2 & R3	NCP SCRP Policy	NCP SCRP Standard #	NCP CSOP Procedure #	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US DFARS Cybersecurity	US FAR 52.204-21	US FAR 52.204-25	US FAR 52.204-27	US CMMC 2.0 Level 1	US CMMC 2.0 Level 1 AOs	US CMMC 2.0 Level 2	Conformity Validation Cadence	Evidence Request List (ERL) #
	R3	R2 & R3	Asset Management	AST-02.8	P-AST-02.8	Data Action Mapping	AST-02.8	Mechanisms exist to create and maintain a map of Technology Assets, Applications and/or Services (TAAS) where sensitive and/or regulated data is stored, transmitted or processed.			03.04.11.a 03.04.11.b	A.03.04.11.a[01] A.03.04.11.a[02] A.03.04.11.a[03] A.03.04.11.b[01] A.03.04.11.b[02]								Semi-Annual	E-DCH-05
	R3	R2 & R3	Asset Management	AST-02.9	P-AST-02.9	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.			03.04.08.a 03.04.10.a 03.04.10.b	A.03.04.08.a A.03.04.10.a A.03.04.10.b[02]								Quarterly	
	R3	R2 & R3	Asset Management	AST-03	P-AST-03	Asset Ownership Assignment	AST-03	Mechanisms exist to ensure asset ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common understanding of requirements for asset protection.			03.09.02.a.03	A.03.09.02.a.03								Annual	E-AST-01 E-CPL-03
	R3	R2 & R3	Asset Management	AST-03.1	P-AST-03.1	Accountability Information	AST-03.1	Mechanisms exist to include capturing the name, position and/or role of individuals responsible/accountable for administering assets as part of the technology asset inventory process.			03.09.02.a.03	A.03.09.02.a.03								Annual	E-AST-01
	R3	R2 & R3	Asset Management	AST-04	P-AST-04	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive and/or regulated data flows.			03.01.03 03.04.11.a 03.04.11.b	A.03.01.03[02] A.03.04.11.a[02] A.03.04.11.b[01] A.03.04.11.b[02]								Annual	E-DCH-03 E-DCH-04 E-DCH-05
	R3	R2 & R3	Asset Management	AST-04.1	P-AST-04.1	Asset Scope Classification	AST-04.1	Mechanisms exist to determine security, compliance and resilience control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all Technology Assets, Applications and/or Services (TAAS) and personnel (internal and third-parties).			03.04.11.a 03.04.11.b	A.03.04.11.a[02] A.03.04.11.b[01] A.03.04.11.b[02]								Annual	E-AST-02 E-CPL-02 E-DCH-01 E-DCH-02
	R3	R2 & R3	Asset Management	AST-04.2	P-AST-04.2	Control Applicability Boundary Graphical Representation	AST-04.2	Mechanisms exist to ensure control applicability is appropriately-determined for Technology Assets, Applications and/or Services (TAAS) and third parties by graphically representing applicable boundaries.			03.04.11.a 03.04.11.b 03.15.02.a.04	A.03.04.11.a[02] A.03.04.11.b[01] A.03.04.11.b[02]								Annual	E-AST-02 E-CPL-02
	R3	R2 & R3	Asset Management	AST-04.3	P-AST-04.3	Compliance-Specific Asset Identification	AST-04.3	Mechanisms exist to create and maintain a current inventory of Technology Assets, Applications, Services and/or Data (TAASD) that are in scope for statutory, regulatory and/or contractual compliance obligations that provides sufficient detail to determine control applicability, based on asset scope categorization.			03.01.03	A.03.01.03[02]								Semi-Annual	E-AST-02 E-CPL-02
R2	R3	R2 & R3	Asset Management	AST-05	P-AST-05	Security of Assets & Media	AST-05	Mechanisms exist to maintain strict control over Technology Assets, Applications, Services and/or Data (TAASD) to ensure its confidentiality and integrity.	NFO - MP-1		03.07.04.a	A.03.07.04.a[02]								Annual	
R2	R3	R2 & R3	Asset Management	AST-09	P-AST-09	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	3.8.3		03.07.04.c 03.08.03	A.03.07.04.c A.03.08.03		52.204-21(b)(1)(vii)			MP.L1-B.1.VII		MPL2.-3.8.3	Annual	E-AST-03
	R3	R2 & R3	Asset Management	AST-10	P-AST-10	Return of Assets	AST-10	Mechanisms exist to ensure that employees and third-party users return all organizational assets in their possession upon termination of employment, contract or agreement.			03.09.02.a.03	A.03.09.02.a.03								Annual	E-AST-01
	R3	R2 & R3	Asset Management	AST-12	P-AST-12	Use of Personal Devices	AST-12	Mechanisms exist to restrict the possession and/or use of personally-owned Technology Assets, Applications and/or Services (TAAS) within organization-controlled facilities.			03.01.18.a	A.03.01.18.a[01]								Annual	
	R3	R2 & R3	Asset Management	AST-13	P-AST-13	Use of Third-Party Devices	AST-13	Mechanisms exist to reduce the risk associated with third-party assets that are attached to the network from harming organizational assets or exfiltrating organizational data.			03.01.18.a	A.03.01.18.a[01]								Annual	
	R3	R2 & R3	Asset Management	AST-14	P-AST-14	Usage Parameters	AST-14	Mechanisms exist to monitor and enforce usage parameters that limit the potential damage caused from the unauthorized or unintentional alteration of system parameters.			03.01.18.a	A.03.01.18.a[01]								Annual	
	R3	R2 & R3	Asset Management	AST-16	P-AST-16	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.			03.01.18.a	A.03.01.18.a[01]								Annual	
R2	R3	R2 & R3	Asset Management	AST-17	P-AST-17	Prohibited Equipment & Services	AST-17	Mechanisms exist to govern Supply Chain Risk Management (SCRM) sanctions that require the removal and prohibition of certain Technology Assets, Applications and/or Services (TAAS) that are designated as supply chain threats by a statutory or regulatory body.			03.11.01.a 03.16.01	A.03.11.01.a A.03.16.01			52.204-25(b)(1) 52.204-25(b)(2)	52.204-27(b)				Semi-Annual	E-AST-10
	R3	R2 & R3	Asset Management	AST-24	P-AST-24	Travel-Only Devices	AST-24	Mechanisms exist to issue personnel travelling overseas with temporary, loaner or "travel-only" end user technology (e.g., laptops and mobile devices) when travelling to authoritarian countries with a higher-than average risk for Intellectual Property (IP) theft or espionage against individuals and private companies.			03.04.12.a 03.04.12.b	A.03.04.12.a A.03.04.12.b								Annual	
	R3	R2 & R3	Asset Management	AST-25	P-AST-25	Re-Imaging Devices After Travel	AST-25	Mechanisms exist to re-image end user technology (e.g., laptops and mobile devices) when returning from overseas travel to an authoritarian country with a higher-than average risk for Intellectual Property (IP) theft or espionage against individuals and private companies.			03.04.12.b	A.03.04.12.b								Annual	
	R3	R2 & R3	Asset Management	AST-27	P-AST-27	Jump Server	AST-27	Mechanisms exist to conduct remote system administrative functions via a "jump box" or "jump server" that is located in a separate network zone to user workstations.			03.01.12.a 03.01.12.c	A.03.01.12.a[01] A.03.01.12.c[01] A.03.01.12.c[02]								Annual	
	R3	R2 & R3	Asset Management	AST-31	P-AST-31	Asset Categorization	AST-31	Mechanisms exist to categorize Technology Assets, Applications and/or Services (TAAS).			03.01.03	A.03.01.03[02]								Annual	E-AST-24
R2	R3	R2 & R3	Business Continuity & Disaster Recovery	BCD-01	P-BCD-01	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).												Annual	E-BCM-01
R2	R3	R2 & R3	Business Continuity & Disaster Recovery	BCD-11	P-BCD-11	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	3.8.9	3.8.9	03.08.09.a	A.03.08.09.a							MPL2.-3.8.9	Quarterly	E-BCM-10 E-BCM-11 E-BCM-12 E-BCM-13

Applies To NIST 800-171 R2 & CMMC L2	Applies To NIST 800-171 R3	Applies To Both 171 R2 & R3	NCP SCRP Policy	NCP SCRP Standard #	NCP CSQP Procedure #	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US DFARS Cybersecurity	US FAR 52.204-21	US FAR 52.204-25	US FAR 52.204-27	US CMMC 2.0 Level 1	US CMMC 2.0 Level 1 AOs	US CMMC 2.0 Level 2	Conformity Validation Cadence	Evidence Request List (ERL) #
R2	R3	R2 & R3	Business Continuity & Disaster Recovery	BCD-11.4	P-BCD-11.4	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	3.8.9	3.8.9	03.08.09.a 03.08.09.b	A.03.08.09.a A.03.08.09.b							MPL2.-3.8.9	Annual	E-BCM-16
R2	R3	R2 & R3	Change Management	CHG-01	P-CHG-01	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	3.4.3		03.04.02.b 03.04.03.a 03.04.03.d	A.03.04.02.b[01] A.03.04.03.a A.03.04.03.d[01] A.03.04.03.d[02]							CML2.-3.4.3	Annual	E-CHG-02
R2	R3	R2 & R3	Change Management	CHG-02	P-CHG-02	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	3.4.3	3.4.3[a] 3.4.3[b] 3.4.3[c] 3.4.3[d]	03.04.02.b 03.04.03.a 03.04.03.b 03.04.03.c 03.07.05.a	A.03.04.02.b[01] A.03.04.03.a A.03.04.03.b[02] A.03.04.03.c[01] A.03.07.05.a[01]							CML2.-3.4.3	Annual	E-CHG-02 E-CHG-05
	R3	R2 & R3	Change Management	CHG-02.1	P-CHG-02.1	Prohibition Of Changes	CHG-02.1	Mechanisms exist to prohibit unauthorized changes, unless organization-approved change requests are received.			03.04.02.b 03.04.03.a 03.04.03.b 03.07.05.a	A.03.04.02.b[01] A.03.04.03.a A.03.04.03.b[02] A.03.04.05[05] A.03.07.05.a[01]								Annual	E-CHG-02
R2	R3	R2 & R3	Change Management	CHG-02.2	P-CHG-02.2	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	NFO - CM-3(2)		03.04.03.b 03.04.03.c 03.04.04.a 03.04.11.b	A.03.04.03.b[02] A.03.04.03.c[02] A.03.04.04.a A.03.04.11.b[01] A.03.04.11.b[02]								Annual	E-CHG-03 E-CHG-05
	R3	R2 & R3	Change Management	CHG-02.3	P-CHG-02.3	Security, Compliance & Resilience Representative for Asset Lifecycle Changes	CHG-02.3	Mechanisms exist to include a cybersecurity and/or data protection representative in the configuration change control review process.			03.04.04.a	A.03.04.04.a								Annual	E-CHG-04
R2	R3	R2 & R3	Change Management	CHG-03	P-CHG-03	Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	3.4.4	3.4.4	03.04.03.b 03.04.04.a 03.04.11.b	A.03.04.03.b[01] A.03.04.04.a A.03.04.11.b[01] A.03.04.11.b[02]							CML2.-3.4.4	Annual	E-CHG-04
R2	R3	R2 & R3	Change Management	CHG-04	P-CHG-04	Access Restriction For Change	CHG-04	Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	3.4.5	3.4.5[a] 3.4.5[b] 3.4.5[c] 3.4.5[d] 3.4.5[e] 3.4.5[f]	03.04.02.b 03.04.05	A.03.04.02.b[01] A.03.04.05[06]							CML2.-3.4.5	Annual	E-HRS-13 E-IAM-02
	R3	R2 & R3	Change Management	CHG-04.4	P-CHG-04.4	Permissions To Implement Changes	CHG-04.4	Mechanisms exist to limit operational privileges for implementing changes.			03.04.05	A.03.04.05[06]								Annual	
R2	R3	R2 & R3	Change Management	CHG-05	P-CHG-05	Stakeholder Notification of Changes	CHG-05	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	NFO - CM-9		03.04.11.b	A.03.04.11.b[01] A.03.04.11.b[02]								Annual	E-CHG-06
	R3	R2 & R3	Change Management	CHG-06	P-CHG-06	Control Functionality Verification	CHG-06	Mechanisms exist to verify the functionality of security, compliance and resilience controls following implemented changes to ensure applicable controls operate as designed.			03.04.04.b	A.03.04.04.b								Annual	
R2	R3	R2 & R3	Cloud Security	CLD-01	P-CLD-01	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	3.1.22 NFO-PL-8					52.204-21(b)(1)(iv)			AC.L1-B.1.IV		AC.L2.-3.1.22	Annual	E-AST-06
R2	R3	R2 & R3	Cloud Security	CLD-02	P-CLD-02	Cloud Security Architecture	CLD-02	Mechanisms exist to ensure the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud employments.	3.1.22 NFO-PL-8					52.204-21(b)(1)(iv)			AC.L1-B.1.IV		AC.L2.-3.1.22	Annual	E-TDA-09
R2		R2 & R3	Cloud Security	CLD-03	P-CLD-03	Cloud Infrastructure Security Subnet	CLD-03	Mechanisms exist to host security-specific technologies in a dedicated subnet.	3.13.2 NFO-PL-8										SCL2.-3.13.2	Annual	
R2	R3	R2 & R3	Cloud Security	CLD-06	P-CLD-06	Multi-Tenant Environments	CLD-06	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	3.1.22	3.1.22[a] 3.1.22[b] 3.1.22[c] 3.1.22[d] 3.1.22[e]				52.204-21(b)(1)(iv)			AC.L1-B.1.IV		AC.L2.-3.1.22	Annual	
R2	R3	R2 & R3	Cloud Security	CLD-10	P-CLD-10	Sensitive Data In Public Cloud Providers	CLD-10	Mechanisms exist to limit and manage the storage of sensitive and/or regulated data in public cloud providers.	3.1.22	3.1.22[a] 3.1.22[b] 3.1.22[c] 3.1.22[d] 3.1.22[e]				52.204-21(b)(1)(iv)			AC.L1-B.1.IV		AC.L2.-3.1.22	Annual	E-AST-08
R2	R3	R2 & R3	Compliance	CPL-01	P-CPL-01	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	NFO - PL-1		03.04.11.a 03.12.01	A.03.04.11.a[01] A.03.12.01	252.204-7012(b)(1)(i) 252.204-7012(b)(1)(ii) 252.204-7012(k)							Semi-Annual	E-CPL-01 E-GOV-10
	R3	R2 & R3	Compliance	CPL-01.1	P-CPL-01.1	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.			03.12.02.a.01 03.12.02.a.02	A.03.12.02.a.01 A.03.12.02.a.02								Semi-Annual	E-CPL-05
	R3	R2 & R3	Compliance	CPL-01.2	P-CPL-01.2	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of security, compliance and resilience controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.			03.04.11.a 03.15.02.a.04	A.03.04.11.a[01]								Semi-Annual	E-AST-02 E-CPL-02 E-GOV-10
R2	R3	R2 & R3	Compliance	CPL-02	P-CPL-02	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	3.12.1 3.12.3	3.12.1[a] 3.12.1[b] 3.12.3	03.12.01 03.12.03	A.03.12.01 A.03.12.03[01] A.03.12.03[03] A.03.12.03[04]							CAL2.-3.12.1 CAL2.-3.12.3	Annual	E-CPL-07 E-CPL-09 E-GOV-04 E-GOV-05 E-GOV-06 E-GOV-13
R2	R3	R2 & R3	Compliance	CPL-02.1	P-CPL-02.1	Internal Audit Function	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	3.12.1		03.12.01	A.03.12.01.ODP[01] A.03.12.01							CAL2.-3.12.1	Annual	E-CPL-04 E-CPL-07
R2	R3	R2 & R3	Compliance	CPL-03	P-CPL-03	Security, Compliance & Resilience Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	3.12.1		03.12.01 03.12.03	A.03.12.01 A.03.12.03[01]							CAL2.-3.12.1	Semi-Annual	E-CPL-05 E-CPL-07

Applies To NIST 800-171 R2 & CMMC L2	Applies To NIST 800-171 R3	Applies To Both 171 R2 & R3	NCP SCRP Policy	NCP SCRP Standard #	NCP CSOP Procedure #	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US DFARS Cybersecurity	US FAR 52.204-21	US FAR 52.204-25	US FAR 52.204-27	US CMMC 2.0 Level 1	US CMMC 2.0 Level 1 AOs	US CMMC 2.0 Level 2	Conformity Validation Cadence	Evidence Request List (ERL) #
R2		R2 & R3	Compliance	CPL-03.1	P-CPL-03.1	Independent Assessors	CPL-03.1	Mechanisms exist to utilize independent assessors to evaluate security, compliance and resilience at planned intervals or when the Technology Asset, Application and/or Service (TAAS) undergoes significant changes.	NFO - CA-7(1)											Annual	E-CPL-07
	R3	R2 & R3	Compliance	CPL-03.2	P-CPL-03.2	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.			03.04.02.b 03.04.08.c 03.12.03	A.03.04.02.b[01] A.03.04.08.c A.03.12.03[02]								Quarterly	E-CPL-08
R2	R3	R2 & R3	Configuration Management	CFG-01	P-CFG-01	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	NFO - CM-1 NFO - CM-9		03.04.01.a 03.04.03.a	A.03.04.01.a[02] A.03.04.03.a								Annual	E-AST-01 E-AST-27
R2	R3	R2 & R3	Configuration Management	CFG-02	P-CFG-02	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	3.3.3 3.4.1 3.4.2	3.4.1[a] 3.4.1[b] 3.4.1[c] 3.4.2[a] 3.4.2[b]	03.01.01.h 03.01.03 03.01.08.a 03.01.08.b 03.01.09	A.03.01.01.h A.03.01.03[01] A.03.01.03[02] A.03.01.08.a A.03.01.08.b A.03.01.09						AUL2.-3.3.3 CML2.-3.4.1 CML2.-3.4.2	Annual	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17
R2	R3	R2 & R3	Configuration Management	CFG-02.1	P-CFG-02.1	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and upgrades.	3.3.3 NFO - CM-2(1)		03.04.01.b 03.04.06.c	A.03.04.01.ODP[01] A.03.04.01.b[01] A.03.04.01.b[02] A.03.04.01.b[03] A.03.04.01.b[04] A.03.04.06.c						AUL2.-3.3.3	Annual	E-AST-12
	R3	R2 & R3	Configuration Management	CFG-02.2	P-CFG-02.2	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar technologies.			03.04.02.b 03.04.03.d 03.13.13.b	A.03.04.02.b[01] A.03.04.03.d[01] A.03.04.03.d[02] A.03.13.13.b[02]								Quarterly	
R2	R3	R2 & R3	Configuration Management	CFG-02.5	P-CFG-02.5	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	NFO - CM-2(7)		03.04.01.a 03.04.02.a 03.04.06.a 03.04.06.d 03.04.12.a	A.03.04.01.a[01] A.03.04.02.a[01] A.03.04.06.a A.03.04.06.d A.03.04.12.ODP[01] A.03.04.12.ODP[02]								Annual	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17
	R3	R2 & R3	Configuration Management	CFG-02.7	P-CFG-02.7	Approved Configuration Deviations	CFG-02.7	Mechanisms exist to document, assess risk and approve or deny deviations to standardized configurations.			03.04.01.a 03.04.02.b	A.03.04.01.a[01] A.03.04.02.b[02]								Annual	E-AST-33
R2	R3	R2 & R3	Configuration Management	CFG-02.9	P-CFG-02.9	Baseline Tailoring	CFG-02.9	Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to: (1) Mission / business functions; (2) Operational environment; (3) Specific threats or vulnerabilities; or (4) Other conditions or situations that could affect mission / business success.	3.3.3		03.03.02.b 03.04.01.a 03.04.02.a 03.04.02.b 03.04.06.a 03.04.08.a	A.03.03.02.b A.03.04.01.a[01] A.03.04.02.a[01] A.03.04.02.b[01] A.03.04.06.a A.03.04.08.a						AUL2.-3.3.3	Annual	E-AST-33 E-GOV-20
R2	R3	R2 & R3	Configuration Management	CFG-03	P-CFG-03	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	3.4.6	3.4.6[a] 3.4.6[b]	03.04.02.a 03.04.06.a 03.04.06.b 03.04.06.d 03.04.08.a	A.03.04.02.ODP[01] A.03.04.02.a[01] A.03.04.06.a A.03.04.06.b[01] A.03.04.06.b[02] A.03.04.06.b[03]						CML2.-3.4.6	Annual	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17
R2	R3	R2 & R3	Configuration Management	CFG-03.1	P-CFG-03.1	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	3.4.7	3.4.7[a] 3.4.7[b] 3.4.7[c] 3.4.7[d] 3.4.7[e] 3.4.7[f]	03.04.06.c 03.04.08.c	A.03.04.06.ODP[06] A.03.04.06.c A.03.04.08.c						CML2.-3.4.7	Annual	
R2	R3	R2 & R3	Configuration Management	CFG-03.2	P-CFG-03.2	Prevent Unauthorized Software Execution	CFG-03.2	Mechanisms exist to configure systems to prevent the execution of unauthorized software programs.	3.4.7		03.04.08.b	A.03.04.08.b						CML2.-3.4.7	Annual	E-AST-20 E-AST-21
R2	R3	R2 & R3	Configuration Management	CFG-03.3	P-CFG-03.3	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	3.4.8	3.4.8[a] 3.4.8[b] 3.4.8[c]	03.04.08.a 03.04.08.b 03.13.13.a 03.13.13.b	A.03.04.08.ODP[01] A.03.04.08.a A.03.04.08.b A.03.13.13.a[01] A.03.13.13.a[02] A.03.13.13.b[01]						CML2.-3.4.8	Annual	E-AST-31
R2		R2 & R3	Configuration Management	CFG-03.4	P-CFG-03.4	Split Tunneling	CFG-03.4	Mechanisms exist to prevent split tunneling for remote devices unless the split tunnel is securely provisioned using organization-defined safeguards.	3.13.7	3.13.7								SCL2.-3.13.7	Annual	
	R3	R2 & R3	Configuration Management	CFG-04	P-CFG-04	Software Usage Restrictions	CFG-04	Mechanisms exist to enforce software usage restrictions to comply with applicable contract agreements and copyright laws.			03.13.13.b	A.03.13.13.a[02] A.03.13.13.b[01] A.03.13.13.b[03]								Annual	
	R3	R2 & R3	Configuration Management	CFG-04.1	P-CFG-04.1	Open Source Software	CFG-04.1	Mechanisms exist to establish parameters for the secure use of open source software.			03.13.13.b	A.03.13.13.a[02] A.03.13.13.b[03]								Annual	
R2	R3	R2 & R3	Configuration Management	CFG-05	P-CFG-05	User-Installed Software	CFG-05	Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software.	3.4.9	3.4.9[b] 3.4.9[c]	03.13.13.b	A.03.13.13.a[02] A.03.13.13.b[03]						CML2.-3.4.9	Annual	E-AST-01 E-AST-21 E-IAM-02
	R3	R2 & R3	Configuration Management	CFG-06	P-CFG-06	Configuration Enforcement	CFG-06	Automated mechanisms exist to monitor, enforce and report on configurations for endpoint devices.			03.04.02.a 03.04.02.b 03.04.03.a	A.03.04.02.a[01] A.03.04.02.b[01] A.03.04.03.a								Quarterly	
	R3	R2 & R3	Configuration Management	CFG-08	P-CFG-08	Sensitive / Regulated Data Access Enforcement	CFG-08	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to restrict access to sensitive and/or regulated data.			03.01.02	A.03.01.02[01] A.03.01.02[02]								Annual	E-DCH-08
R2	R3	R2 & R3	Continuous Monitoring	MON-01	P-MON-01	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	3.3.3 3.14.6 NFO - AU-1		03.03.01.a 03.12.03 03.14.06.a 03.14.06.a.02	A.03.03.01.a A.03.12.03[01] A.03.14.06.a.01[01] A.03.14.06.a.01[02] A.03.14.06.a.02						AUL2.-3.3.3 SIL2.-3.14.6	Annual	E-MON-01 E-MON-06 E-MON-07
	R3	R2 & R3	Continuous Monitoring	MON-01.1	P-MON-01.1	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.			03.13.01.a	A.03.13.01.a[01]								Annual	E-MON-01 E-MON-06 E-MON-07
R2	R3	R2 & R3	Continuous Monitoring	MON-01.3	P-MON-01.3	Inbound & Outbound Communications Traffic	MON-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	3.14.6	3.14.6[a] 3.14.6[b] 3.14.6[c]	03.13.01.a 03.14.06.c	A.03.13.01.a[01] A.03.13.01.a[03] A.03.14.06.b A.03.14.06.c[01]						SIL2.-3.14.6	Semi-Annual	E-MON-01 E-MON-06 E-MON-07

Applies To NIST 800-171 R2 & CMMC L2	Applies To NIST 800-171 R3	Applies To Both 171 R2 & R3	NCP SCRP Policy	NCP SCRP Standard #	NCP CSOP Procedure #	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US DFARS Cybersecurity	US FAR 52.204-21	US FAR 52.204-25	US FAR 52.204-27	US CMMC 2.0 Level 1	US CMMC 2.0 Level 1 AOs	US CMMC 2.0 Level 2	Conformity Validation Cadence	Evidence Request List (ERL) #
R2	R3	R2 & R3	Continuous Monitoring	MON-01.4	P-MON-01.4	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	NFO - SI-4(5)		03.03.01.a 03.03.03.a 03.14.06.a.01 03.14.06.b 03.14.06.c	A.03.03.01.a A.03.03.03.a A.03.14.06.a.01[01] A.03.14.06.a.01[02] A.03.14.06.b									Semi-Annual	E-END-03 E-MON-01 E-MON-06 E-MON-07
R2	R3	R2 & R3	Continuous Monitoring	MON-01.8	P-MON-01.8	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	3.3.3 3.14.3	3.3.3[a] 3.3.3[b] 3.3.3[c] 3.14.3[a] 3.14.3[b] 3.14.3[c]	03.03.05.a	A.03.03.01.ODP[02] A.03.03.05.ODP[01] A.03.03.05.a							AUL2.-3.3.3 SIL2.-3.14.3	Annual	E-MON-01 E-MON-02 E-MON-05
	R3	R2 & R3	Continuous Monitoring	MON-01.12	P-MON-01.12	Automated Alerts	MON-01.12	Mechanisms exist to automatically alert incident response personnel to inappropriate or anomalous activities that have potential security incident implications.			03.03.04.a 03.03.05.b	A.03.03.05.b									Annual	E-MON-06
	R3	R2 & R3	Continuous Monitoring	MON-01.15	P-MON-01.15	Privileged User Oversight	MON-01.15	Mechanisms exist to implement enhanced activity monitoring for privileged users.			03.01.07.b	A.03.01.07.b									Annual	E-MON-03
R2		R2 & R3	Continuous Monitoring	MON-01.16	P-MON-01.16	Analyze and Prioritize Monitoring Requirements	MON-01.16	Mechanisms exist to assess the organization's needs for monitoring and prioritize the monitoring of Technology Assets, Applications and/or Services (TAAS), based on TAAS criticality and the sensitivity of the data it stores, transmits and processes.	3.3.3										AUL2.-3.3.3	Annual	E-AST-30
R2	R3	R2 & R3	Continuous Monitoring	MON-02	P-MON-02	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	3.3.1 3.3.3 3.3.5 3.3.6 3.3.8 3.3.9		03.03.05.a 03.03.05.c	A.03.03.05.ODP[01] A.03.03.05.a A.03.03.05.c[01]							AUL2.-3.3.1 AUL2.-3.3.3 AUL2.-3.3.5 AUL2.-3.3.6 AUL2.-3.3.8 AUL2.-3.3.9	Annual	E-MON-01 E-MON-05
R2	R3	R2 & R3	Continuous Monitoring	MON-02.1	P-MON-02.1	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	3.3.5 3.14.7	3.3.5[a] 3.3.5[b] 3.14.7[a] 3.14.7[b]	03.03.05.a 03.03.05.c	A.03.03.05.a A.03.03.05.c[02]							AUL2.-3.3.5 SIL2.-3.14.7	Quarterly	E-MON-05 E-MON-07
	R3	R2 & R3	Continuous Monitoring	MON-02.2	P-MON-02.2	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.			03.03.05.a 03.03.05.c	A.03.03.05.a A.03.03.05.c[01]									Quarterly	E-MON-01 E-MON-02 E-MON-05
	R3	R2 & R3	Continuous Monitoring	MON-02.3	P-MON-02.3	Integration of Scanning & Other Monitoring Information	MON-02.3	Automated mechanisms exist to integrate the analysis of audit records with analysis of vulnerability scanners, network performance, system monitoring and other sources to further enhance the ability to identify inappropriate or unusual activity.			03.03.05.c	A.03.03.05.c[02]									Quarterly	
	R3	R2 & R3	Continuous Monitoring	MON-02.6	P-MON-02.6	Audit Level Adjustments	MON-02.6	Mechanisms exist to adjust the level of audit review, analysis and reporting based on evolving threat information from law enforcement, industry associations or other credible sources of threat intelligence.			03.03.01.b	A.03.03.01.b[01]									Annual	
	R3	R2 & R3	Continuous Monitoring	MON-02.7	P-MON-02.7	System-Wide / Time-Correlated Audit Trail	MON-02.7	Automated mechanisms exist to compile audit records into an organization-wide audit trail that is time-correlated.			03.03.01.a	A.03.03.01.a									Quarterly	
R2	R3	R2 & R3	Continuous Monitoring	MON-03	P-MON-03	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event;	3.3.2	3.3.1[a] 3.3.1[b] 3.3.1[d] 3.3.2[a] 3.3.2[b]	03.03.01.a 03.03.02.a 03.03.02.a.01 03.03.02.a.02 03.03.02.a.03 03.03.02.a.04	A.03.03.01.ODP[01] A.03.03.01.a A.03.03.02.a.01 A.03.03.02.a.02 A.03.03.02.a.03 A.03.03.02.a.04						AUL2.-3.3.2	Annual	E-AST-01 E-CPL-01
R2		R2 & R3	Continuous Monitoring	MON-03.1	P-MON-03.1	Sensitive Event Log Information	MON-03.1	Mechanisms exist to protect sensitive and/or regulated data contained in log files.	3.3.8										AUL2.-3.3.8	Annual	
R2	R3	R2 & R3	Continuous Monitoring	MON-03.2	P-MON-03.2	Audit Trails	MON-03.2	Mechanisms exist to link system access to individual users or service accounts.		3.3.1[c] 3.3.2[a]	03.03.01.a	A.03.03.01.a									Annual	E-MON-09
	R3	R2 & R3	Continuous Monitoring	MON-03.3	P-MON-03.3	Privileged Functions Logging	MON-03.3	Mechanisms exist to log and review the actions of users and/or services with elevated privileges.			03.01.07.b	A.03.01.07.b									Annual	MON-03.2
	R3	R2 & R3	Continuous Monitoring	MON-03.6	P-MON-03.6	Centralized Management of Event Log Content	MON-03.6	Mechanisms exist to centrally manage and update the criteria to be captured in event logs generated by organization-defined system components.			03.03.01.b	A.03.03.01.b[01] A.03.03.01.b[02]									Annual	
R2		R2 & R3	Continuous Monitoring	MON-03.7	P-MON-03.7	Database Logging	MON-03.7	Mechanisms exist to ensure databases produce audit records that contain sufficient information to monitor database activities.		3.3.2[a]											Annual	
R2	R3	R2 & R3	Continuous Monitoring	MON-05	P-MON-05	Response To Event Log Processing Failures	MON-05	Mechanisms exist to alert appropriate personnel in the event of a log processing failure and take actions to remedy the disruption.	3.3.4	3.3.4[a] 3.3.4[b] 3.3.4[c]	03.03.04.b	A.03.03.04.ODP[01] A.03.03.04.ODP[02] A.03.03.04.a A.03.03.04.b							AUL2.-3.3.4	Annual	E-MON-10
R2	R3	R2 & R3	Continuous Monitoring	MON-06	P-MON-06	Monitoring Reporting	MON-06	Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.	3.3.6	3.3.6[a] 3.3.6[b]	03.03.05.b 03.03.06.a	A.03.03.05.b A.03.03.06.a[01] A.03.03.06.a[02] A.03.03.06.a[03] A.03.03.06.a[04]							AUL2.-3.3.6	Annual	
R2	R3	R2 & R3	Continuous Monitoring	MON-07	P-MON-07	Time Stamps	MON-07	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to use an authoritative time source to generate time stamps for event logs.		3.3.7[a] 3.3.7[b]	03.03.02.a.02 03.03.07.a	A.03.03.02.a.02 A.03.03.07.ODP[01] A.03.03.07.a A.03.03.07.b[01]								Annual	
R2	R3	R2 & R3	Continuous Monitoring	MON-07.1	P-MON-07.1	Synchronization With Authoritative Time Source	MON-07.1	Mechanisms exist to synchronize internal system clocks with an authoritative time source.	3.3.7	3.3.7[b] 3.3.7[c]	03.03.07.b	A.03.03.07.b[02]							AUL2.-3.3.7	Annual	
R2	R3	R2 & R3	Continuous Monitoring	MON-08	P-MON-08	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	3.3.8	3.3.8[a] 3.3.8[b] 3.3.8[c] 3.3.8[d] 3.3.8[e] 3.3.8[f]	03.03.03.b 03.03.06.b 03.03.08.a 03.03.08.b	A.03.03.03.b A.03.03.06.b[01] A.03.03.06.b[02] A.03.03.08.a[01] A.03.03.08.b							AUL2.-3.3.8	Annual	

Applies To NIST 800-171 R2 & CMMC L2	Applies To NIST 800-171 R3	Applies To Both 171 R2 & R3	NCP SCRP Policy	NCP SCRP Standard #	NCP CSOP Procedure #	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US DFARS Cybersecurity	US FAR 52.204-21	US FAR 52.204-25	US FAR 52.204-27	US CMMC 2.0 Level 1	US CMMC 2.0 Level 1 AOs	US CMMC 2.0 Level 2	Conformity Validation Cadence	Evidence Request List (ERL) #
	R3	R2 & R3	Continuous Monitoring	MON-08.1	P-MON-08.1	Event Log Backup on Separate Physical Systems / Components	MON-08.1	Mechanisms exist to back up event logs onto a physically different system or system component than the Security Incident Event Manager (SIEM) or similar automated tool.			03.03.08.a	A.03.03.08.a[01]								Annual	
R2	R3	R2 & R3	Continuous Monitoring	MON-08.2	P-MON-08.2	Access by Subset of Privileged Users	MON-08.2	Mechanisms exist to restrict access to the management of event logs to privileged users with a specific business need.	3.3.9	3.3.9[a] 3.3.9[b]	03.03.08.a 03.03.08.b	A.03.03.08.a[01] A.03.03.08.b							AUL2.-3.3.9	Annual	
	R3	R2 & R3	Continuous Monitoring	MON-08.3	P-MON-08.3	Cryptographic Protection of Event Log Information	MON-08.3	Cryptographic mechanisms exist to protect the integrity of event logs and audit tools.			03.03.08.a	A.03.03.08.a[01]								Annual	
R2	R3	R2 & R3	Continuous Monitoring	MON-10	P-MON-10	Event Log Retention	MON-10	Mechanisms exist to retain event logs for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	3.3.1	3.3.1[e] 3.3.1[f]	03.03.03.b	A.03.03.03.b							AUL2.-3.3.1	Semi-Annual	E-AST-11
	R3	R2 & R3	Continuous Monitoring	MON-11	P-MON-11	Monitoring For Information Disclosure	MON-11	Mechanisms exist to monitor for evidence of unauthorized exfiltration or disclosure of non-public information.			03.01.22.b	A.03.01.22.b[01]								Annual	
R2	R3	R2 & R3	Continuous Monitoring	MON-11.3	P-MON-11.3	Monitoring for Indicators of Compromise (IOC)	MON-11.3	Automated mechanisms exist to identify and alert on Indicators of Compromise (IoC).	3.14.7		03.14.06.a.01 03.14.06.a.02 03.14.06.b 03.14.06.c	A.03.14.06.a.01[01] A.03.14.06.a.01[02] A.03.14.06.a.02 A.03.14.06.b							SIL2.-3.14.7	Quarterly	E-IRO-02 E-MON-07
R2	R3	R2 & R3	Continuous Monitoring	MON-16	P-MON-16	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	3.14.7		03.01.01.e 03.03.05.a 03.14.06.a.01 03.14.06.a.02 03.14.06.b 03.14.06.c	A.03.01.01.e A.03.03.05.a A.03.14.06.a.01[01] A.03.14.06.a.01[02] A.03.14.06.a.02 A.03.14.06.b							SIL2.-3.14.7	Semi-Annual	E-IRO-02 E-MON-07
R2	R3	R2 & R3	Cryptographic Protections	CRY-01	P-CRY-01	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	3.13.11	3.13.8[a] 3.13.11	03.13.08 03.13.11	A.03.13.08[01] A.03.13.08[02] A.03.13.11.ODP[01] A.03.13.11							SCL2.-3.13.11	Annual	E-CRY-01
R2	R3	R2 & R3	Cryptographic Protections	CRY-01.1	P-CRY-01.1	Alternate Physical Protection	CRY-01.1	Cryptographic mechanisms exist to prevent unauthorized disclosure of information as an alternative to physical safeguards.	3.8.6 3.13.8	3.13.8[b] 3.13.8[c]	03.13.08	A.03.13.08[02]							MPL2.-3.8.6 SCL2.-3.13.8	Annual	E-GOV-18
	R3	R2 & R3	Cryptographic Protections	CRY-01.5	P-CRY-01.5	Cryptographic Cipher Suites and Protocols Inventory	CRY-01.5	Mechanisms exist to identify, document and review deployed cryptographic cipher suites and protocols to proactively respond to industry trends regarding the continued viability of utilized cryptographic cipher suites and protocols.			03.13.11	A.03.13.11								Semi-Annual	
R2	R3	R2 & R3	Cryptographic Protections	CRY-03	P-CRY-03	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	3.13.8	3.13.8[a] 3.13.11	03.13.08 03.13.11	A.03.13.08[01] A.03.13.11.ODP[01] A.03.13.11							SCL2.-3.13.8	Annual	E-CRY-01
R2		R2 & R3	Cryptographic Protections	CRY-04	P-CRY-04	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	NFO - SI-1											Annual	E-CRY-01
R2	R3	R2 & R3	Cryptographic Protections	CRY-05	P-CRY-05	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	3.8.6 3.13.16	3.8.6	03.13.08 03.13.11	A.03.13.08[02] A.03.13.11.ODP[01] A.03.13.11							MPL2.-3.8.6 SCL2.-3.13.16	Annual	E-CRY-01
	R3	R2 & R3	Cryptographic Protections	CRY-05.1	P-CRY-05.1	Storage Media	CRY-05.1	Cryptographic mechanisms exist to protect the confidentiality and integrity of sensitive and/or regulated data residing on storage media.			03.13.08	A.03.13.08[02]								Annual	
	R3	R2 & R3	Cryptographic Protections	CRY-07	P-CRY-07	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.			03.01.16.a	A.03.01.16.a[02]								Annual	
R2	R3	R2 & R3	Cryptographic Protections	CRY-08	P-CRY-08	Public Key Infrastructure (PKI)	CRY-08	Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider.	3.13.10	3.13.10[a] 3.13.10[b]	03.13.10	A.03.13.10[01]							SCL2.-3.13.10	Annual	
R2	R3	R2 & R3	Cryptographic Protections	CRY-09	P-CRY-09	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	3.13.10	3.13.10[a] 3.13.10[b]	03.13.10	A.03.13.10.ODP[01] A.03.13.10[01] A.03.13.10[02]							SCL2.-3.13.10	Annual	E-CRY-01 E-CRY-02
	R3	R2 & R3	Cryptographic Protections	CRY-09.3	P-CRY-09.3	Cryptographic Key Loss or Change	CRY-09.3	Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users.			03.13.10	A.03.13.10[02]								Annual	
	R3	R2 & R3	Cryptographic Protections	CRY-09.4	P-CRY-09.4	Control & Distribution of Cryptographic Keys	CRY-09.4	Mechanisms exist to facilitate the secure distribution of symmetric and asymmetric cryptographic keys using industry recognized key management technology and processes.			03.13.10	A.03.13.10[02]								Annual	
R2	R3	R2 & R3	Data Classification & Handling	DCH-01	P-DCH-01	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	3.8.1 3.8.3 NFO - MP-1	3.8.1[a] 3.8.1[b] 3.8.1[c] 3.8.1[d]	03.01.01.d.01 03.01.01.d.02 03.08.01	A.03.01.01.d.01 A.03.01.01.d.02 A.03.08.01[01] A.03.08.01[02]		52.204-21(b)(1) 52.204-21(b)(1)(vii)			MP.L1-B.1.VII		MPL2.-3.8.1 MPL2.-3.8.3	Annual	E-CRY-01
	R3	R2 & R3	Data Classification & Handling	DCH-01.1	P-DCH-01.1	Data Stewardship	DCH-01.1	Mechanisms exist to ensure data stewardship is assigned, documented and communicated.			03.08.01 03.08.05.a	A.03.08.01[01] A.03.08.01[02] A.03.08.05.a[01]								Annual	E-DCH-02 E-DCH-09
R2	R3	R2 & R3	Data Classification & Handling	DCH-01.2	P-DCH-01.2	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive and/or regulated data wherever it is processed and/or stored.	3.10.6		03.01.01.d.01 03.01.01.d.02 03.01.02 03.01.20.a 03.01.20.b 03.01.20.c.01	A.03.01.01.d.01 A.03.01.01.d.02 A.03.01.02[01] A.03.01.02[02] A.03.01.20.a A.03.01.20.b		52.204-21(b)(1)					PEL2.-3.10.6	Annual	E-CRY-01 E-DCH-02 E-DCH-09

Applies To NIST 800-171 R2 & CMMC L2	Applies To NIST 800-171 R3	Applies To Both 171 R2 & R3	NCP SCRP Policy	NCP SCRP Standard #	NCP CSOP Procedure #	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US DFARS Cybersecurity	US FAR 52.204-21	US FAR 52.204-25	US FAR 52.204-27	US CMMC 2.0 Level 1	US CMMC 2.0 Level 1 AOs	US CMMC 2.0 Level 2	Conformity Validation Cadence	Evidence Request List (ERL) #
	R3	R2 & R3	Data Classification & Handling	DCH-01.3	P-DCH-01.3	Sensitive / Regulated Media Records	DCH-01.3	Mechanisms exist to ensure media records for sensitive and/or regulated data contain sufficient information to determine the potential impact in the event of a data loss incident.			03.08.05.c	A.03.08.05.c									Annual	E-AST-08
	R3	R2 & R3	Data Classification & Handling	DCH-01.4	P-DCH-01.4	Defining Access Authorizations for Sensitive / Regulated Data	DCH-01.4	Mechanisms exist to explicitly define authorizations for specific individuals and/or roles for logical and /or physical access to sensitive and/or regulated data.			03.01.02 03.01.03 03.01.04.b 03.08.01 03.08.02 03.10.01.a	A.03.01.02[01] A.03.01.02[02] A.03.01.03[01] A.03.01.03[02] A.03.01.04.a A.03.08.01[01]									Annual	E-DCH-02 E-DCH-08
	R3	R2 & R3	Data Classification & Handling	DCH-02	P-DCH-02	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.			03.04.11.a 03.08.01 03.08.04	A.03.04.11.a[02] A.03.08.01[01] A.03.08.01[02] A.03.08.04[01]									Semi-Annual	E-DCH-01 E-DCH-02
R2	R3	R2 & R3	Data Classification & Handling	DCH-03	P-DCH-03	Media Access	DCH-03	Mechanisms exist to control and restrict access to digital and non-digital media to authorized individuals.	3.1.3 3.8.2	3.1.3[c] 3.8.2	03.01.03 03.08.01 03.08.02	A.03.01.03[01] A.03.01.03[02] A.03.08.01[01] A.03.08.01[02] A.03.08.02							ACL2.-3.1.3 MPL2.-3.8.2	Annual	E-IAM-02
	R3	R2 & R3	Data Classification & Handling	DCH-03.1	P-DCH-03.1	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive and/or regulated data to authorized parties with a need to know.			03.01.22.a 03.15.02.c 03.17.01.c	A.03.01.22.a A.03.15.02.c A.03.17.01.c									Annual	
R2	R3	R2 & R3	Data Classification & Handling	DCH-04	P-DCH-04	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	3.8.4	3.8.4[a] 3.8.4[b]	03.08.04	A.03.08.04[01] A.03.08.04[02] A.03.08.04[03]							MPL2.-3.8.4	Annual	
R2	R3	R2 & R3	Data Classification & Handling	DCH-06	P-DCH-06	Media Storage	DCH-06	Mechanisms exist to: (1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and (2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures.	3.8.1		03.08.01	A.03.08.01[01] A.03.08.01[02]							MPL2.-3.8.1	Annual	E-DCH-02 E-DCH-13
	R3	R2 & R3	Data Classification & Handling	DCH-06.1	P-DCH-06.1	Physically Secure All Media	DCH-06.1	Mechanisms exist to physically secure all media that contains sensitive information.			03.08.01	A.03.08.01[01] A.03.08.01[02]									Annual	
	R3	R2 & R3	Data Classification & Handling	DCH-06.2	P-DCH-06.2	Sensitive Data Inventories	DCH-06.2	Mechanisms exist to maintain inventory logs of all sensitive media and conduct sensitive media inventories at least annually.			03.04.11.a 03.04.11.b	A.03.04.11.a[02] A.03.04.11.b[01] A.03.04.11.b[02]									Annual	E-AST-08
	R3	R2 & R3	Data Classification & Handling	DCH-06.4	P-DCH-06.4	Making Sensitive Data Unreadable In Storage	DCH-06.4	Mechanisms exist to ensure sensitive and/or regulated data is rendered human unreadable anywhere sensitive and/or regulated data is stored.			03.08.01	A.03.08.01[01] A.03.08.01[02]									Annual	
R2	R3	R2 & R3	Data Classification & Handling	DCH-07	P-DCH-07	Media Transportation	DCH-07	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.	3.8.5	3.8.5[a] 3.8.5[b]	03.08.05.a 03.08.05.b 03.08.05.c	A.03.08.05.a[01] A.03.08.05.a[02] A.03.08.05.b A.03.08.05.c							MPL2.-3.8.5	Annual	E-DCH-14
	R3	R2 & R3	Data Classification & Handling	DCH-07.1	P-DCH-07.1	Custodians	DCH-07.1	Mechanisms exist to identify custodians throughout the transport of digital or non-digital media.			03.08.05.a 03.08.05.b	A.03.08.05.a[02] A.03.08.05.b									Annual	
	R3	R2 & R3	Data Classification & Handling	DCH-07.2	P-DCH-07.2	Encrypting Data In Storage Media	DCH-07.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.			03.08.05.a	A.03.08.05.a[02]									Annual	
R2	R3	R2 & R3	Data Classification & Handling	DCH-08	P-DCH-08	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	3.8.3		03.08.03	A.03.08.03		52.204-21(b)(1)(vii)			MP.L1-B.1.VII		MPL2.-3.8.3	Annual	E-AST-03
R2	R3	R2 & R3	Data Classification & Handling	DCH-09	P-DCH-09	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	3.7.3 3.8.3	3.7.3 3.8.3[a] 3.8.3[b]	03.07.04.c 03.08.03	A.03.07.04.c A.03.08.03		52.204-21(b)(1)(vii)			MP.L1-B.1.VII	MP.L1-B.1.VII[a] MP.L1-B.1.VII[b]	MAL2.-3.7.3 MPL2.-3.8.3	Annual	E-AST-03 E-DCH-07
R2	R3	R2 & R3	Data Classification & Handling	DCH-10	P-DCH-10	Media Use	DCH-10	Mechanisms exist to restrict the use of types of digital media on systems or system components.	3.8.7	3.8.7	03.08.07.a	A.03.08.07.ODP[01] A.03.08.07.a							MPL2.-3.8.7	Annual	
R2	R3	R2 & R3	Data Classification & Handling	DCH-10.2	P-DCH-10.2	Prohibit Use Without Owner	DCH-10.2	Mechanisms exist to prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.	3.8.8	3.8.8	03.08.07.b	A.03.08.07.b							MPL2.-3.8.8	Annual	
	R3	R2 & R3	Data Classification & Handling	DCH-12	P-DCH-12	Removable Media Security	DCH-12	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.			03.08.07.a	A.03.08.07.a									Annual	
R2	R3	R2 & R3	Data Classification & Handling	DCH-13	P-DCH-13	Use of External Technology Assets, Applications and/or Services (TAAS)	DCH-13	Mechanisms exist to govern how external parties, including Technology Assets, Applications and/or Services (TAAS), are used to securely store, process and transmit data.	3.1.20	3.1.20[a] 3.1.20[b] 3.1.20[c] 3.1.20[d] 3.1.20[e] 3.1.20[f]	03.01.20.a 03.01.20.b 03.01.20.c.01 03.01.20.c.02 03.01.20.d	A.03.01.20.ODP[01] A.03.01.20.a A.03.01.20.b A.03.01.20.c.01 A.03.01.20.c.02 A.03.01.20.d		52.204-21(b)(1)(iii)			AC.L1-B.1.III	AC.L1-B.1.III[a] AC.L1-B.1.III[b] AC.L1-B.1.III[c] AC.L1-B.1.III[d] AC.L1-B.1.III[e] AC.L1-B.1.III[f]	ACL2.-3.1.20	Annual	
R2	R3	R2 & R3	Data Classification & Handling	DCH-13.1	P-DCH-13.1	Limits of Authorized Use	DCH-13.1	Mechanisms exist to prohibit external parties, including Technology Assets, Applications and/or Services (TAAS), from storing, processing and transmitting data unless authorized individuals first: (1) Verifying the implementation of required security, compliance and/or resilience controls; or (2) Retaining a processing agreement with the entity hosting the external TAAS.	3.1.20		03.01.20.a 03.01.20.b 03.01.20.c.01 03.01.20.c.02 03.01.20.d	A.03.01.20.a A.03.01.20.b A.03.01.20.c.01 A.03.01.20.c.02 A.03.01.20.d		52.204-21(b)(1)(iii)			AC.L1-B.1.III		ACL2.-3.1.20	Annual	
R2	R3	R2 & R3	Data Classification & Handling	DCH-13.2	P-DCH-13.2	Portable Storage Devices	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.	3.1.21	3.1.21[a] 3.1.21[b] 3.1.21[c]	03.01.20.a 03.01.20.d	A.03.01.20.a A.03.01.20.d							ACL2.-3.1.21	Annual	
	R3	R2 & R3	Data Classification & Handling	DCH-13.3	P-DCH-13.3	Protecting Sensitive / Regulated Data on External Technology Assets, Applications and/or Services (TAAS)	DCH-13.3	Mechanisms exist to ensure that the requirements for the protection of sensitive and/or regulated data processed, stored or transmitted on external Technology Assets, Applications and/or Services (TAAS), are implemented in accordance with applicable statutory, regulatory and contractual obligations.			03.01.20.b 03.01.20.c.01	A.03.01.20.b A.03.01.20.c.01									Semi-Annual	

Applies To NIST 800-171 R2 & CMMC L2	Applies To NIST 800-171 R3	Applies To Both 171 R2 & R3	NCP SCRP Policy	NCP SCRP Standard #	NCP CSQP Procedure #	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US DFARS Cybersecurity	US FAR 52.204-21	US FAR 52.204-25	US FAR 52.204-27	US CMMC 2.0 Level 1	US CMMC 2.0 Level 1 AOs	US CMMC 2.0 Level 2	Conformity Validation Cadence	Evidence Request List (ERL) #
	R3	R2 & R3	Data Classification & Handling	DCH-13.4	P-DCH-13.4	Non-Organizationally Owned Technology Assets, Applications and/or Services (TAAS)	DCH-13.4	Mechanisms exist to restrict the use of non-organizationally owned Technology Assets, Applications and/or Services (TAAS) to process, store or transmit organizational information.			03.01.20.a 03.01.20.c.01 03.01.20.d	A.03.01.20.a A.03.01.20.c.01 A.03.01.20.d									Annual	
	R3	R2 & R3	Data Classification & Handling	DCH-14	P-DCH-14	Information Sharing	DCH-14	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.			03.01.20.b	A.03.01.20.b									Annual	E-DCH-09 E-SAT-06
	R3	R2 & R3	Data Classification & Handling	DCH-14.2	P-DCH-14.2	Transfer Authorizations	DCH-14.2	Mechanisms exist to verify that individuals or Technology Assets, Applications and/or Services (TAAS) transferring data between interconnecting TAAS have the requisite authorizations (e.g., write permissions or privileges) prior to transferring said data.			03.01.20.b 03.01.20.c.02 03.12.05.a	A.03.01.20.b A.03.01.20.c.02 A.03.12.05.a[01]									Annual	
	R3	R2 & R3	Data Classification & Handling	DCH-14.3	P-DCH-14.3	Data Access Mapping	DCH-14.3	Mechanisms exist to leverage data-specific Access Control Lists (ACL) or Interconnection Security Agreements (ISAs) to generate a logical map of the parties with whom sensitive and/or regulated data is shared.			03.01.03 03.01.20.c.02 03.12.05.a	A.03.01.03[02] A.03.01.20.c.02 A.03.12.05.a[01]									Semi-Annual	
R2	R3	R2 & R3	Data Classification & Handling	DCH-15	P-DCH-15	Publicly Accessible Content	DCH-15	Mechanisms exist to control publicly-accessible content.	3.1.22	3.1.22[a] 3.1.22[b] 3.1.22[c] 3.1.22[d] 3.1.22[e]	03.01.22.a 03.01.22.b	A.03.01.22.a A.03.01.22.b[01]		52.204-21(b)(1)(iv)			AC.L1-B.1.IV	AC.L1-B.1.IV[a] AC.L1-B.1.IV[b] AC.L1-B.1.IV[c] AC.L1-B.1.IV[d] AC.L1-B.1.IV[e]	ACL2.-3.1.22	Annual	E-DCH-12
R2	R3	R2 & R3	Data Classification & Handling	DCH-17	P-DCH-17	Ad-Hoc Transfers	DCH-17	Mechanisms exist to secure ad-hoc exchanges of large digital files with internal or external parties.	3.1.20		03.01.20.a	A.03.01.20.a		52.204-21(b)(1)(iii)			AC.L1-B.1.III		ACL2.-3.1.20	Annual	
	R3	R2 & R3	Data Classification & Handling	DCH-18	P-DCH-18	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.			03.01.20.c.02 03.10.07.b 03.14.08	A.03.01.20.c.02 A.03.10.07.b A.03.14.08[01] A.03.14.08[02] A.03.14.08[03] A.03.14.08[04]									Semi-Annual	E-AST-11
	R3	R2 & R3	Data Classification & Handling	DCH-19	P-DCH-19	Geographic Location of Data	DCH-19	Mechanisms exist to inventory, document and maintain data flows for data that is resident (permanently or temporarily) within a service's geographically distributed applications (physical and virtual), infrastructure, systems components and/or shared with other third-parties.			03.04.11.a 03.04.11.b	A.03.04.11.a[01] A.03.04.11.b[01] A.03.04.11.b[02]									Annual	E-AST-23
	R3	R2 & R3	Data Classification & Handling	DCH-21	P-DCH-21	Information Disposal	DCH-21	Mechanisms exist to securely dispose of, destroy or erase information.			03.08.03	A.03.08.03									Annual	
	R3	R2 & R3	Data Classification & Handling	DCH-24	P-DCH-24	Information Location	DCH-24	Mechanisms exist to identify and document the location of information and the specific system components on which the information resides.			03.04.11.a	A.03.04.11.a[01]									Annual	E-AST-23
R2	R3	R2 & R3	Endpoint Security	END-01	P-END-01	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	3.14.2	3.4.1[a] 3.4.1[b] 3.4.1[c] 3.4.2[a] 3.4.2[b]	03.01.03 03.14.02.a	A.03.01.03[01] A.03.01.03[02] A.03.14.02.a[01]		52.204-21(b)(1)(xii)			SI.L1-B.1.XIII		SIL2.-3.14.2	Annual	E-AST-01 E-END-01
R2		R2 & R3	Endpoint Security	END-02	P-END-02	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	3.13.16	3.13.16									SCL2.-3.13.16	Annual	
R2		R2 & R3	Endpoint Security	END-03	P-END-03	Prohibit Installation Without Privileged Status	END-03	Automated mechanisms exist to prohibit software installations without explicitly assigned privileged status.	3.4.9										CML2.-3.4.9	Quarterly	E-IAM-02
R2		R2 & R3	Endpoint Security	END-03.2	P-END-03.2	Governing Access Restriction for Change	END-03.2	Mechanisms exist to define, document, approve and enforce access restrictions associated with changes to Technology Assets, Applications and/or Services (TAAS).		3.4.5[a] 3.4.5[b] 3.4.5[c] 3.4.5[d] 3.4.5[e] 3.4.5[f]									Annual	
R2	R3	R2 & R3	Endpoint Security	END-04	P-END-04	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	3.14.2	3.14.2[a] 3.14.2[b] 3.14.5[a] 3.14.5[b] 3.14.5[c]	03.14.02.c 03.14.02.c.01 03.14.02.c.02	A.03.14.02.ODP[01] A.03.14.02.a[01] A.03.14.02.a[02] A.03.14.02.c.01[01] A.03.14.02.c.02		52.204-21(b)(1)(xiii) 52.204-21(b)(1)(xv)			SI.L1-B.1.XIII SI.L1-B.1.XV	SI.L1-B.1.XIII[a] SI.L1-B.1.XIII[b] SI.L1-B.1.XV[a] SI.L1-B.1.XV[b]	SIL2.-3.14.2	Annual	E-END-01 E-MON-02
R2	R3	R2 & R3	Endpoint Security	END-04.1	P-END-04.1	Automatic Antimalware Signature Updates	END-04.1	Automated mechanisms exist to update antimalware technologies, including signature definitions.	3.14.4	3.14.4	03.14.02.b	A.03.14.02.b		52.204-21(b)(1)(xiv)			SI.L1-B.1.XIV	SI.L1-B.1.XIV[a]	SIL2.-3.14.4	Quarterly	E-END-02
	R3	R2 & R3	Endpoint Security	END-04.3	P-END-04.3	Centralized Management of Antimalware Technologies	END-04.3	Mechanisms exist to centrally-manage antimalware technologies.			03.14.02.a	A.03.14.02.a[01]									Quarterly	E-END-03 E-MON-02
R2	R3	R2 & R3	Endpoint Security	END-04.7	P-END-04.7	Always On Protection	END-04.7	Mechanisms exist to ensure that anti-malware technologies are continuously running in real-time and cannot be disabled or altered by non-privileged users, unless specifically authorized by management on a case-by-case basis for a limited time period.	3.14.5	3.14.5[c]	03.14.02.a 03.14.02.c.01 03.14.02.c.02	A.03.14.02.a[01] A.03.14.02.c.01[01] A.03.14.02.c.01[02]		52.204-21(b)(1)(xv)			SI.L1-B.1.XV	SI.L1-B.1.XV[c]	SIL2.-3.14.5	Quarterly	
	R3	R2 & R3	Endpoint Security	END-07	P-END-07	Host Intrusion Detection and Prevention Systems (HIDS / HIPS)	END-07	Mechanisms exist to utilize Host-based Intrusion Detection / Prevention Systems (HIDS / HIPS), or similar technologies, to monitor for and protect against anomalous host activity, including lateral movement across the network.			03.14.06.a.01 03.14.06.a.02 03.14.06.b 03.14.06.c	A.03.14.06.a.01[01] A.03.14.06.a.01[02] A.03.14.06.b									Annual	
R2	R3	R2 & R3	Endpoint Security	END-10	P-END-10	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	3.13.13	3.13.13[a] 3.13.13[b]	03.13.13.a 03.13.13.b	A.03.13.13.a[01] A.03.13.13.a[02] A.03.13.13.b[01] A.03.13.13.b[03]							SCL2.-3.13.13	Annual	E-AST-32
R2	R3	R2 & R3	Endpoint Security	END-14	P-END-14	Collaborative Computing Devices	END-14	Mechanisms exist to unplug or prohibit the remote activation of collaborative computing devices with the following exceptions: (1) Networked whiteboards; (2) Video teleconference cameras; and (3) Teleconference microphones.	3.13.12	3.13.12[a] 3.13.12[b] 3.13.12[c]	03.13.12.a	A.03.13.12.ODP[01] A.03.13.12.a							SCL2.-3.13.12	Annual	
	R3	R2 & R3	Endpoint Security	END-14.6	P-END-14.6	Explicit Indication Of Use	END-14.6	Mechanisms exist to configure collaborative computing devices to provide physically-present individuals with an explicit indication of use.			03.13.12.b	A.03.13.12.b									Annual	

Applies To NIST 800-171 R2 & CMMC L2	Applies To NIST 800-171 R3	Applies To Both 171 R2 & R3	NCP SCRP Policy	NCP SCRP Standard #	NCP CSOP Procedure #	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US DFARS Cybersecurity	US FAR 52.204-21	US FAR 52.204-25	US FAR 52.204-27	US CMMC 2.0 Level 1	US CMMC 2.0 Level 1 AOs	US CMMC 2.0 Level 2	Conformity Validation Cadence	Evidence Request List (ERL) #
R2	R3	R2 & R3	Human Resources Security	HRS-01	P-HRS-01	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	3.1.22 NFO - PS-1	3.2.2[a] 3.2.2[b] 3.2.2[c] 3.9.2[a]	03.01.01.g.02 03.15.03.a 03.15.03.d	A.03.01.01.ODP[01] A.03.01.01.ODP[02] A.03.01.01.ODP[03] A.03.01.01.ODP[04] A.03.01.01.g.02 A.03.15.03.a		52.204-21(b)(1)(iv)			AC.L1-B.1.IV		AC.L2-3.1.22	Annual	E-HRS-01 E-HRS-15 E-HRS-27
R2		R2 & R3	Human Resources Security	HRS-01.1	P-HRS-01.1	Onboarding, Transferring & Offboarding Personnel	HRS-01.1	Mechanisms exist to proactively govern the following personnel management actions: (1) Onboarding new personnel (e.g., new hires); (2) Transferring personnel into new roles within the organization; and (3) Offboarding personnel (e.g., termination of employment).	3.9.2										PSL2.-3.9.2	Quarterly	
	R3	R2 & R3	Human Resources Security	HRS-02	P-HRS-02	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.			03.01.01.c.01 03.01.01.c.02 03.01.01.d.01 03.01.01.d.02 03.01.02 03.09.01.a	A.03.01.01.c.01 A.03.01.01.c.02 A.03.01.01.d.01 A.03.01.01.d.02 A.03.01.02[01] A.03.01.02[02]							Annual	E-HRS-01 E-HRS-02 E-HRS-03 E-HRS-04 E-HRS-11 E-HRS-22
	R3	R2 & R3	Human Resources Security	HRS-02.1	P-HRS-02.1	Users With Elevated Privileges	HRS-02.1	Mechanisms exist to ensure that every user accessing Technology Assets, Applications and/or Services (TAAS) that process, store and/or transmit sensitive and/or regulated data is cleared and regularly trained to handle the information in question.			03.01.02	A.03.01.02[01] A.03.01.02[02]							Quarterly	E-HRS-02 E-HRS-03 E-HRS-04 E-HRS-11 E-HRS-22
	R3	R2 & R3	Human Resources Security	HRS-03	P-HRS-03	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.			03.01.22.a 03.02.02.a.01 03.06.04.a 03.06.05.d 03.07.06.a 03.07.06.d	A.03.01.22.a A.03.02.02.a.01[01] A.03.06.04.ODP[01] A.03.06.05.d A.03.07.06.a A.03.07.06.d[01]							Annual	E-HRS-01 E-HRS-02 E-HRS-03 E-HRS-04 E-HRS-11 E-HRS-13
	R3	R2 & R3	Human Resources Security	HRS-03.1	P-HRS-03.1	User Awareness	HRS-03.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.			03.01.22.a 03.15.03.b	A.03.01.22.a A.03.15.03.b							Annual	E-HRS-01 E-HRS-13 E-HRS-16 E-HRS-18
	R3	R2 & R3	Human Resources Security	HRS-03.2	P-HRS-03.2	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.			03.07.06.d	A.03.07.06.d[01]							Annual	E-HRS-21 E-HRS-23
R2	R3	R2 & R3	Human Resources Security	HRS-04	P-HRS-04	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	3.9.1	3.9.1	03.09.01.a 03.09.01.b 03.09.02.b.01	A.03.09.01.ODP[01] A.03.09.01.a A.03.09.01.b A.03.09.02.b.01[01]						PSL2.-3.9.1	Annual	E-HRS-17 E-HRS-21
R2	R3	R2 & R3	Human Resources Security	HRS-04.1	P-HRS-04.1	Roles With Special Protection Measures	HRS-04.1	Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria.	3.9.1		03.01.22.a 03.02.02.a.01 03.09.01.a 03.09.01.b	A.03.01.22.a A.03.02.02.a.01[01] A.03.09.01.ODP[01] A.03.09.01.a A.03.09.01.b						PSL2.-3.9.1	Annual	E-HRS-17 E-HRS-21
R2	R3	R2 & R3	Human Resources Security	HRS-04.2	P-HRS-04.2	Formal Indoctrination	HRS-04.2	Mechanisms exist to formally educate authorized users on proper data handling practices for all the relevant types of data to which they have access.	3.2.1 3.2.2		03.01.22.a 03.02.02.a.01 03.06.04.a 03.06.04.a.01 03.15.03.b	A.03.01.22.a A.03.02.02.a.01[01] A.03.06.04.ODP[01] A.03.06.04.a.01 A.03.15.03.b						ATL2.-3.2.1 ATL2.-3.2.2	Annual	E-HRS-18
R2	R3	R2 & R3	Human Resources Security	HRS-05	P-HRS-05	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to enable secure, compliant and resilient capabilities.	3.1.22 NFO - PL-4		03.01.01.h 03.01.22.a 03.15.03.a 03.15.03.b	A.03.01.01.h A.03.01.22.a A.03.15.03.a A.03.15.03.b		52.204-21(b)(1)(iv)			AC.L1-B.1.IV		AC.L2-3.1.22	Annual	E-HRS-16 E-HRS-22
R2	R3	R2 & R3	Human Resources Security	HRS-05.1	P-HRS-05.1	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	3.1.22 NFO - PL-4		03.01.12.a 03.01.18.a 03.01.22.a 03.15.03.a 03.15.03.d	A.03.01.18.a[01] A.03.01.22.a A.03.15.03.ODP[01] A.03.15.03.a A.03.15.03.d[01] A.03.15.03.d[02]		52.204-21(b)(1)(iv)			AC.L1-B.1.IV		AC.L2-3.1.22	Annual	E-HRS-22
R2	R3	R2 & R3	Human Resources Security	HRS-05.2	P-HRS-05.2	Social Media & Social Networking Restrictions	HRS-05.2	Mechanisms exist to define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information.	3.1.22 NFO - PL-4(1)		03.15.03.a	A.03.15.03.a		52.204-21(b)(1)(iv)			AC.L1-B.1.IV		AC.L2-3.1.22	Annual	E-DCH-11 E-HRS-22
	R3	R2 & R3	Human Resources Security	HRS-05.3	P-HRS-05.3	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.			03.01.01.h 03.01.12.a 03.01.18.a 03.15.03.a	A.03.01.01.h A.03.01.18.a[01] A.03.15.03.a							Annual	E-HRS-22
	R3	R2 & R3	Human Resources Security	HRS-05.4	P-HRS-05.4	Use of Critical Technologies	HRS-05.4	Mechanisms exist to govern usage policies for critical technologies.			03.15.03.a	A.03.15.03.a							Annual	E-HRS-22
	R3	R2 & R3	Human Resources Security	HRS-05.5	P-HRS-05.5	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.			03.01.18.a 03.15.03.a	A.03.01.18.a[01] A.03.15.03.a							Annual	E-HRS-22
	R3	R2 & R3	Human Resources Security	HRS-05.7	P-HRS-05.7	Policy Familiarization & Acknowledgement	HRS-05.7	Mechanisms exist to ensure personnel receive recurring familiarization with the organization's security, compliance and resilience policies and provide acknowledgement.			03.15.03.c 03.15.03.d	A.03.15.03.c A.03.15.03.d[02]							Annual	E-HRS-18 E-SAT-02 E-SAT-04
R2	R3	R2 & R3	Human Resources Security	HRS-06	P-HRS-06	Access Agreements	HRS-06	Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access.	NFO - PS-6		03.01.18.a 03.12.05.a 03.15.03.c	A.03.01.18.a[01] A.03.12.05.a[01] A.03.15.03.c							Annual	E-HRS-16
	R3	R2 & R3	Human Resources Security	HRS-06.1	P-HRS-06.1	Confidentiality Agreements	HRS-06.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, or both employees and third-parties.			03.12.05.a 03.15.03.c	A.03.12.05.a[01] A.03.15.03.c							Annual	E-HRS-20
R2	R3	R2 & R3	Human Resources Security	HRS-07	P-HRS-07	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	NFO - PS-8	3.9.2[a] 3.9.2[b] 3.9.2[c]	03.01.01.f.04 03.01.01.f.05	A.03.01.01.f.04 A.03.01.01.f.05							Annual	E-HRS-27 E-HRS-29
	R3	R2 & R3	Human Resources Security	HRS-07.1	P-HRS-07.1	Workplace Investigations	HRS-07.1	Mechanisms exist to conduct employee misconduct investigations when there is reasonable assurance that a policy has been violated.			03.01.01.f.04 03.01.01.f.05	A.03.01.01.f.04 A.03.01.01.f.05							Annual	
R2	R3	R2 & R3	Human Resources Security	HRS-08	P-HRS-08	Personnel Transfer	HRS-08	Mechanisms exist to adjust logical and physical access authorizations to Technology Assets, Applications and/or Services (TAAS) and facilities upon personnel reassignment or transfer, in a timely manner.	3.9.2	3.9.2[a] 3.9.2[b] 3.9.2[c]	03.01.01.g.02 03.09.02.a 03.09.02.b.01 03.09.02.b.02	A.03.01.01.g.02 A.03.09.02.ODP[01] A.03.09.02.a.01 A.03.09.02.b.01[01] A.03.09.02.b.01[02] A.03.09.02.b.02						PSL2.-3.9.2	Annual	E-HRS-29

Applies To NIST 800-171 R2 & CMMC L2	Applies To NIST 800-171 R3	Applies To Both 171 R2 & R3	NCP SCRP Policy	NCP SCRP Standard #	NCP CSOP Procedure #	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US DFARS Cybersecurity	US FAR 52.204-21	US FAR 52.204-25	US FAR 52.204-27	US CMMC 2.0 Level 1	US CMMC 2.0 Level 1 AOs	US CMMC 2.0 Level 2	Conformity Validation Cadence	Evidence Request List (ERL) #
R2	R3	R2 & R3	Human Resources Security	HRS-09	P-HRS-09	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	3.9.2	3.9.2[a] 3.9.2[b] 3.9.2[c]	03.01.01.f.03 03.01.01.g.02 03.09.02.a 03.09.02.a.02 03.09.02.a.03 03.09.02.b.01	A.03.01.01.f.03 A.03.01.01.g.02 A.03.09.02.ODP[01] A.03.09.02.a.01 A.03.09.02.a.02[01] A.03.09.02.a.02[02]							PSL2.-3.9.2	Annual	E-HRS-19 E-HRS-29
	R3	R2 & R3	Human Resources Security	HRS-09.1	P-HRS-09.1	Asset Collection	HRS-09.1	Mechanisms exist to retrieve organization-owned assets upon termination of an individual's employment.			03.09.02.a.03	A.03.09.02.a.03									Annual	E-HRS-19
	R3	R2 & R3	Human Resources Security	HRS-09.2	P-HRS-09.2	High-Risk Terminations	HRS-09.2	Mechanisms exist to expedite the process of removing "high risk" individual's access to Technology Assets, Applications, Services and/or Data (TAASD) upon termination, as determined by management.			03.09.02.a.01 03.09.02.a.02 03.09.02.b.01	A.03.09.02.a.01 A.03.09.02.a.02[01] A.03.09.02.a.02[02] A.03.09.02.b.01[01]								Annual	E-HRS-19
	R3	R2 & R3	Human Resources Security	HRS-09.4	P-HRS-09.4	Automated Employment Status Notifications	HRS-09.4	Automated mechanisms exist to notify Identity and Access Management (IAM) personnel or roles upon termination of an individual employment or contract.			03.01.01.g.02 03.09.02.a.01 03.09.02.a.02	A.03.01.01.g.02 A.03.09.02.a.01 A.03.09.02.a.02[01] A.03.09.02.a.02[02]								Quarterly	
R2	R3	R2 & R3	Human Resources Security	HRS-10	P-HRS-10	Third-Party Personnel	HRS-10	Mechanisms exist to govern third-party personnel by reviewing and monitoring third-party security, compliance and/or resilience roles and responsibilities.	NFO - PS-7		03.16.03.b	A.03.16.03.b								Annual	E-HRS-16 E-HRS-18 E-HRS-22
R2	R3	R2 & R3	Human Resources Security	HRS-11	P-HRS-11	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	3.1.4	3.1.4[a] 3.1.4[b] 3.1.4[c]	03.01.04.a	A.03.01.04.a							ACL2.-3.1.4	Annual	E-HRS-25
	R3	R2 & R3	Human Resources Security	HRS-12	P-HRS-12	Incompatible Roles	HRS-12	Mechanisms exist to avoid incompatible development-specific roles through limiting and reviewing developer privileges to change hardware, software and firmware components within a production/operational environment.			03.01.04.a	A.03.01.04.a								Annual	E-HRS-25
R2	R3	R2 & R3	Identification & Authentication	IAC-01	P-IAC-01	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	3.1.1 NFO - AC-1 NFO - IA-1		03.01.01.a 03.01.18.b 03.05.01.a 03.05.05.a 03.05.12.a	A.03.01.01.a[01] A.03.01.01.a[02] A.03.01.18.b A.03.05.01.a[01] A.03.05.05.a A.03.05.12.a		52.204-21(b)(1)(i)			AC.L1-B.1.I		ACL2.-3.1.1	Annual	E-AST-01 E-IAM-05 E-IAM-12 E-MON-11
	R3	R2 & R3	Identification & Authentication	IAC-01.2	P-IAC-01.2	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).			03.01.01.d.01 03.01.16.b 03.05.01.a 03.05.02 03.05.05.d 03.05.07.a	A.03.01.01.d.01 A.03.01.16.b A.03.05.01.a[01] A.03.05.01.a[02] A.03.05.02[01] A.03.05.02[02]								Annual	E-IAM-06
R2	R3	R2 & R3	Identification & Authentication	IAC-02	P-IAC-02	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	3.1.1 3.5.1 3.5.2	3.5.1[a] 3.5.1[b] 3.5.1[c] 3.5.2[a] 3.5.2[b] 3.5.2[c]	03.05.01.a 03.05.05.d	A.03.05.01.a[03] A.03.05.05.d		52.204-21(b)(1)(i) 52.204-21(b)(1)(v) 52.204-21(b)(1)(vi)			AC.L1-B.1.I IA.L1-B.1.V IA.L1-B.1.VI	IA.L1-B.1.V[a] IA.L1-B.1.V[c] IA.L1-B.1.VI[a] IA.L1-B.1.VI[b] IA.L1-B.1.VI[c]	ACL2.-3.1.1 IAL2.-3.5.1 IAL2.-3.5.2	Annual	E-IAM-05 E-IAM-06 E-IAM-13
R2	R3	R2 & R3	Identification & Authentication	IAC-02.2	P-IAC-02.2	Replay-Resistant Authentication	IAC-02.2	Automated mechanisms exist to employ replay-resistant authentication.	3.5.4	3.5.4	03.05.04 03.07.05.b	A.03.05.04[01] A.03.05.04[02] A.03.07.05.b[02]							IAL2.-3.5.4	Quarterly	E-AST-01 E-IAM-05 E-IAM-06
	R3	R2 & R3	Identification & Authentication	IAC-03	P-IAC-03	Identification & Authentication for Non-Organizational Users	IAC-03	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.			03.05.01.a	A.03.05.01.a[03]								Annual	E-IAM-05 E-IAM-06
R2	R3	R2 & R3	Identification & Authentication	IAC-04	P-IAC-04	Identification & Authentication for Devices	IAC-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically- based and replay resistant.	3.5.1 3.5.2		03.01.18.b 03.05.02	A.03.01.18.b A.03.05.02.ODP[01] A.03.05.02[01] A.03.05.02[02]		52.204-21(b)(1)(v) 52.204-21(b)(1)(vi)			IA.L1-B.1.V IA.L1-B.1.VI		IAL2.-3.5.1 IAL2.-3.5.2	Annual	E-IAM-05 E-IAM-06
	R3	R2 & R3	Identification & Authentication	IAC-05	P-IAC-05	Identification & Authentication for Third-Party Technology Assets, Applications and/or Services (TAAS)	IAC-05	Mechanisms exist to identify and authenticate third-party Technology Assets, Applications and/or Services (TAAS).			03.05.01.a 03.05.02	A.03.05.01.a[03] A.03.05.02[01] A.03.05.02[02]								Annual	E-IAM-05 E-IAM-06
	R3	R2 & R3	Identification & Authentication	IAC-05.2	P-IAC-05.2	Privileged Access by Non-Organizational Users	IAC-05.2	Mechanisms exist to prohibit privileged access by non-organizational users.			03.07.05.a	A.03.07.05.a[01]								Annual	
R2	R3	R2 & R3	Identification & Authentication	IAC-06	P-IAC-06	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	3.5.3 3.7.5		03.05.03 03.07.05.b	A.03.05.03[01] A.03.05.03[02] A.03.07.05.b[01]						IAL2.-3.5.3 MAL2.-3.7.5	Quarterly	
R2	R3	R2 & R3	Identification & Authentication	IAC-06.1	P-IAC-06.1	Network Access to Privileged Accounts	IAC-06.1	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	3.5.3	3.5.3[a] 3.5.3[c]	03.05.03	A.03.05.03[01]							IAL2.-3.5.3	Annual	
R2	R3	R2 & R3	Identification & Authentication	IAC-06.2	P-IAC-06.2	Network Access to Non-Privileged Accounts	IAC-06.2	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for non-privileged accounts.	3.5.3	3.5.3[d]	03.05.03	A.03.05.03[02]							IAL2.-3.5.3	Annual	
R2	R3	R2 & R3	Identification & Authentication	IAC-06.3	P-IAC-06.3	Local Access to Privileged Accounts	IAC-06.3	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate local access for privileged accounts.	3.5.3	3.5.3[a] 3.5.3[b]	03.05.03	A.03.05.03[01]							IAL2.-3.5.3	Annual	
	R3	R2 & R3	Identification & Authentication	IAC-06.4	P-IAC-06.4	Out-of-Band Multi-Factor Authentication	IAC-06.4	Mechanisms exist to implement Multi-Factor Authentication (MFA) for access to privileged and non-privileged accounts such that one of the factors is independently provided by a device separate from the system being accessed.			03.05.03	A.03.05.03[01] A.03.05.03[02]								Annual	
	R3	R2 & R3	Identification & Authentication	IAC-07	P-IAC-07	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.			03.01.01.b 03.01.01.g.01 03.01.01.g.02 03.01.01.g.03 03.05.05.a 03.09.02.a.01	A.03.01.01.b[01] A.03.01.01.b[02] A.03.01.01.b[03] A.03.01.01.b[04] A.03.01.01.b[05] A.03.01.01.e.01								Annual	E-HRS-12 E-HRS-18 E-HRS-19
	R3	R2 & R3	Identification & Authentication	IAC-07.1	P-IAC-07.1	Change of Roles & Duties	IAC-07.1	Mechanisms exist to revoke user access rights following changes in personnel roles and duties, if no longer necessary or permitted.			03.01.01.g.01 03.01.01.g.02 03.01.01.g.03 03.05.05.a 03.09.02.b.02	A.03.01.01.g.01 A.03.01.01.g.02 A.03.01.01.g.03 A.03.05.05.a A.03.09.02.b.01[02] A.03.09.02.b.02								Annual	E-HRS-12 E-HRS-19

Applies To NIST 800-171 R2 & CMMC L2	Applies To NIST 800-171 R3	Applies To Both 171 R2 & R3	NCP SCRP Policy	NCP SCRP Standard #	NCP CSOP Procedure #	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US DFARS Cybersecurity	US FAR 52.204-21	US FAR 52.204-25	US FAR 52.204-27	US CMMC 2.0 Level 1	US CMMC 2.0 Level 1 AOs	US CMMC 2.0 Level 2	Conformity Validation Cadence	Evidence Request List (ERL) #
	R3	R2 & R3	Identification & Authentication	IAC-07.2	P-IAC-07.2	Termination of Employment	IAC-07.2	Mechanisms exist to revoke user access rights in a timely manner, upon termination of employment or contract.			03.09.02.a.01 03.09.02.a.02	A.03.09.02.a.01 A.03.09.02.a.02[01] A.03.09.02.a.02[02]								Annual	E-HRS-19
R2	R3	R2 & R3	Identification & Authentication	IAC-08	P-IAC-08	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	3.1.1 3.1.2 3.1.3	3.1.3[c]	03.01.01.c.01 03.01.01.c.02 03.01.01.c.03 03.01.02 03.01.05.b 03.01.06.a	A.03.01.01.c.01 A.03.01.01.c.02 A.03.01.01.c.03 A.03.01.02[01] A.03.01.02[02] A.03.01.05.ODP[01]		52.204-21(b)(1)(i) 52.204-21(b)(1)(ii)			AC.L1-B.1.I AC.L1-B.1.II		ACL2.-3.1.1 ACL2.-3.1.2 ACL2.-3.1.3	Annual	E-HRS-12 E-IAM-02
R2	R3	R2 & R3	Identification & Authentication	IAC-09	P-IAC-09	Identifier Management (User Names)	IAC-09	Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS).	3.5.5	3.5.5[a] 3.5.5[b]	03.05.05.b 03.05.05.c 03.05.05.d	A.03.05.05.ODP[01] A.03.05.05.b[01] A.03.05.05.b[02] A.03.05.05.c A.03.05.05.d							IAL2.-3.5.5	Annual	
	R3	R2 & R3	Identification & Authentication	IAC-09.1	P-IAC-09.1	User Identity (ID) Management	IAC-09.1	Mechanisms exist to ensure proper user identification management for non-consumer users and administrators.			03.05.05.b	A.03.05.05.b[01] A.03.05.05.b[02]								Annual	
	R3	R2 & R3	Identification & Authentication	IAC-09.2	P-IAC-09.2	Identity User Status	IAC-09.2	Mechanisms exist to identify contractors and other third-party users through unique username characteristics.			03.05.05.d	A.03.05.05.ODP[02] A.03.05.05.d								Annual	
R2	R3	R2 & R3	Identification & Authentication	IAC-09.5	P-IAC-09.5	Privileged Account Identifiers	IAC-09.5	Mechanisms exist to uniquely manage privileged accounts to identify the account as a privileged user or service.		3.1.5[a]	03.01.07.b 03.05.05.d	A.03.01.07.b A.03.05.05.d								Annual	
R2	R3	R2 & R3	Identification & Authentication	IAC-10	P-IAC-10	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	3.5.8 3.5.9	3.5.8[a] 3.5.8[b] 3.5.9	03.05.07.a 03.05.07.b 03.05.07.c 03.05.07.d 03.05.07.e 03.05.07.f	A.03.05.07.a[01] A.03.05.07.b A.03.05.07.c A.03.05.07.d A.03.05.07.e A.03.05.07.f							IAL2.-3.5.8 IAL2.-3.5.9	Annual	
R2	R3	R2 & R3	Identification & Authentication	IAC-10.1	P-IAC-10.1	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	3.5.7	3.5.7[a] 3.5.7[b] 3.5.7[c] 3.5.7[d]	03.05.07.e 03.05.07.f 03.05.12.b 03.05.12.d 03.05.12.e	A.03.05.07.ODP[02] A.03.05.07.e A.03.05.07.f A.03.05.12.b A.03.05.12.d A.03.05.12.e							IAL2.-3.5.7	Annual	
	R3	R2 & R3	Identification & Authentication	IAC-10.3	P-IAC-10.3	In-Person or Trusted Third-Party Registration	IAC-10.3	Mechanisms exist to conduct in-person or trusted third-party identify verification before user accounts for third-parties are created.			03.05.12.a	A.03.05.12.a								Annual	
	R3	R2 & R3	Identification & Authentication	IAC-10.4	P-IAC-10.4	Automated Support For Password Strength	IAC-10.4	Automated mechanisms exist to determine if password authenticators are sufficiently strong enough to satisfy organization-defined password length and complexity requirements.			03.05.07.a 03.05.07.b	A.03.05.07.ODP[01] A.03.05.07.a[01] A.03.05.07.a[02] A.03.05.07.a[03] A.03.05.07.b								Quarterly	
R2	R3	R2 & R3	Identification & Authentication	IAC-10.5	P-IAC-10.5	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	3.5.10	3.5.10[a] 3.5.10[b]	03.05.07.c 03.05.07.d 03.05.12.f	A.03.05.07.c A.03.05.07.d A.03.05.12.f[01] A.03.05.12.f[02]							IAL2.-3.5.10	Annual	
	R3	R2 & R3	Identification & Authentication	IAC-10.6	P-IAC-10.6	No Embedded Unencrypted Static Authenticators	IAC-10.6	Mechanisms exist to ensure that unencrypted, static authenticators are not embedded in applications, scripts or stored on function keys.			03.05.07.d	A.03.05.07.d								Annual	
	R3	R2 & R3	Identification & Authentication	IAC-10.8	P-IAC-10.8	Default Authenticators	IAC-10.8	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.			03.05.07.e 03.05.12.d	A.03.05.07.e A.03.05.12.d								Annual	
	R3	R2 & R3	Identification & Authentication	IAC-10.11	P-IAC-10.11	Password Managers	IAC-10.11	Mechanisms exist to protect and store passwords via a password manager tool.			03.05.07.a 03.05.07.b 03.05.07.c 03.05.07.d 03.05.07.f	A.03.05.07.ODP[01] A.03.05.07.a[01] A.03.05.07.a[02] A.03.05.07.a[03] A.03.05.07.b A.03.05.07.c								Quarterly	
R2	R3	R2 & R3	Identification & Authentication	IAC-11	P-IAC-11	Authenticator Feedback	IAC-11	Mechanisms exist to obscure the feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	3.5.11	3.5.11	03.05.11	A.03.05.11							IAL2.-3.5.11	Annual	
	R3	R2 & R3	Identification & Authentication	IAC-14	P-IAC-14	Re-Authentication	IAC-14	Mechanisms exist to force users and devices to re-authenticate according to organization-defined circumstances that necessitate re-authentication.			03.05.01.b	A.03.05.01.ODP[01] A.03.05.01.b								Annual	
R2	R3	R2 & R3	Identification & Authentication	IAC-15	P-IAC-15	Account Management	IAC-15	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and (3) Proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	3.1.2	3.1.2[a] 3.1.2[b]	03.01.01.a 03.01.01.b 03.01.01.c.01 03.01.01.c.02 03.01.01.d.01 03.01.01.d.02	A.03.01.01.ODP[01] A.03.01.01.a[01] A.03.01.01.a[02] A.03.01.01.b[01] A.03.01.01.b[02] A.03.01.01.b[03]		52.204-21(b)(1)(ii)			AC.L1-B.1.II	AC.L1-B.1.II.[a] AC.L1-B.1.II.[b]	ACL2.-3.1.2	Quarterly	E-IAM-07 E-IAM-08
R2	R3	R2 & R3	Identification & Authentication	IAC-15.1	P-IAC-15.1	Automated System Account Management (Directory Services)	IAC-15.1	Automated mechanisms exist to support the management of system accounts (e.g., directory services).	3.1.1 3.5.1 3.5.2		03.01.01.d.01 03.05.05.b 03.05.05.c 03.05.05.d 03.05.07.c 03.05.07.d	A.03.01.01.d.01 A.03.05.05.b[01] A.03.05.05.b[02] A.03.05.05.c A.03.05.05.d A.03.05.07.c		52.204-21(b)(1)(i) 52.204-21(b)(1)(v) 52.204-21(b)(1)(vi)			AC.L1-B.1.I IA.L1-B.1.V IA.L1-B.1.VI		ACL2.-3.1.1 IAL2.-3.5.1 IAL2.-3.5.2	Quarterly	
R2	R3	R2 & R3	Identification & Authentication	IAC-15.3	P-IAC-15.3	Disable Inactive Accounts	IAC-15.3	Automated mechanisms exist to disable inactive accounts after an organization-defined time period.	3.5.6	3.5.6[a] 3.5.6[b]	03.01.01.f.02	A.03.01.01.f.02							IAL2.-3.5.6	Quarterly	
	R3	R2 & R3	Identification & Authentication	IAC-15.5	P-IAC-15.5	Restrictions on Shared Groups / Accounts	IAC-15.5	Mechanisms exist to authorize the use of shared/group accounts only under certain organization-defined conditions.			03.01.01.c.01	A.03.01.01.c.01								Annual	E-IAM-08
	R3	R2 & R3	Identification & Authentication	IAC-15.6	P-IAC-15.6	Account Disabling for High Risk Individuals	IAC-15.6	Mechanisms exist to disable accounts immediately upon notification for users posing a significant risk to the organization.			03.01.01.f.04 03.01.01.f.05	A.03.01.01.f.04 A.03.01.01.f.05								Annual	
	R3	R2 & R3	Identification & Authentication	IAC-15.7	P-IAC-15.7	System Account Reviews	IAC-15.7	Mechanisms exist to review all system accounts and disable any account that cannot be associated with a business process and owner.			03.01.01.b 03.01.01.e 03.01.05.c	A.03.01.01.b[04] A.03.01.01.b[05] A.03.01.01.e A.03.01.05.c								Annual	E-IAM-07

Applies To NIST 800-171 R2 & CMMC L2	Applies To NIST 800-171 R3	Applies To Both 171 R2 & R3	NCP SCRP Policy	NCP SCRP Standard #	NCP CSQP Procedure #	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US DFARS Cybersecurity	US FAR 52.204-21	US FAR 52.204-25	US FAR 52.204-27	US CMMC 2.0 Level 1	US CMMC 2.0 Level 1 AOs	US CMMC 2.0 Level 2	Conformity Validation Cadence	Evidence Request List (ERL) #
R2	R3	R2 & R3	Identification & Authentication	IAC-16	P-IAC-16	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	3.1.5		03.01.06.a 03.01.07.a 03.01.07.b	A.03.01.06.a A.03.01.07.a A.03.01.07.b							ACL2.-3.1.5	Quarterly	E-IAM-03
R2		R2 & R3	Identification & Authentication	IAC-16.1	P-IAC-16.1	Privileged Account Inventories	IAC-16.1	Mechanisms exist to inventory all privileged accounts and validate that each person with elevated privileges is authorized by the appropriate level of organizational management.	3.1.5										ACL2.-3.1.5	Annual	E-IAM-03
	R3	R2 & R3	Identification & Authentication	IAC-17	P-IAC-17	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.			03.01.01.g.03 03.01.05.c 03.01.05.d 03.10.01.c 03.10.01.d	A.03.01.01.g.03 A.03.01.05.ODP[03] A.03.01.05.c A.03.01.05.d A.03.10.01.c A.03.10.01.d								Annual	E-HRS-12 E-HRS-14 E-IAM-01
R2	R3	R2 & R3	Identification & Authentication	IAC-20	P-IAC-20	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	3.1.1	3.1.1[a] 3.1.1[b] 3.1.1[c] 3.1.1[d] 3.1.1[e]	03.01.01.c.03 03.01.01.d.01 03.01.01.d.02 03.01.02 03.01.03	A.03.01.01.c.03 A.03.01.01.d.01 A.03.01.01.d.02 A.03.01.02[01] A.03.01.02[02]		52.204-21(b)(1)(i)			AC.L1-B.1.I	AC.L1-B.1.I[a] AC.L1-B.1.I[b] AC.L1-B.1.I[c] AC.L1-B.1.I[d] AC.L1-B.1.I[e]	ACL2.-3.1.1	Annual	
	R3	R2 & R3	Identification & Authentication	IAC-20.1	P-IAC-20.1	Access To Sensitive / Regulated Data	IAC-20.1	Mechanisms exist to limit access to sensitive and/or regulated data to only those individuals whose job requires such access.			03.01.01.c.03 03.01.01.d.01 03.01.01.d.02 03.01.02 03.01.03	A.03.01.01.c.03 A.03.01.01.d.01 A.03.01.01.d.02 A.03.01.02[01] A.03.01.02[02]								Annual	
R2	R3	R2 & R3	Identification & Authentication	IAC-21	P-IAC-21	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	3.1.5	3.1.5[b] 3.1.5[c] 3.1.5[d]	03.01.01.c.03 03.01.01.d.01 03.01.01.d.02 03.01.02 03.01.04.b	A.03.01.01.c.03 A.03.01.01.d.01 A.03.01.01.d.02 A.03.01.02[01] A.03.01.02[02]							ACL2.-3.1.5	Annual	E-IAM-02 E-IAM-05 E-IAM-06
R2		R2 & R3	Identification & Authentication	IAC-21.1	P-IAC-21.1	Authorize Access to Security Functions	IAC-21.1	Mechanisms exist to limit access to security functions to explicitly-authorized privileged users.	3.1.5										ACL2.-3.1.5	Annual	
R2	R3	R2 & R3	Identification & Authentication	IAC-21.2	P-IAC-21.2	Non-Privileged Access for Non-Security Functions	IAC-21.2	Mechanisms exist to prohibit privileged users from using privileged accounts, while performing non-security functions.	3.1.6	3.1.6[a] 3.1.6[b]	03.01.06.b	A.03.01.06.b							ACL2.-3.1.6	Annual	
R2	R3	R2 & R3	Identification & Authentication	IAC-21.3	P-IAC-21.3	Management Approval For Privileged Accounts	IAC-21.3	Mechanisms exist to restrict the assignment of privileged accounts to management-approved personnel and/or roles.	3.1.5		03.01.06.a 03.01.07.a	A.03.01.06.ODP[01] A.03.01.06.a A.03.01.07.a							ACL2.-3.1.5	Annual	E-IAM-09
R2	R3	R2 & R3	Identification & Authentication	IAC-21.4	P-IAC-21.4	Auditing Use of Privileged Functions	IAC-21.4	Mechanisms exist to audit the execution of privileged functions.	3.1.7		03.01.07.b	A.03.01.07.b							ACL2.-3.1.7	Annual	
R2	R3	R2 & R3	Identification & Authentication	IAC-21.5	P-IAC-21.5	Prohibit Non-Privileged Users from Executing Privileged Functions	IAC-21.5	Mechanisms exist to prevent non-privileged users from executing privileged functions to include disabling, circumventing or altering implemented security safeguards / countermeasures.	3.1.7	3.1.7[a] 3.1.7[b] 3.1.7[c] 3.1.7[d]	03.01.07.a	A.03.01.07.a							ACL2.-3.1.7	Annual	
R2	R3	R2 & R3	Identification & Authentication	IAC-22	P-IAC-22	Account Lockout	IAC-22	Mechanisms exist to enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period and automatically locks the account when the maximum number of unsuccessful attempts is exceeded.	3.1.8	3.1.8[a] 3.1.8[b]	03.01.08.a 03.01.08.b	A.03.01.08.ODP[01] A.03.01.08.ODP[02] A.03.01.08.ODP[03] A.03.01.08.ODP[04] A.03.01.08.a A.03.01.08.b							ACL2.-3.1.8	Annual	
R2	R3	R2 & R3	Identification & Authentication	IAC-24	P-IAC-24	Session Lock	IAC-24	Mechanisms exist to initiate a session lock after an organization-defined time period of inactivity, or upon receiving a request from a user and retain the session lock until the user reestablishes access using established identification and authentication methods.	3.1.10	3.1.10[a] 3.1.10[b] 3.1.10[c]	03.01.10.a 03.01.10.b	A.03.01.10.ODP[01] A.03.01.10.ODP[02] A.03.01.10.a A.03.01.10.b							ACL2.-3.1.10	Annual	
R2	R3	R2 & R3	Identification & Authentication	IAC-24.1	P-IAC-24.1	Pattern-Hiding Displays	IAC-24.1	Mechanisms exist to implement pattern-hiding displays to conceal information previously visible on the display during the session lock.	3.1.10		03.01.10.c	A.03.01.10.c							ACL2.-3.1.10	Annual	
R2	R3	R2 & R3	Identification & Authentication	IAC-25	P-IAC-25	Session Termination	IAC-25	Automated mechanisms exist to log out users, both locally on the network and for remote sessions, at the end of the session or after an organization-defined period of inactivity.	3.1.11	3.1.11[a] 3.1.11[b]	03.01.01.h 03.01.11 03.07.05.c	A.03.01.01.ODP[05] A.03.01.01.ODP[06] A.03.01.01.h A.03.01.11.ODP[01] A.03.01.11 A.03.07.05.c[01]							ACL2.-3.1.11	Quarterly	
	R3	R2 & R3	Identification & Authentication	IAC-28	P-IAC-28	Identity Proofing (Identity Verification)	IAC-28	Mechanisms exist to verify the identity of a user before issuing authenticators or modifying access permissions.			03.05.12.a	A.03.05.12.a								Annual	E-IAM-02 E-IAM-05 E-IAM-06 E-HRS-18
	R3	R2 & R3	Identification & Authentication	IAC-28.1	P-IAC-28.1	Management Approval For New or Changed Accounts	IAC-28.1	Mechanisms exist to ensure management approvals are required for new accounts or changes in permissions to existing accounts.			03.01.01.b 03.05.05.a	A.03.01.01.b[02] A.03.05.05.a								Annual	E-IAM-09
R2	R3	R2 & R3	Incident Response	IRO-01	P-IRO-01	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	NFO - IR-1	3.6.1[a] 3.6.1[b] 3.6.1[c] 3.6.1[d] 3.6.1[e] 3.6.1[f]	03.06.01	A.03.06.01[01]								Annual	E-IRO-01
R2	R3	R2 & R3	Incident Response	IRO-02	P-IRO-02	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment;	3.6.1 3.6.2	3.6.1[a] 3.6.1[b] 3.6.1[c] 3.6.1[d] 3.6.1[e]	03.03.04.b 03.06.01 03.06.02.a 03.06.02.b 03.06.02.c	A.03.03.04.b A.03.06.01[02] A.03.06.01[03] A.03.06.01[04] A.03.06.01[05]	252.204-7012(c)(1)(i)						IRL2.-3.6.1 IRL2.-3.6.2	Annual	E-IRO-03
R2		R2 & R3	Incident Response	IRO-03	P-IRO-03	Indicators of Compromise (IOC)	IRO-03	Mechanisms exist to define specific Indicators of Compromise (IOC) to identify the signs of potential cybersecurity events.	3.14.7										SIL2.-3.14.7	Semi-Annual	E-IRO-02
R2	R3	R2 & R3	Incident Response	IRO-04	P-IRO-04	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	NFO - IR-8		03.06.01 03.06.05.a 03.06.05.a.01 03.06.05.a.02 03.06.05.a.03	A.03.06.01[01] A.03.06.02.ODP[01] A.03.06.02.ODP[02] A.03.06.05.a.01 A.03.06.05.a.02								Annual	E-IRO-01
R2	R3	R2 & R3	Incident Response	IRO-04.2	P-IRO-04.2	IRP Update	IRO-04.2	Mechanisms exist to regularly review and modify incident response practices to incorporate lessons learned, business process changes and industry developments, as necessary.	NFO - IR-1		03.06.05.c	A.03.06.05.c								Quarterly	E-IRO-07

Applies To NIST 800-171 R2 & CMMC L2	Applies To NIST 800-171 R3	Applies To Both 171 R2 & R3	NCP SCRP Policy	NCP SCRP Standard #	NCP CSQP Procedure #	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US DFARS Cybersecurity	US FAR 52.204-21	US FAR 52.204-25	US FAR 52.204-27	US CMMC 2.0 Level 1	US CMMC 2.0 Level 1 AOs	US CMMC 2.0 Level 2	Conformity Validation Cadence	Evidence Request List (ERL) #
	R3	R2 & R3	Incident Response	IRO-04.3	P-IRO-04.3	Continuous Incident Response Improvements	IRO-04.3	Mechanisms exist to use qualitative and quantitative data from incident response testing to: (1) Determine the effectiveness of incident response processes; (2) Continuously improve incident response processes; and (3) Provide incident response measures and metrics that are accurate, consistent and in a reproducible format.			03.06.04.b	A.03.06.04.b[03]							Annual	
R2	R3	R2 & R3	Incident Response	IRO-05	P-IRO-05	Incident Response Training	IRO-05	Mechanisms exist to train personnel in their incident response roles and responsibilities.	3.6.1		03.06.04.a 03.06.04.a.03	A.03.06.04.a.01 A.03.06.04.a.03							IRL2.-3.6.1	Annual	E-IRO-05 E-IRO-06
R2	R3	R2 & R3	Incident Response	IRO-06	P-IRO-06	Incident Response Testing	IRO-06	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	3.6.3	3.6.3	03.06.03	A.03.06.03.ODP[01] A.03.06.03							IRL2.-3.6.3	Annual	E-IRO-04
	R3	R2 & R3	Incident Response	IRO-07	P-IRO-07	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations.			03.06.02.b 03.06.02.d	A.03.06.02.b A.03.06.02.d								Annual	E-IRO-01 E-IRO-09
R2	R3	R2 & R3	Incident Response	IRO-08	P-IRO-08	Chain of Custody & Forensics	IRO-08	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.					252.204-7012(e)							Annual	E-IRO-01 E-IRO-10
	R3	R2 & R3	Incident Response	IRO-09	P-IRO-09	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.			03.06.02.a 03.06.02.b	A.03.06.02.a[01] A.03.06.02.a[02] A.03.06.02.b								Annual	E-IRO-03
	R3	R2 & R3	Incident Response	IRO-10	P-IRO-10	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.			03.06.02.b 03.06.02.c 03.06.02.d	A.03.06.02.ODP[01] A.03.06.02.b A.03.06.02.c A.03.06.02.d								Annual	E-IRO-01 E-IRO-11 E-IRO-13
R2	R3	R2 & R3	Incident Response	IRO-10.2	P-IRO-10.2	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive and/or regulated data incidents in a timely manner.			03.06.02.b 03.06.02.c	A.03.06.02.ODP[02] A.03.06.02.b	252.204-7012(c)(1)(ii) 252.204-7012(c)(2) 252.204-7012(c)(3) 252.204-7012(d)							Annual	E-IRO-01 E-IRO-11
	R3	R2 & R3	Incident Response	IRO-11	P-IRO-11	Incident Reporting Assistance	IRO-11	Mechanisms exist to provide incident response advice and assistance to users of Technology Assets, Applications and/or Services (TAAS) for the handling and reporting of actual and potential cybersecurity and data protection incidents.			03.06.02.d	A.03.06.02.d								Annual	
R2	R3	R2 & R3	Incident Response	IRO-11.2	P-IRO-11.2	Coordination With External Providers	IRO-11.2	Mechanisms exist to establish a direct, cooperative relationship between the organization's incident response capability and external service providers.					252.204-7012(f) 252.204-7012(g)							Annual	
	R3	R2 & R3	Incident Response	IRO-12	P-IRO-12	Sensitive / Regulated Data Spill Response	IRO-12	Mechanisms exist to respond to sensitive and/or regulated data spills.			03.01.22.b 03.06.01	A.03.01.22.b[02] A.03.06.01[01]								Semi-Annual	E-IRO-12
R2	R3	R2 & R3	Incident Response	IRO-13	P-IRO-13	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	NFO - IR-1		03.06.04.b	A.03.06.04.b[03] A.03.06.04.b[04]								Annual	E-IRO-08
	R3	R2 & R3	Incident Response	IRO-14	P-IRO-14	Regulatory & Law Enforcement Contacts	IRO-14	Mechanisms exist to maintain incident response contacts with applicable regulatory and law enforcement agencies.			03.06.02.c	A.03.06.02.ODP[02]								Annual	
R2	R3	R2 & R3	Information Assurance	IAO-01	P-IAO-01	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	NFO - CA-1		03.12.01	A.03.12.01								Annual	E-IAO-01
	R3	R2 & R3	Information Assurance	IAO-01.1	P-IAO-01.1	Assessment Boundaries	IAO-01.1	Mechanisms exist to establish the scope of assessments by defining the assessment boundary, according to people, processes and technology that directly or indirectly impact the confidentiality, integrity, availability and safety of the Technology Assets, Applications, Services and/or Data (TAASD) under review.			03.12.01	A.03.12.01								Annual	E-AST-02
R2	R3	R2 & R3	Information Assurance	IAO-02	P-IAO-02	Assessments	IAO-02	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	3.12.1		03.12.01	A.03.12.01						CAL2.-3.12.1	Semi-Annual	E-IAO-03 E-IAO-04
R2		R2 & R3	Information Assurance	IAO-02.1	P-IAO-02.1	Assessor Independence	IAO-02.1	Mechanisms exist to ensure assessors or assessment teams have the appropriate independence to conduct security, compliance and/or resilience control assessments.	NFO - CA-2(1)											Annual	
R2	R3	R2 & R3	Information Assurance	IAO-03	P-IAO-03	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and (3) Provides a [illegible]	3.12.4	3.12.4[a] 3.12.4[b] 3.12.4[c] 3.12.4[d] 3.12.4[e] 3.12.4[f]	03.01.16.a 03.04.11.a 03.04.11.b 03.15.02.a 03.15.02.a.01 03.15.02.a.02	A.03.01.16.a[01] A.03.04.11.a[02] A.03.04.11.a[03] A.03.04.11.b[01] A.03.04.11.b[02] A.03.15.02.ODP[01]						CAL2.-3.12.4	Annual	E-TDA-14
R2		R2 & R3	Information Assurance	IAO-03.1	P-IAO-03.1	Plan / Coordinate with Other Organizational Entities	IAO-03.1	Mechanisms exist to plan and coordinate Information Assurance Program (IAP) activities with affected stakeholders before conducting such activities in order to reduce the potential impact on operations.	NFO - PL-2(3)											Annual	
R2		R2 & R3	Information Assurance	IAO-03.2	P-IAO-03.2	Adequate Security for Sensitive / Regulated Data In Support of Contracts	IAO-03.2	Mechanisms exist to protect sensitive and/or regulated data that is collected, developed, received, transmitted, used or stored in support of the performance of a contract.	3.12.4										CAL2.-3.12.4	Annual	E-IAO-03
R2	R3	R2 & R3	Information Assurance	IAO-05	P-IAO-05	Capabilities Deficiency Tracking	IAO-05	Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum: (1) Deficiency tracking number; (2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies); (4) [illegible]	3.12.2	3.12.2[a] 3.12.2[b] 3.12.2[c]	03.04.11.b 03.12.02.a 03.12.02.a.01 03.12.02.a.02 03.12.02.b 03.12.02.b.01	A.03.04.11.b[01] A.03.04.11.b[02] A.03.12.02.a.01 A.03.12.02.a.02 A.03.12.02.b.01 A.03.12.02.b.02	252.204-7012(b)(2)(ii)(B)					CAL2.-3.12.2	Annual	E-RSK-03
R2	R3	R2 & R3	Maintenance	MNT-01	P-MNT-01	Maintenance Operations	MNT-01	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.	NFO - MA-1		03.04.03.c 03.07.04.a 03.07.06.a	A.03.04.03.c[01] A.03.07.04.a[01] A.03.07.04.a[02] A.03.07.06.a								Annual	E-MNT-02 E-MNT-04

Applies To NIST 800-171 R2 & CMMC L2	Applies To NIST 800-171 R3	Applies To Both 171 R2 & R3	NCP SCRP Policy	NCP SCRP Standard #	NCP CSOP Procedure #	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US DFARS Cybersecurity	US FAR 52.204-21	US FAR 52.204-25	US FAR 52.204-27	US CMMC 2.0 Level 1	US CMMC 2.0 Level 1 AOs	US CMMC 2.0 Level 2	Conformity Validation Cadence	Evidence Request List (ERL) #
R2	R3	R2 & R3	Maintenance	MNT-02	P-MNT-02	Controlled Maintenance	MNT-02	Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or Service (TAAS).	3.7.1	3.7.1	03.04.03.c 03.07.04.a 03.07.05.a	A.03.04.03.c[01] A.03.07.04.a[02] A.03.07.05.a[01]							MAL2.-3.7.1	Annual	E-MNT-04
	R3	R2 & R3	Maintenance	MNT-03	P-MNT-03	Timely Maintenance	MNT-03	Mechanisms exist to obtain maintenance support and/or spare parts for Technology Assets, Applications and/or Services (TAAS) within a defined Recovery Time Objective (RTO).			03.07.04.a	A.03.07.04.a[02]								Annual	E-MNT-04
	R3	R2 & R3	Maintenance	MNT-03.1	P-MNT-03.1	Preventative Maintenance	MNT-03.1	Mechanisms exist to perform preventive maintenance on critical Technology Assets, Applications and/or Services (TAAS).			03.07.04.a	A.03.07.04.a[02]								Annual	E-MNT-04
R2	R3	R2 & R3	Maintenance	MNT-04	P-MNT-04	Maintenance Tools	MNT-04	Mechanisms exist to control and monitor the use of system maintenance tools.	3.7.2	3.7.2[a] 3.7.2[b] 3.7.2[c] 3.7.2[d]	03.07.04.a	A.03.07.04.a[01] A.03.07.04.a[02] A.03.07.04.a[03]							MAL2.-3.7.2	Annual	
	R3	R2 & R3	Maintenance	MNT-04.1	P-MNT-04.1	Inspect Tools	MNT-04.1	Mechanisms exist to inspect maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.			03.07.04.b	A.03.07.04.b								Annual	
R2	R3	R2 & R3	Maintenance	MNT-04.2	P-MNT-04.2	Inspect Media	MNT-04.2	Mechanisms exist to check media containing diagnostic and test programs for malicious code before the media are used.	3.7.4	3.7.4		A.03.07.04.b							MAL2.-3.7.4	Annual	E-MNT-05
	R3	R2 & R3	Maintenance	MNT-04.3	P-MNT-04.3	Prevent Unauthorized Removal	MNT-04.3	Mechanisms exist to prevent or control the removal of equipment undergoing maintenance that contains organizational information.			03.07.04.c	A.03.07.04.c								Annual	
R2	R3	R2 & R3	Maintenance	MNT-05	P-MNT-05	Remote Maintenance	MNT-05	Mechanisms exist to authorize, monitor and control remote, non-local maintenance and diagnostic activities.	3.7.5	3.7.5[a] 3.7.5[b]	03.01.12.d 03.07.05.a 03.07.05.b 03.07.05.c	A.03.01.12.d[1] A.03.07.05.a[01] A.03.07.05.a[02] A.03.07.05.b[01] A.03.07.05.c[01]							MAL2.-3.7.5	Annual	
	R3	R2 & R3	Maintenance	MNT-05.1	P-MNT-05.1	Auditing Remote Maintenance	MNT-05.1	Mechanisms exist to audit remote, non-local maintenance and diagnostic sessions, as well as review the maintenance action performed during remote maintenance sessions.			03.07.05.a	A.03.07.05.a[02]								Annual	
R2		R2 & R3	Maintenance	MNT-05.2	P-MNT-05.2	Remote Maintenance Notifications	MNT-05.2	Mechanisms exist to require maintenance personnel to notify affected stakeholders when remote, non-local maintenance is planned (e.g., date/time).	NFO - MA-4(2)											Annual	
	R3	R2 & R3	Maintenance	MNT-05.3	P-MNT-05.3	Remote Maintenance Cryptographic Protection	MNT-05.3	Cryptographic mechanisms exist to protect the integrity and confidentiality of remote, non-local maintenance and diagnostic communications.			03.07.05.b	A.03.07.05.b[01]								Annual	
R2	R3	R2 & R3	Maintenance	MNT-05.4	P-MNT-05.4	Remote Maintenance Disconnect Verification	MNT-05.4	Mechanisms exist to provide remote disconnect verification to ensure remote, non-local maintenance and diagnostic sessions are properly terminated.	3.7.5		03.07.05.c	A.03.07.05.c[01]							MAL2.-3.7.5	Annual	
	R3	R2 & R3	Maintenance	MNT-05.5	P-MNT-05.5	Remote Maintenance Pre-Approval	MNT-05.5	Mechanisms exist to require maintenance personnel to obtain pre-approval and scheduling for remote, non-local maintenance sessions.			03.07.05.a	A.03.07.05.a[01]								Annual	
R2	R3	R2 & R3	Maintenance	MNT-06	P-MNT-06	Authorized Maintenance Personnel	MNT-06	Mechanisms exist to maintain a current list of authorized maintenance organizations or personnel.	3.7.6	3.7.6	03.07.06.a 03.07.06.b 03.07.06.c 03.07.06.d	A.03.07.06.a A.03.07.06.b A.03.07.06.c A.03.07.06.d[01]							MAL2.-3.7.6	Annual	
R2	R3	R2 & R3	Maintenance	MNT-06.1	P-MNT-06.1	Maintenance Personnel Without Appropriate Access	MNT-06.1	Mechanisms exist to ensure the risks associated with maintenance personnel who do not have appropriate access authorizations, clearances or formal access approvals are appropriately mitigated.	3.7.6		03.07.06.c 03.07.06.d	A.03.07.06.c A.03.07.06.d[01] A.03.07.06.d[02]							MAL2.-3.7.6	Annual	E-MNT-01
R2	R3	R2 & R3	Maintenance	MNT-06.2	P-MNT-06.2	Non-System Related Maintenance	MNT-06.2	Mechanisms exist to ensure that non-escorted personnel performing non-IT maintenance activities in the physical proximity of systems have required access authorizations.	3.7.6		03.07.06.c	A.03.07.06.c							MAL2.-3.7.6	Annual	
	R3	R2 & R3	Maintenance	MNT-09	P-MNT-09	Off-Site Maintenance	MNT-09	Mechanisms exist to ensure off-site maintenance activities are conducted securely and the asset(s) undergoing maintenance actions are secured during physical transfer and storage while off-site.			03.07.04.a	A.03.07.04.a[02]								Annual	
R2	R3	R2 & R3	Mobile Device Management	MDM-01	P-MDM-01	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	3.1.18		03.01.18.a 03.01.20.d	A.03.01.18.a[01] A.03.01.20.d							ACL2.-3.1.18	Annual	
R2	R3	R2 & R3	Mobile Device Management	MDM-02	P-MDM-02	Access Control For Mobile Devices	MDM-02	Mechanisms exist to enforce access control requirements for the connection of mobile devices to organizational Technology Assets, Applications and/or Services (TAAS).	3.1.18	3.1.18[a] 3.1.18[b] 3.1.18[c]	03.01.18.a 03.01.18.b	A.03.01.18.a[02] A.03.01.18.b							ACL2.-3.1.18	Annual	
R2	R3	R2 & R3	Mobile Device Management	MDM-03	P-MDM-03	Full Device & Container-Based Encryption	MDM-03	Cryptographic mechanisms exist to protect the confidentiality and integrity of information on mobile devices through full-device or container encryption.	3.1.19	3.1.19[a] 3.1.19[b]	03.01.18.c	A.03.01.18.c							ACL2.-3.1.19	Annual	
	R3	R2 & R3	Mobile Device Management	MDM-04	P-MDM-04	Mobile Device Tampering	MDM-04	Mechanisms exist to protect mobile devices from tampering through inspecting devices returning from locations that the organization deems to be of significant risk, prior to the device being connected to the organization's network.			03.04.12.b	A.03.04.12.b								Annual	
R2	R3	R2 & R3	Mobile Device Management	MDM-06	P-MDM-06	Personally-Owned Mobile Devices	MDM-06	Mechanisms exist to restrict the connection of personally-owned, mobile devices to organizational Technology Assets, Applications and/or Services (TAAS).	3.1.18		03.01.18.a 03.01.18.b	A.03.01.18.a[01] A.03.01.18.b							ACL2.-3.1.18	Annual	

Applies To NIST 800-171 R2 & CMMC L2	Applies To NIST 800-171 R3	Applies To Both 171 R2 & R3	NCP SCRP Policy	NCP SCRP Standard #	NCP CSOP Procedure #	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US DFARS Cybersecurity	US FAR 52.204-21	US FAR 52.204-25	US FAR 52.204-27	US CMMC 2.0 Level 1	US CMMC 2.0 Level 1 AOs	US CMMC 2.0 Level 2	Conformity Validation Cadence	Evidence Request List (ERL) #
R2	R3	R2 & R3	Mobile Device Management	MDM-07	P-MDM-07	Organization-Owned Mobile Devices	MDM-07	Mechanisms exist to prohibit the installation of non-approved applications or approved applications not obtained through the organization-approved application store.	3.1.18		03.01.18.a 03.01.18.b 03.01.20.d	A.03.01.18.a[01] A.03.01.18.b A.03.01.20.d							ACL2-.3.1.18	Annual	
	R3	R2 & R3	Mobile Device Management	MDM-11	P-MDM-11	Restricting Access To Authorized Technology Assets, Applications and/or Services (TAAS)	MDM-11	Mechanisms exist to restrict the connectivity of unauthorized mobile devices from communicating with organizational Technology Assets, Applications and/or Services (TAAS).			03.01.18.b	A.03.01.18.b								Annual	E-NET-06
R2	R3	R2 & R3	Network Security	NET-01	P-NET-01	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	3.13.1 NFO - SC-1		03.01.12.a 03.01.16.a 03.01.18.a 03.13.01.a	A.03.01.16.a[02] A.03.01.18.a[03] A.03.13.01.a[02]		52.204-21(b)(1)(x)			SC.L1-B.1.X		SCL2-.3.13.1	Annual	E-NET-04
	R3	R2 & R3	Network Security	NET-02	P-NET-02	Layered Network Defenses	NET-02	Mechanisms exist to implement security functions as a layered structure that minimizes interactions between layers of the design and avoids any dependence by lower layers on the functionality or correctness of higher layers.			03.13.01.b	A.03.13.01.b								Annual	E-DCH-03 E-DCH-04 E-DCH-05
R2	R3	R2 & R3	Network Security	NET-02.2	P-NET-02.2	Guest Networks	NET-02.2	Mechanisms exist to implement and manage a secure guest network.	3.13.1	3.13.1[e] 3.13.1[g]	03.01.16.a 03.01.16.b	A.03.01.16.a[01] A.03.01.16.a[02] A.03.01.16.a[04] A.03.01.16.b		52.204-21(b)(1)(x)			SC.L1-B.1.X		SCL2-.3.13.1	Annual	
R2	R3	R2 & R3	Network Security	NET-03	P-NET-03	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	3.13.1	3.13.1[a] 3.13.1[b] 3.13.1[c] 3.13.1[d] 3.13.1[e] 3.13.1[f]	03.01.12.a 03.01.18.a 03.13.01.a 03.13.01.b 03.13.01.c	A.03.01.18.a[03] A.03.13.01.a[02] A.03.13.01.a[04] A.03.13.01.b A.03.13.01.c		52.204-21(b)(1)(x)			SC.L1-B.1.X	SC.L1-B.1.X[a] SC.L1-B.1.X[b] SC.L1-B.1.X[c] SC.L1-B.1.X[d] SC.L1-B.1.X[e] SC.L1-B.1.X[f]	SCL2-.3.13.1	Annual	E-NET-08 E-NET-09
R2		R2 & R3	Network Security	NET-03.1	P-NET-03.1	Limit Network Connections	NET-03.1	Mechanisms exist to limit the number of concurrent external network connections to its Technology Assets, Applications and/or Services (TAAS).	NFO - SC-7(3)											Annual	
R2		R2 & R3	Network Security	NET-03.2	P-NET-03.2	External Telecommunications Services	NET-03.2	Mechanisms exist to maintain a managed interface for each external telecommunication service that protects the confidentiality and integrity of the information being transmitted across each interface.	NFO - SC-7(4)											Annual	
	R3	R2 & R3	Network Security	NET-03.8	P-NET-03.8	Separate Subnet for Connecting to Different Security Domains	NET-03.8	Mechanisms exist to implement separate network addresses (e.g., different subnets) to connect to systems in different security domains.			03.13.01.b	A.03.13.01.b								Annual	
R2	R3	R2 & R3	Network Security	NET-04	P-NET-04	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	3.1.3	3.1.3[a] 3.1.3[b] 3.1.3[c] 3.1.3[d] 3.1.3[e]	03.01.03 03.13.01.a 03.13.01.c	A.03.01.03[02] A.03.13.01.a[02] A.03.13.01.c							ACL2-.3.1.3	Annual	E-AST-12 E-AST-19 E-NET-06 E-NET-07 E-NET-10
R2	R3	R2 & R3	Network Security	NET-04.1	P-NET-04.1	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	3.13.6 NFO - CA-3(5)	3.13.6[a] 3.13.6[b]	03.13.01.a 03.13.06	A.03.13.01.a[02] A.03.13.06[01] A.03.13.06[02]							SCL2-.3.13.6	Annual	E-AST-12 E-AST-19 E-NET-07 E-NET-10
R2	R3	R2 & R3	Network Security	NET-05	P-NET-05	Interconnection Security Agreements (ISAs)	NET-05	Mechanisms exist to authorize connections from systems to other systems using Interconnection Security Agreements (ISAs), or similar methods, that document, for each interconnection: (1) Interface characteristics; (2) Security, compliance and resilience requirements; and; (3) The nature of the information communicated.	NFO - CA-3		03.01.03 03.01.20.c.02 03.12.05.a 03.12.05.b	A.03.01.03[02] A.03.01.20.c.02 A.03.12.05.ODP[01] A.03.12.05.ODP[02] A.03.12.05.a[01] A.03.12.05.a[02]								Annual	E-NET-06
R2	R3	R2 & R3	Network Security	NET-05.2	P-NET-05.2	Internal System Connections	NET-05.2	Mechanisms exist to control internal system connections through authorizing internal connections of systems and documenting, for each internal connection, the interface characteristics, security requirements and the nature of the information communicated.	NFO - CA-9		03.01.03 03.12.05.b 03.12.05.c	A.03.01.03[02]								Annual	
R2	R3	R2 & R3	Network Security	NET-06	P-NET-06	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	3.13.5	3.13.5[a] 3.13.5[b]	03.13.01.b	A.03.13.01.b		52.204-21(b)(1)(xi)			SC.L1-B.1.XI	SC.L1-B.1.XI[a] SC.L1-B.1.XI[b]	SCL2-.3.13.5	Annual	
	R3	R2 & R3	Network Security	NET-06.3	P-NET-06.3	Sensitive / Regulated Data Enclave (Secure Zone)	NET-06.3	Mechanisms exist to implement segmentation controls to restrict inbound and outbound connectivity for sensitive and/or regulated data enclaves (secure zones).			03.13.01.b	A.03.13.01.b								Annual	
R2	R3	R2 & R3	Network Security	NET-07	P-NET-07	Network Connection Termination	NET-07	Mechanisms exist to terminate network connections at the end of a session or after an organization-defined time period of inactivity.	3.13.9	3.13.9[a] 3.13.9[b] 3.13.9[c]	03.07.05.c 03.13.09	A.03.07.05.c[02] A.03.13.09.ODP[01] A.03.13.09							SCL2-.3.13.9	Annual	
R2	R3	R2 & R3	Network Security	NET-08	P-NET-08	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-08	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	3.14.6		03.13.01.a 03.14.06.c	A.03.13.01.a[02] A.03.14.06.c[01]							SIL2-.3.14.6	Annual	
	R3	R2 & R3	Network Security	NET-08.1	P-NET-08.1	DMZ Networks	NET-08.1	Mechanisms exist to monitor De-Militarized Zone (DMZ) network segments to separate untrusted networks from trusted networks.			03.13.01.b	A.03.13.01.b								Annual	
R2	R3	R2 & R3	Network Security	NET-09	P-NET-09	Session Integrity	NET-09	Mechanisms exist to protect the authenticity and integrity of communications sessions.	3.13.15	3.13.15	03.13.15	A.03.13.15							SCL2-.3.13.15	Annual	
R2		R2 & R3	Network Security	NET-10	P-NET-10	Domain Name Service (DNS) Resolution	NET-10	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	NFO - SC-20											Annual	
R2		R2 & R3	Network Security	NET-10.1	P-NET-10.1	Architecture & Provisioning for Name / Address Resolution Service	NET-10.1	Mechanisms exist to ensure systems that collectively provide Domain Name Service (DNS) resolution service are fault-tolerant and implement internal/external role separation.	NFO - SC-22											Annual	
R2		R2 & R3	Network Security	NET-10.2	P-NET-10.2	Secure Name / Address Resolution Service (Recursive or Caching Resolver)	NET-10.2	Mechanisms exist to perform data origin authentication and data integrity verification on the Domain Name Service (DNS) resolution responses received from authoritative sources when requested by client systems.	NFO - SC-21											Annual	

Applies To NIST 800-171 R2 & CMMC L2	Applies To NIST 800-171 R3	Applies To Both 171 R2 & R3	NCP SCRP Policy	NCP SCRP Standard #	NCP CSOP Procedure #	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US DFARS Cybersecurity	US FAR 52.204-21	US FAR 52.204-25	US FAR 52.204-27	US CMMC 2.0 Level 1	US CMMC 2.0 Level 1 AOs	US CMMC 2.0 Level 2	Conformity Validation Cadence	Evidence Request List (ERL) #
R2		R2 & R3	Network Security	NET-13	P-NET-13	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	3.13.14	3.13.14[a] 3.13.14[b]									SCL2-.3.13.14	Annual	
R2	R3	R2 & R3	Network Security	NET-14	P-NET-14	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	3.1.12		03.01.12.a 03.01.12.b 03.01.12.c	A.03.01.12.a[01] A.03.01.12.a[02] A.03.01.12.a[04] A.03.01.12.b A.03.01.12.c[01] A.03.01.12.c[02]							AC L2-.3.1.12	Annual	E-NET-03 E-IAM-14
R2	R3	R2 & R3	Network Security	NET-14.1	P-NET-14.1	Automated Monitoring & Control	NET-14.1	Automated mechanisms exist to monitor and control remote access sessions.	3.1.12	3.1.12[a] 3.1.12[b] 3.1.12[c] 3.1.12[d]	03.01.12.b	A.03.01.12.b							AC L2-.3.1.12	Quarterly	
R2	R3	R2 & R3	Network Security	NET-14.2	P-NET-14.2	Protection of Confidentiality / Integrity Using Encryption	NET-14.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of remote access sessions (e.g., VPN).	3.1.13	3.1.13[a] 3.1.13[b]	03.01.12.a	A.03.01.12.a[04]							AC L2-.3.1.13	Annual	
R2	R3	R2 & R3	Network Security	NET-14.3	P-NET-14.3	Managed Access Control Points	NET-14.3	Mechanisms exist to route all remote accesses through managed network access control points (e.g., VPN concentrator).	3.1.14	3.1.14[a] 3.1.14[b]	03.01.12.c	A.03.01.12.c[01] A.03.01.12.c[02]							AC L2-.3.1.14	Annual	E-NET-09
R2	R3	R2 & R3	Network Security	NET-14.4	P-NET-14.4	Remote Privileged Commands & Sensitive Data Access	NET-14.4	Mechanisms exist to restrict the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs.	3.1.15	3.1.15[a] 3.1.15[b] 3.1.15[c] 3.1.15[d]	03.01.12.d	A.03.01.12.d[1] A.03.01.12.d[2]							AC L2-.3.1.15	Annual	
R2	R3	R2 & R3	Network Security	NET-14.5	P-NET-14.5	Work From Anywhere (WFA) - Telecommuting Security	NET-14.5	Mechanisms exist to define secure telecommuting practices and govern remote access to Technology Assets, Applications, Services and/or Data (TAASD) for remote workers.	3.1.12 3.10.6		03.01.12.a 03.10.06.a 03.10.06.b	A.03.01.12.a[01] A.03.10.06.ODP[01] A.03.10.06.a A.03.10.06.b							AC L2-.3.1.12 PE L2-.3.10.6	Annual	E-NET-03 E-IAM-14
R2	R3	R2 & R3	Network Security	NET-15	P-NET-15	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	3.1.16	3.1.16[a] 3.1.16[b]	03.01.16.a 03.01.16.b	A.03.01.16.a[01] A.03.01.16.a[02] A.03.01.16.a[04] A.03.01.16.b							AC L2-.3.1.16	Annual	
R2	R3	R2 & R3	Network Security	NET-15.1	P-NET-15.1	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	3.1.17	3.1.17[a] 3.1.17[b]	03.01.16.a 03.01.16.b 03.01.16.d	A.03.01.16.a[04] A.03.01.16.b A.03.01.16.d[01] A.03.01.16.d[02]							AC L2-.3.1.17	Annual	
	R3	R2 & R3	Network Security	NET-15.2	P-NET-15.2	Disable Wireless Networking	NET-15.2	Mechanisms exist to disable unnecessary wireless networking capabilities that are internally embedded within system components prior to issuance to end users.			03.01.16.c	A.03.01.16.c								Annual	
	R3	R2 & R3	Network Security	NET-15.3	P-NET-15.3	Restrict Configuration By Users	NET-15.3	Mechanisms exist to identify and explicitly authorize users who are allowed to independently configure wireless networking capabilities.			03.01.16.a 03.01.16.c	A.03.01.16.a[03] A.03.01.16.c								Annual	
R2	R3	R2 & R3	Network Security	NET-18	P-NET-18	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	3.1.3		03.14.06.c	A.03.14.06.c[02]							AC L2-.3.1.3	Annual	E-NET-01
R2	R3	R2 & R3	Physical & Environmental Security	PES-01	P-PES-01	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	3.10.2 NFO - PE-1	3.10.2[a] 3.10.2[b] 3.10.2[c] 3.10.2[d]	03.08.01 03.08.02 03.10.01.a 03.10.07.a 03.10.07.a.01	A.03.08.01[01] A.03.08.01[02] A.03.08.02 A.03.10.01.a[01] A.03.10.01.a[02] A.03.10.01.a[03]							PE L2-.3.10.2	Annual	E-PES-01 E-PES-05
R2	R3	R2 & R3	Physical & Environmental Security	PES-02	P-PES-02	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	3.10.1	3.10.1[a] 3.10.1[b] 3.10.1[c] 3.10.1[d]	03.04.05 03.08.01 03.08.02 03.10.01.a 03.10.01.b 03.10.01.c	A.03.04.05[02] A.03.08.01[01] A.03.08.01[02] A.03.08.02 A.03.10.01.ODP[01] A.03.10.01.a[01]		52.204-21(b)(1)(viii)			PE.L1-B.1.VIII	PE.L1-B.1.VIII[a] PE.L1-B.1.VIII[b] PE.L1-B.1.VIII[c] PE.L1-B.1.VIII[d]	PE L2-.3.10.1	Annual	E-HRS-28 E-PES-03 E-PES-05 E-PES-10
R2	R3	R2 & R3	Physical & Environmental Security	PES-02.1	P-PES-02.1	Role-Based Physical Access	PES-02.1	Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.	3.10.1		03.04.05 03.08.01 03.08.02 03.10.01.b 03.10.01.d	A.03.04.05[01] A.03.08.01[01] A.03.08.01[02] A.03.08.02 A.03.10.01.ODP[01] A.03.10.01.b		52.204-21(b)(1)(viii)			PE.L1-B.1.VIII		PE L2-.3.10.1	Annual	E-PES-03 E-PES-05 E-PES-10
R2	R3	R2 & R3	Physical & Environmental Security	PES-03	P-PES-03	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	3.10.3 3.10.5	3.10.5[a] 3.10.5[b] 3.10.5[c]	03.04.05 03.10.02.a 03.10.07.a 03.10.07.a.01 03.10.07.a.02 03.10.07.d	A.03.04.05[03] A.03.10.02.a[01] A.03.10.07.a.01 A.03.10.07.a.02 A.03.10.07.d		52.204-21(b)(1)(ix)			PE.L1-B.1.IX	PE.L1-B.1.IX[a] PE.L1-B.1.IX[d] PE.L1-B.1.IX[e] PE.L1-B.1.IX[f]	PE L2-.3.10.3 PE L2-.3.10.5	Annual	E-PES-05 E-PES-06 E-PES-07 E-PES-08 E-PES-09
	R3	R2 & R3	Physical & Environmental Security	PES-03.1	P-PES-03.1	Controlled Ingress & Egress Points	PES-03.1	Physical access control mechanisms exist to limit and monitor physical access through controlled ingress and egress points.			03.10.02.a 03.10.07.a 03.10.07.a.01 03.10.07.a.02	A.03.10.02.a[01] A.03.10.07.a.01 A.03.10.07.a.02								Annual	E-PES-12
R2	R3	R2 & R3	Physical & Environmental Security	PES-03.3	P-PES-03.3	Physical Access Logs	PES-03.3	Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points.	3.10.4 NFO - PE-8	3.10.4	03.10.02.a 03.10.07.a.02 03.10.07.b	A.03.10.02.a[01] A.03.10.07.a.02 A.03.10.07.b						PE.L1-B.1.IX[c]	PE L2-.3.10.4	Annual	E-PES-02
R2	R3	R2 & R3	Physical & Environmental Security	PES-03.4	P-PES-03.4	Access To Critical Systems	PES-03.4	Physical access control mechanisms exist to enforce physical access to critical systems or sensitive and/or regulated data, in addition to the physical access controls for the facility.	3.10.1		03.10.07.a.01 03.10.07.a.02	A.03.10.07.a.01 A.03.10.07.a.02		52.204-21(b)(1)(viii)			PE.L1-B.1.VIII		PE L2-.3.10.1	Annual	
R2	R3	R2 & R3	Physical & Environmental Security	PES-04	P-PES-04	Physical Security of Offices, Rooms & Facilities	PES-04	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	3.10.5		03.08.01 03.08.02 03.10.07.a.01 03.10.07.a.02 03.10.07.d	A.03.08.01[01] A.03.08.01[02] A.03.08.02 A.03.10.07.a.01 A.03.10.07.a.02 A.03.10.07.d		52.204-21(b)(1)(viii)			PE.L1-B.1.VIII		PE L2-.3.10.5	Annual	
	R3	R2 & R3	Physical & Environmental Security	PES-04.1	P-PES-04.1	Working in Secure Areas	PES-04.1	Physical security mechanisms exist to allow only authorized personnel access to secure areas.			03.08.01 03.08.02 03.10.07.a.01 03.10.07.a.02 03.10.07.d	A.03.08.01[01] A.03.08.01[02] A.03.08.02 A.03.10.07.a.01 A.03.10.07.a.02 A.03.10.07.d								Annual	
R2	R3	R2 & R3	Physical & Environmental Security	PES-05	P-PES-05	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	3.10.2	3.10.2[c] 3.10.2[d]	03.10.02.a 03.10.02.b	A.03.10.02.ODP[01] A.03.10.02.ODP[02] A.03.10.02.a[01] A.03.10.02.a[02] A.03.10.02.b[01] A.03.10.02.b[02]							PE L2-.3.10.2	Semi-Annual	E-PES-05

Applies To NIST 800-171 R2 & CMMC L2	Applies To NIST 800-171 R3	Applies To Both 171 R2 & R3	NCP SCRP Policy	NCP SCRP Standard #	NCP CSOP Procedure #	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US DFARS Cybersecurity	US FAR 52.204-21	US FAR 52.204-25	US FAR 52.204-27	US CMMC 2.0 Level 1	US CMMC 2.0 Level 1 AOs	US CMMC 2.0 Level 2	Conformity Validation Cadence	Evidence Request List (ERL) #
R2	R3	R2 & R3	Physical & Environmental Security	PES-05.1	P-PES-05.1	Intrusion Alarms / Surveillance Equipment	PES-05.1	Physical access control mechanisms exist to monitor physical intrusion alarms and surveillance equipment.	3.10.2 NFO - PE-6(1)	3.10.2[c] 3.10.2[d]	03.10.02.a	A.03.10.02.a[01]							PEL2.-3.10.2	Annual	
R2	R3	R2 & R3	Physical & Environmental Security	PES-05.2	P-PES-05.2	Monitoring Physical Access To Critical Systems	PES-05.2	Facility security mechanisms exist to monitor physical access to critical systems or sensitive and/or regulated data, in addition to the physical access monitoring of the facility.	3.10.2	3.10.2[c] 3.10.2[d]	03.10.02.a 03.10.02.b	A.03.10.02.a[01] A.03.10.02.b[01] A.03.10.02.b[02]							PEL2.-3.10.2	Annual	
R2	R3	R2 & R3	Physical & Environmental Security	PES-06	P-PES-06	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	3.10.3	3.10.3[a] 3.10.3[b]	03.10.01.a 03.10.07.c	A.03.10.01.a[02] A.03.10.07.c[01] A.03.10.07.c[02]		52.204-21(b)(1)(ix)			PE.L1-B.1.IX		PEL2.-3.10.3	Annual	E-PES-02
R2	R3	R2 & R3	Physical & Environmental Security	PES-06.1	P-PES-06.1	Distinguish Visitors from On-Site Personnel	PES-06.1	Physical access control mechanisms exist to easily distinguish between onsite personnel and visitors, especially in areas where sensitive and/or regulated data is accessible.	3.10.3	3.10.3[a] 3.10.3[b]	03.10.01.a 03.10.07.c	A.03.10.01.a[02] A.03.10.07.c[01] A.03.10.07.c[02]		52.204-21(b)(1)(ix)			PE.L1-B.1.IX		PEL2.-3.10.3	Annual	
	R3	R2 & R3	Physical & Environmental Security	PES-06.2	P-PES-06.2	Identification Requirement	PES-06.2	Physical access control mechanisms exist to requires at least one(1) form of government-issued or organization-issued photo identification to authenticate individuals before they can gain access to the facility.			03.10.07.c	A.03.10.07.c[01] A.03.10.07.c[02]								Annual	
R2	R3	R2 & R3	Physical & Environmental Security	PES-06.3	P-PES-06.3	Restrict Unescorted Access	PES-06.3	Physical access control mechanisms exist to restrict unescorted access to facilities to personnel with required security clearances, formal access authorizations and validate the need for access.	3.10.3	3.10.3[a] 3.10.3[b]	03.10.07.c	A.03.10.07.c[01] A.03.10.07.c[02]		52.204-21(b)(1)(ix)			PE.L1-B.1.IX	PE.L1-B.1.IX[b]	PEL2.-3.10.3	Annual	
	R3	R2 & R3	Physical & Environmental Security	PES-06.6	P-PES-06.6	Visitor Access Revocation	PES-06.6	Mechanisms exist to ensure visitor badges, or other issued identification, are surrendered before visitors leave the facility or are deactivated at a pre-determined time/date of expiration.			03.10.07.c	A.03.10.07.c[01] A.03.10.07.c[02]								Annual	
	R3	R2 & R3	Physical & Environmental Security	PES-07	P-PES-07	Supporting Utilities	PES-07	Facility security mechanisms exist to protect power equipment and power cabling for the system from damage and destruction.			03.10.08	A.03.10.08								Annual	E-PES-01
R2		R2 & R3	Physical & Environmental Security	PES-10	P-PES-10	Delivery & Removal	PES-10	Physical security mechanisms exist to isolate information processing facilities from points such as delivery and loading areas and other points to avoid unauthorized access.	NFO - PE-16											Annual	
R2	R3	R2 & R3	Physical & Environmental Security	PES-11	P-PES-11	Alternate Work Site	PES-11	Physical security mechanisms exist to utilize appropriate management, operational and technical controls at alternate work sites.	3.10.6	3.10.6[a] 3.10.6[b]	03.10.06.a 03.10.06.b	A.03.10.06.ODP[01] A.03.10.06.a A.03.10.06.b							PEL2.-3.10.6	Annual	
R2	R3	R2 & R3	Physical & Environmental Security	PES-12	P-PES-12	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	3.10.1		03.10.07.e 03.10.08	A.03.10.07.e A.03.10.08		52.204-21(b)(1)(viii)			PE.L1-B.1.VIII		PEL2.-3.10.1	Annual	
R2	R3	R2 & R3	Physical & Environmental Security	PES-12.1	P-PES-12.1	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	3.10.1		03.10.08	A.03.10.08		52.204-21(b)(1)(viii)			PE.L1-B.1.VIII		PEL2.-3.10.1	Annual	
R2	R3	R2 & R3	Physical & Environmental Security	PES-12.2	P-PES-12.2	Access Control for Output Devices	PES-12.2	Physical security mechanisms exist to restrict access to printers and other system output devices to prevent unauthorized individuals from obtaining the output.	3.10.1		03.10.07.e	A.03.10.07.e		52.204-21(b)(1)(viii)			PE.L1-B.1.VIII		PEL2.-3.10.1	Annual	
R2	R3	R2 & R3	Project & Resource Management	PRM-01	P-PRM-01	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	NFO - PL-1		03.16.01	A.03.16.01								Annual	E-PRM-02
R2		R2 & R3	Project & Resource Management	PRM-03	P-PRM-03	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	NFO - SA-2											Annual	E-PRM-01 E-PRM-02
	R3	R2 & R3	Project & Resource Management	PRM-05	P-PRM-05	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to proactively govern Technology Assets, Applications and/or Services (TAAS) by: (1) Defining technical security, compliance and resilience requirements; and (2) Performing a criticality analysis at pre-defined decision points in the Secure Development Life Cycle (SDLC).			03.16.01	A.03.16.01								Annual	E-PRM-03 E-PRM-05
R2		R2 & R3	Project & Resource Management	PRM-07	P-PRM-07	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	NFO - SA-3											Annual	E-PRM-03
R2	R3	R2 & R3	Risk Management	RSK-01	P-RSK-01	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with: (1) The organization's Enterprise Risk Management (ERM); and (2) Industry-recognized cybersecurity risk management practices.	NFO - RA-1		03.11.01.a 03.17.01.a 03.17.03.b	A.03.11.01.a A.03.17.01.a[01] A.03.17.03.b								Annual	E-RSK-01
	R3	R2 & R3	Risk Management	RSK-01.1	P-RSK-01.1	Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.			03.11.01.a	A.03.11.01.a								Annual	E-RSK-01 E-RSK-06 E-RSK-07 E-RSK-08
	R3	R2 & R3	Risk Management	RSK-02	P-RSK-02	Risk-Based Security Categorization	RSK-02	Mechanisms exist to categorize Technology Assets, Applications, Services and/or Data (TAASD) in accordance with applicable laws, regulations and contractual obligations that: (1) Document the security categorization results (including supporting rationale) in the security plan for systems; and (2) Ensure the security categorization decision is reviewed and approved by the asset owner.			03.11.01.a	A.03.11.01.a								Annual	E-RSK-01 E-RSK-04 E-BCM-08 E-TPM-02
	R3	R2 & R3	Risk Management	RSK-02.1	P-RSK-02.1	Impact-Level Prioritization	RSK-02.1	Mechanisms exist to prioritize the impact level for Technology Assets, Applications and/or Services (TAAS) to prevent potential disruptions.			03.11.01.a 03.14.03.b	A.03.11.01.a A.03.14.03.a								Annual	E-BCM-08 E-RSK-04 E-TPM-02
	R3	R2 & R3	Risk Management	RSK-03	P-RSK-03	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.			03.11.01.a	A.03.11.01.a								Annual	E-RSK-04

Applies To NIST 800-171 R2 & CMMC L2	Applies To NIST 800-171 R3	Applies To Both 171 R2 & R3	NCP SCRP Policy	NCP SCRP Standard #	NCP CSOP Procedure #	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US DFARS Cybersecurity	US FAR 52.204-21	US FAR 52.204-25	US FAR 52.204-27	US CMMC 2.0 Level 1	US CMMC 2.0 Level 1 AOs	US CMMC 2.0 Level 2	Conformity Validation Cadence	Evidence Request List (ERL) #
	R3	R2 & R3	Risk Management	RSK-03.1	P-RSK-03.1	Risk Catalog	RSK-03.1	Mechanisms exist to develop and keep current a catalog of applicable risks associated with the organization's business operations and technologies in use.			03.11.01.a 03.15.02.a.03	A.03.11.01.a								Annual	E-RSK-09
R2	R3	R2 & R3	Risk Management	RSK-04	P-RSK-04	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3.11.1	3.11.1[a] 3.11.1[b]	03.11.01.a	A.03.11.01.a							RAL2.-3.11.1	Annual	E-RSK-04
	R3	R2 & R3	Risk Management	RSK-04.1	P-RSK-04.1	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.			03.12.02.a.01 03.12.02.a.02	A.03.12.02.a.01 A.03.12.02.a.02								Semi-Annual	E-RSK-03
	R3	R2 & R3	Risk Management	RSK-05	P-RSK-05	Risk Ranking	RSK-05	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities that is based on industry-recognized practices.			03.11.01.a	A.03.11.01.a								Annual	E-RSK-04
R2	R3	R2 & R3	Risk Management	RSK-06	P-RSK-06	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	3.11.3		03.11.02.b 03.12.02.a.02	A.03.11.02.b A.03.12.02.a.02							RAL2.-3.11.3	Semi-Annual	E-RSK-03
	R3	R2 & R3	Risk Management	RSK-06.1	P-RSK-06.1	Risk Response	RSK-06.1	Mechanisms exist to ensure proper risk response actions were performed to remediate findings from security, compliance and/or resilience-related: (1) Assessments; (2) Audits; and/or (3) Incidents.			03.11.02.b 03.11.04	A.03.11.02.b A.03.11.04[01] A.03.11.04[02] A.03.11.04[03]								Semi-Annual	E-RSK-03
R2	R3	R2 & R3	Risk Management	RSK-06.2	P-RSK-06.2	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.			03.11.02.b	A.03.11.02.b	252.204-7012(b)(2)(ii)(B) 252.204-7012(b)(2)(ii)(C)							Annual	E-GOV-20 E-RSK-03
	R3	R2 & R3	Risk Management	RSK-07	P-RSK-07	Risk Assessment Update	RSK-07	Mechanisms exist to routinely update risk assessments and react accordingly upon identifying new security vulnerabilities, including using outside sources for security vulnerability information.			03.11.01.b	A.03.11.01.ODP[01] A.03.11.01.b								Annual	
	R3	R2 & R3	Risk Management	RSK-09	P-RSK-09	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.			03.11.01.a 03.17.01.a 03.17.01.b 03.17.03.a 03.17.03.b	A.03.11.01.a A.03.17.01.ODP[01] A.03.17.01.a[01] A.03.17.01.a[02] A.03.17.01.a[03] A.03.17.01.a[04]								Annual	E-RSK-02
	R3	R2 & R3	Risk Management	RSK-09.1	P-RSK-09.1	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).			03.11.01.a 03.11.01.b 03.17.03.a	A.03.11.01.a A.03.11.01.b A.03.17.03.a[01]								Annual	E-RSK-05
R2	R3	R2 & R3	Secure Engineering & Architecture	SEA-01	P-SEA-01	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	3.13.2	3.13.2[a] 3.13.2[c] 3.13.2[d] 3.13.2[f]	03.01.12.a 03.01.16.a 03.01.16.c 03.01.18.a 03.13.01.c 03.16.01	A.03.01.12.a[04] A.03.01.16.a[02] A.03.01.16.c A.03.01.18.a[01] A.03.13.01.c A.03.16.01.ODP[01]							SCL2.-3.13.2	Annual	E-TDA-01 E-TDA-02 E-TDA-04 E-TDA-08 E-TDA-09
R2	R3	R2 & R3	Secure Engineering & Architecture	SEA-02	P-SEA-02	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	NFO - PL-8		03.01.12.a 03.01.16.a 03.01.18.a 03.13.01.c 03.16.01	A.03.01.16.a[02] A.03.01.18.a[01] A.03.13.01.c A.03.16.01								Annual	E-TDA-04 E-TDA-09
R2	R3	R2 & R3	Secure Engineering & Architecture	SEA-02.1	P-SEA-02.1	Standardized Terminology	SEA-02.1	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.						52.204-21(a)						Annual	
R2		R2 & R3	Secure Engineering & Architecture	SEA-03	P-SEA-03	Defense-In-Depth (DiD) Architecture	SEA-03	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	3.13.2											SCL2.-3.13.2	Annual	E-TDA-04 E-TDA-09
R2		R2 & R3	Secure Engineering & Architecture	SEA-03.2	P-SEA-03.2	Application Partitioning	SEA-03.2	Mechanisms exist to separate user functionality from system management functionality.	3.13.3	3.13.3[a] 3.13.3[b] 3.13.3[c]									SCL2.-3.13.3	Annual	
R2		R2 & R3	Secure Engineering & Architecture	SEA-04	P-SEA-04	Process Isolation	SEA-04	Mechanisms exist to implement a separate execution domain for each executing process.	NFO - SC-39											Annual	
R2	R3	R2 & R3	Secure Engineering & Architecture	SEA-05	P-SEA-05	Information In Shared Resources	SEA-05	Mechanisms exist to prevent unauthorized and unintended information transfer via shared system resources.	3.13.4	3.13.4	03.13.04	A.03.13.04[01] A.03.13.04[02]							SCL2.-3.13.4	Annual	
R2	R3	R2 & R3	Secure Engineering & Architecture	SEA-07	P-SEA-07	Predictable Failure Analysis	SEA-07	Mechanisms exist to determine the Mean Time to Failure (MTTF) for system components in specific environments of operation.	NFO - SA-3		03.16.02.b	A.03.16.02.b								Annual	E-AST-09
R2	R3	R2 & R3	Secure Engineering & Architecture	SEA-07.1	P-SEA-07.1	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	NFO - SA-3		03.16.02.a 03.16.02.b	A.03.16.02.a A.03.16.02.b								Annual	E-AST-09
R2		R2 & R3	Secure Engineering & Architecture	SEA-10	P-SEA-10	Memory Protection	SEA-10	Mechanisms exist to implement security safeguards to protect system memory from unauthorized code execution.	NFO - SI-16											Annual	
R2	R3	R2 & R3	Secure Engineering & Architecture	SEA-18	P-SEA-18	System Use Notification (Logon Banner)	SEA-18	Mechanisms exist to utilize system use notification / logon banners that display an approved system use notification message or banner before granting access to Technology Assets, Applications and/or Services (TAAS).	3.1.9	3.1.9[a] 3.1.9[b]	03.01.09	A.03.01.09							ACL2.-3.1.9	Annual	E-SEA-01
R2	R3	R2 & R3	Secure Engineering & Architecture	SEA-18.1	P-SEA-18.1	Standardized Microsoft Windows Banner	SEA-18.1	Mechanisms exist to configure Microsoft Windows-based systems to display an approved logon banner before granting access to the system.	3.1.9	3.1.9[a] 3.1.9[b]	03.01.09	A.03.01.09							ACL2.-3.1.9	Annual	E-SEA-01

Applies To NIST 800-171 R2 & CMMC L2	Applies To NIST 800-171 R3	Applies To Both 171 R2 & R3	NCP SCRP Policy	NCP SCRP Standard #	NCP CSQP Procedure #	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US DFARS Cybersecurity	US FAR 52.204-21	US FAR 52.204-25	US FAR 52.204-27	US CMMC 2.0 Level 1	US CMMC 2.0 Level 1 AOs	US CMMC 2.0 Level 2	Conformity Validation Cadence	Evidence Request List (ERL) #
R2	R3	R2 & R3	Secure Engineering & Architecture	SEA-18.2	P-SEA-18.2	Truncated Banner	SEA-18.2	Mechanisms exist to utilize a truncated system use notification / logon banner on systems not capable of displaying a logon banner from a centralized directory services technology (e.g., Active Directory, Entra ID, etc.).	3.1.9	3.1.9[a] 3.1.9[b]	03.01.09	A.03.01.09							ACL2.-3.1.9	Annual	E-SEA-01
R2		R2 & R3	Secure Engineering & Architecture	SEA-20	P-SEA-20	Clock Synchronization	SEA-20	Mechanisms exist to utilize time-synchronization technology to synchronize all critical system clocks.	3.3.7										AUL2.-3.3.7	Annual	
	R3	R2 & R3	Security Operations	OPS-01	P-OPS-01	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.			03.15.01.a 03.15.01.b	A.03.15.01.a[03]								Annual	E-HRS-01 E-HRS-03 E-HRS-04 E-HRS-13 E-HRS-15 E-HRS-27
	R3	R2 & R3	Security Operations	OPS-01.1	P-OPS-01.1	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.			03.15.01.a	A.03.15.01.a[03] A.03.15.01.a[04]								Annual	E-GOV-11
	R3	R2 & R3	Security Operations	OPS-03	P-OPS-03	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.			03.15.01.a	A.03.15.01.a[04]								Annual	E-TPM-04
R2	R3	R2 & R3	Security Awareness & Training	SAT-01	P-SAT-01	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	NFO - AT-1		03.02.01.a	A.03.02.01.ODP[01] A.03.02.01.ODP[02] A.03.02.01.a.01[01]								Annual	E-SAT-02 E-SAT-04 E-SAT-05
	R3	R2 & R3	Security Awareness & Training	SAT-01.1	P-SAT-01.1	Maintaining Workforce Development Relevancy	SAT-01.1	Mechanisms exist to periodically review security workforce development and awareness training to account for changes to: (1) Organizational policies, standards and procedures; (2) Assigned roles and responsibilities; (3) Relevant threats and risks; and (4) Technological developments.			03.02.01.b 03.02.02.a.02 03.02.02.b 03.06.04.b	A.03.02.01.b[01] A.03.02.01.b[02] A.03.02.02.b[01] A.03.02.02.b[02] A.03.06.04.ODP[03] A.03.06.04.ODP[04]									Annual	
R2	R3	R2 & R3	Security Awareness & Training	SAT-02	P-SAT-02	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	3.2.1	3.2.1[a] 3.2.1[b] 3.2.1[c] 3.2.1[d]	03.01.22.a 03.02.01.a.01 03.02.01.a.02 03.02.01.a.03 03.06.04.a.03	A.03.01.22.a A.03.02.01.ODP[03] A.03.02.01.ODP[04] A.03.02.01.a.01[01] A.03.02.01.a.03[03] A.03.02.01.a.03[04]							ATL2.-3.2.1	Annual	E-SAT-02
	R3	R2 & R3	Security Awareness & Training	SAT-02.2	P-SAT-02.2	Social Engineering & Mining	SAT-02.2	Mechanisms exist to include awareness training on recognizing and reporting potential and actual instances of social engineering and social mining.			03.02.01.a.03	A.03.02.01.a.03[03] A.03.02.01.a.03[05] A.03.02.01.a.03[06]								Annual	E-SAT-02
R2	R3	R2 & R3	Security Awareness & Training	SAT-03	P-SAT-03	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	3.2.2	3.2.2[a] 3.2.2[b] 3.2.2[c]	03.01.22.a 03.02.01.a.01 03.02.01.a.02 03.02.02.a 03.02.02.a.01 03.02.02.a.02	A.03.01.22.a A.03.02.01.a.01[01] A.03.02.01.a.01[02] A.03.02.01.a.02 A.03.02.02.ODP[01] A.03.02.02.ODP[02]							ATL2.-3.2.2	Annual	E-SAT-05
	R3	R2 & R3	Security Awareness & Training	SAT-03.3	P-SAT-03.3	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive and/or regulated data is formally trained in data handling requirements.			03.01.22.a 03.02.01.a.01 03.02.02.a.01	A.03.01.22.a A.03.02.01.a.01[01] A.03.02.02.a.01[01]								Annual	
	R3	R2 & R3	Security Awareness & Training	SAT-03.5	P-SAT-03.5	Privileged Users	SAT-03.5	Mechanisms exist to provide specific training for privileged users to ensure privileged users understand their unique roles and responsibilities			03.02.01.a.01 03.02.02.a.01	A.03.02.01.a.01[01] A.03.02.02.a.01[01]								Annual	E-SAT-05
R2	R3	R2 & R3	Security Awareness & Training	SAT-03.6	P-SAT-03.6	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based security, compliance and resilience awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	3.2.3		03.02.01.a.01 03.02.01.a.02 03.02.01.a.03 03.02.02.a.01 03.02.02.a.02 03.06.04.a.02	A.03.02.01.a.01[01] A.03.02.01.a.02 A.03.02.01.b[02] A.03.02.02.a.01[01] A.03.02.02.a.02 A.03.06.04.a.02							ATL2.-3.2.3	Annual	E-SAT-04
R2		R2 & R3	Security Awareness & Training	SAT-04	P-SAT-04	Security, Compliance & Resilience Training Records	SAT-04	Mechanisms exist to document, retain and monitor individual training activities, including: (1) Initial security, compliance and resilience awareness training; (2) Recurring awareness training; and (3) Technology Assets, Applications and/or Services (TAAS)-specific training.	NFO - AT-4											Annual	E-SAT-02 E-SAT-03 E-SAT-04 E-SAT-05 E-SAT-06 E-SAT-07
R2	R3	R2 & R3	Technology Development & Acquisition	TDA-01	P-TDA-01	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	NFO - SA-4		03.12.01 03.12.03 03.14.01.a 03.16.01 03.17.02	A.03.12.01 A.03.12.03[01] A.03.14.01.a[01] A.03.16.01.ODP[01] A.03.16.01 A.03.17.02[04]								Annual	E-TDA-01 E-TDA-02 E-TDA-08 E-TDA-17
	R3	R2 & R3	Technology Development & Acquisition	TDA-01.1	P-TDA-01.1	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and			03.12.03	A.03.12.03[01]								Annual	E-CPL-06 E-TDA-05 E-TDA-06 E-TDA-07 E-TDA-15 E-TDA-17
R2	R3	R2 & R3	Technology Development & Acquisition	TDA-02	P-TDA-02	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	NFO - SA-4		03.16.01	A.03.16.01								Annual	E-TDA-06
R2		R2 & R3	Technology Development & Acquisition	TDA-02.1	P-TDA-02.1	Ports, Protocols & Services In Use	TDA-02.1	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to identify early in the Secure Development Life Cycle (SDLC), the functions, ports, protocols and services intended for use.	NFO - SA-4(9)											Annual	E-CPL-06 E-TDA-07
R2		R2 & R3	Technology Development & Acquisition	TDA-02.2	P-TDA-02.2	Information Assurance Enabled Products	TDA-02.2	Mechanisms exist to limit the use of commercially-provided Information Assurance (IA) and IA-enabled IT products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile or the cryptographic module is FIPS-validated or NSA-approved.	NFO - SA-4(10)											Annual	
	R3	R2 & R3	Technology Development & Acquisition	TDA-02.3	P-TDA-02.3	Development Methods, Techniques & Processes	TDA-02.3	Mechanisms exist to require software developers to ensure that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality control processes and validation techniques to minimize flawed and/or malformed software.			03.16.01	A.03.16.01.ODP[01] A.03.16.01								Annual	E-TDA-04
	R3	R2 & R3	Technology Development & Acquisition	TDA-02.4	P-TDA-02.4	Pre-Established Secure Configurations	TDA-02.4	Mechanisms exist to ensure vendors / manufacturers: (1) Deliver the Technology Asset, Application and/or Service (TAAS) with a pre-established, secure configuration implemented; and (2) Use the pre-established, secure configuration as the default for any subsequent TAAS reinstallation or upgrade.			03.16.01	A.03.16.01								Annual	
	R3	R2 & R3	Technology Development & Acquisition	TDA-03	P-TDA-03	Commercial Off-The-Shelf (COTS) Security Solutions	TDA-03	Mechanisms exist to utilize only Commercial Off-the-Shelf (COTS) security products.			03.16.01	A.03.16.01								Annual	

Applies To NIST 800-171 R2 & CMMC L2	Applies To NIST 800-171 R3	Applies To Both 171 R2 & R3	NCP SCRP Policy	NCP SCRP Standard #	NCP CSQP Procedure #	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US DFARS Cybersecurity	US FAR 52.204-21	US FAR [illegible]	US FAR 52.204-27	US CMMC 2.0 Level 1	US CMMC 2.0 Level 1 AOs	US CMMC 2.0 Level 2	Conformity Validation Cadence	Evidence Request List (ERL) #
R2		R2 & R3	Technology Development & Acquisition	TDA-04	P-TDA-04	Documentation Requirements	TDA-04	Mechanisms exist to obtain, protect and distribute administrator documentation for Technology Assets, Applications and/or Services (TAAS) that describe: (1) Secure configuration, installation and operation of the TAAS; (2) Effective use and maintenance of security features/functions; and (3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	NFO - SA-5											Annual	E-CPL-06 E-TDA-06 E-TDA-10
R2		R2 & R3	Technology Development & Acquisition	TDA-04.1	P-TDA-04.1	Functional Properties	TDA-04.1	Mechanisms exist to require software developers to provide information describing the functional properties of the security, compliance and resilience controls to be utilized within Technology Assets, Applications and/or Services (TAAS) in sufficient detail to permit analysis and testing of the controls.	NFO - SA-4(1) NFO - SA-4(2)											Annual	E-CPL-06 E-TDA-06 E-TDA-10 E-TDA-15
	R3	R2 & R3	Technology Development & Acquisition	TDA-05	P-TDA-05	Developer Architecture & Design	TDA-05	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a design specification and security architecture that: (1) Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture; (2) Accurately and completely describes the required security functionality and the allocation of security, compliance and resilience controls among physical and logical components; and			03.16.01	A.03.16.01							Annual	E-TDA-04
R2	R3	R2 & R3	Technology Development & Acquisition	TDA-06	P-TDA-06	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	NFO - SA-1	3.13.2[b] 3.13.2[e]	03.16.01	A.03.16.01								Annual	E-TDA-08 E-TDA-11
R2		R2 & R3	Technology Development & Acquisition	TDA-08	P-TDA-08	Separation of Development, Testing and Operational Environments	TDA-08	Mechanisms exist to manage separate development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment and to ensure no impact to production Technology Assets, Applications and/or Services (TAAS).	3.4.5										CML2-.3.4.5	Annual	
R2	R3	R2 & R3	Technology Development & Acquisition	TDA-09	P-TDA-09	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and (3) Document the results	NFO - SA-11		03.12.01 03.12.03 03.14.01.a	A.03.12.01 A.03.12.03[01] A.03.14.01.a[01] A.03.14.01.a[02]							Annual	E-TDA-03 E-TDA-05
	R3	R2 & R3	Technology Development & Acquisition	TDA-09.1	P-TDA-09.1	Continuous Monitoring Plan	TDA-09.1	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a plan for the continuous monitoring of security, compliance and/or resilience control effectiveness.			03.12.03	A.03.12.03[01]							Annual	E-TDA-03
R2		R2 & R3	Technology Development & Acquisition	TDA-14	P-TDA-14	Developer Configuration Management	TDA-14	Mechanisms exist to require system developers and integrators to perform configuration management during system design, development, implementation and operation.	NFO - SA-10											Annual	E-TDA-01 E-TDA-02 E-TDA-04 E-TDA-08
	R3	R2 & R3	Technology Development & Acquisition	TDA-17	P-TDA-17	Unsupported Technology Assets, Applications and/or Services (TAAS)	TDA-17	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs.			03.16.02.a	A.03.16.02.a							Annual	E-AST-09
	R3	R2 & R3	Technology Development & Acquisition	TDA-17.1	P-TDA-17.1	Alternate Sources for Continued Support	TDA-17.1	Mechanisms exist to provide in-house support or contract external providers for support with unsupported Technology Assets, Applications and/or Services (TAAS).			03.16.02.b	A.03.16.02.b							Annual	
R2	R3	R2 & R3	Third-Party Management	TPM-01	P-TPM-01	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	3.1.1 NFO - SA-4		03.01.20.a 03.01.20.b 03.01.20.c.01 03.07.06.a 03.16.01 03.16.03.a	A.03.01.20.a A.03.01.20.b A.03.01.20.c.01 A.03.07.06.a A.03.16.01 A.03.16.03.a	252.204-7012(b)(2)(ii)(D)	52.204-21(b)(1)(i)			AC.L1-B.1.I		ACL2-.3.1.1	Annual	E-TPM-03 E-TPM-06
	R3	R2 & R3	Third-Party Management	TPM-01.1	P-TPM-01.1	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).			03.07.06.a 03.07.06.b	A.03.07.06.b							Annual	E-AST-06 E-DCH-06
	R3	R2 & R3	Third-Party Management	TPM-02	P-TPM-02	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.			03.11.01.a 03.17.03.a	A.03.11.01.a A.03.17.03.a[01]							Annual	E-TPM-02
	R3	R2 & R3	Third-Party Management	TPM-03	P-TPM-03	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.			03.11.01.a 03.17.01.a 03.17.03.a 03.17.03.b	A.03.11.01.a A.03.17.01.a[01] A.03.17.03.a[01] A.03.17.03.b							Annual	E-RSK-02
	R3	R2 & R3	Third-Party Management	TPM-03.1	P-TPM-03.1	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets, Applications and/or Services (TAAS).			03.17.01.a 03.17.02 03.17.03.a 03.17.03.b	A.03.17.01.a[01] A.03.17.02[01] A.03.17.02[02] A.03.17.02[03] A.03.17.02[04] A.03.17.02[05]							Annual	
	R3	R2 & R3	Third-Party Management	TPM-03.2	P-TPM-03.2	Limit Potential Harm	TPM-03.2	Mechanisms exist to utilize security safeguards to limit harm from potential adversaries who identify and target the organization's supply chain.			03.17.03.a 03.17.03.b	A.03.17.03.a[01] A.03.17.03.b							Annual	E-TPM-01 E-TPM-02 E-TPM-03 E-TPM-05
	R3	R2 & R3	Third-Party Management	TPM-03.3	P-TPM-03.3	Processes To Address Weaknesses or Deficiencies	TPM-03.3	Mechanisms exist to address identified weaknesses or deficiencies in the security of the supply chain			03.17.03.a 03.17.03.b	A.03.17.03.a[01] A.03.17.03.b							Annual	E-TPM-01 E-TPM-02 E-TPM-03 E-TPM-05
R2	R3	R2 & R3	Third-Party Management	TPM-04	P-TPM-04	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	NFO - SA-9		03.16.03.a 03.16.03.c 03.17.02 03.17.03.a 03.17.03.b	A.03.16.03.a A.03.16.03.c A.03.17.02[02] A.03.17.02[03] A.03.17.02[05] A.03.17.02[06]							Annual	E-CPL-06
	R3	R2 & R3	Third-Party Management	TPM-04.1	P-TPM-04.1	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).			03.11.01.a 03.17.02 03.17.03.a 03.17.03.b	A.03.11.01.a A.03.17.02[02] A.03.17.02[03] A.03.17.02[05] A.03.17.02[06] A.03.17.01.a[01]							Annual	E-TPM-01 E-TPM-02 E-TPM-03
R2		R2 & R3	Third-Party Management	TPM-04.2	P-TPM-04.2	External Connectivity Requirements - Identification of Ports, Protocols & Services	TPM-04.2	Mechanisms exist to require External Service Providers (ESPs) to identify and document the business need for ports, protocols and other services it requires to operate its Technology Assets, Applications and/or Services (TAAS).	NFO - SA-9(2)											Annual	E-CPL-06 E-TDA-07
	R3	R2 & R3	Third-Party Management	TPM-04.4	P-TPM-04.4	Third-Party Processing, Storage and Service Locations	TPM-04.4	Mechanisms exist to restrict the location of information processing/storage based on business requirements.			03.16.03.a	A.03.16.03.a							Annual	E-AST-23
R2	R3	R2 & R3	Third-Party Management	TPM-05	P-TPM-05	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	3.1.1 NFO - SA-4		03.01.20.b 03.01.20.c.01 03.01.20.c.02 03.07.06.a 03.16.03.a 03.16.03.b	A.03.01.20.b A.03.01.20.c.01 A.03.01.20.c.02 A.03.07.06.a A.03.16.03.ODP[01] A.03.16.03.a	252.204-7012(b) 252.204-7012(m)(1)	52.204-21(b)(1)(i)		52.204-27(c)	AC.L1-B.1.I		ACL2-.3.1.1	Annual	E-RSK-02 E-TPM-01 E-TPM-03 E-TPM-06 E-TPM-07

Applies To NIST 800-171 R2 & CMMC L2	Applies To NIST 800-171 R3	Applies To Both 171 R2 & R3	NCP SCRP Policy	NCP SCRP Standard #	NCP CSOP Procedure #	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US DFARS Cybersecurity	US FAR 52.204-21	US FAR 52.204-25	US FAR 52.204-27	US CMMC 2.0 Level 1	US CMMC 2.0 Level 1 AOs	US CMMC 2.0 Level 2	Conformity Validation Cadence	Evidence Request List (ERL) #
	R3	R2 & R3	Third-Party Management	TPM-05.1	P-TPM-05.1	Security Compromise Notification Agreements	TPM-05.1	Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected Technology Assets, Applications and/or Services (TAAS) that the organization utilizes.			03.17.02	A.03.17.02[05]									Annual	
R2	R3	R2 & R3	Third-Party Management	TPM-05.2	P-TPM-05.2	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	3.1.1		03.16.03.a 03.16.03.b 03.16.03.c 03.17.02 03.17.03.b	A.03.16.03.ODP[01] A.03.16.03.a A.03.16.03.b A.03.16.03.c A.03.17.02[05] A.03.17.03.b	252.204-7012(b) 252.204-7012(m)(2)(i)	52.204-21(b)(1)(i)		52.204-27(c)	AC.L1-B.1.I		AC.L2-.3.1.1	Annual	E-RSK-02
	R3	R2 & R3	Third-Party Management	TPM-05.4	P-TPM-05.4	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).			03.07.06.a 03.07.06.b 03.16.03.b	A.03.07.06.b A.03.16.03.b									Annual	E-CPL-03
	R3	R2 & R3	Third-Party Management	TPM-05.5	P-TPM-05.5	Third-Party Scope Review	TPM-05.5	Mechanisms exist to perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure security, compliance and resilience control assignments accurately reflect current: (1) Contractual obligations for the External Service Provider (ESP); (2) Business practices;			03.16.03.c 03.17.02 03.17.03.a 03.17.03.b	A.03.16.03.c A.03.17.02[05] A.03.17.02[06] A.03.17.03.a[02] A.03.17.03.b								Annual	E-TPM-03
	R3	R2 & R3	Third-Party Management	TPM-05.6	P-TPM-05.6	First-Party Declaration (1PD)	TPM-05.6	Mechanisms exist to obtain a First-Party Declaration(1PD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to subcontractors.			03.01.20.c.01 03.16.03.c	A.03.01.20.c.01 A.03.16.03.c									Semi-Annual	E-TPM-01
	R3	R2 & R3	Third-Party Management	TPM-05.7	P-TPM-05.7	Break Clauses	TPM-05.7	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for security, compliance and/or resilience controls.			03.17.01.a 03.17.02 03.17.03.b	A.03.17.01.a[01] A.03.17.02[05] A.03.17.02[06] A.03.17.03.b									Annual	E-TPM-05
	R3	R2 & R3	Third-Party Management	TPM-05.8	P-TPM-05.8	Third-Party Attestation (3PA)	TPM-05.8	Mechanisms exist to obtain an attestation from an independent Third-Party Assessment Organization (3PAO) that provides assurance of conformity with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to contractors and subcontractors.			03.01.20.a 03.01.20.b 03.01.20.c.01 03.16.03.a 03.16.03.c	A.03.01.20.a A.03.01.20.b A.03.01.20.c.01 A.03.16.03.a A.03.16.03.c									Semi-Annual	
	R3	R2 & R3	Third-Party Management	TPM-08	P-TPM-08	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.			03.16.03.c 03.17.02	A.03.16.03.c A.03.17.02[05] A.03.17.02[06]									Semi-Annual	E-TPM-03
	R3	R2 & R3	Third-Party Management	TPM-09	P-TPM-09	Third-Party Deficiency Remediation	TPM-09	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.			03.17.02	A.03.17.02[06]									Annual	E-TPM-03
	R3	R2 & R3	Third-Party Management	TPM-10	P-TPM-10	Managing Changes To Third-Party Services	TPM-10	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.			03.16.01 03.17.02	A.03.16.01 A.03.17.02[06]									Annual	E-TPM-01
R2	R3	R2 & R3	Threat Management	THR-01	P-THR-01	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	3.12.3 3.14.3		03.11.02.a 03.14.01.a 03.14.03.a	A.03.11.02.a[01] A.03.14.01.a[01] A.03.14.03.a							CAL2.-3.12.3 SIL2.-3.14.3	Annual	E-THR-04
R2	R3	R2 & R3	Threat Management	THR-03	P-THR-03	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	3.12.3 3.14.3		03.02.01.a.02 03.02.01.a.03 03.11.02.a 03.14.03.a	A.03.02.01.a.02 A.03.02.01.b[02] A.03.11.02.a[01] A.03.14.03.a							CAL2.-3.12.3 SIL2.-3.14.3	Annual	E-THR-03
	R3	R2 & R3	Threat Management	THR-03.1	P-THR-03.1	Threat Intelligence Reporting	THR-03.1	Mechanisms exist to utilize external threat intelligence feeds to generate and disseminate organization-specific security alerts, advisories and/or directives.			03.14.03.b	A.03.14.03.a A.03.14.03.b[01] A.03.14.03.b[02]									Annual	
R2	R3	R2 & R3	Threat Management	THR-05	P-THR-05	Insider Threat Awareness	THR-05	Mechanisms exist to utilize security awareness training on recognizing and reporting potential indicators of insider threat.	3.2.3	3.2.3[a] 3.2.3[b]	03.02.01.a.03	A.03.02.01.a.03[01] A.03.02.01.a.03[02]							AT.L2.-3.2.3	Annual	E-SAT-04 E-SAT-05 E-THR-04
	R3	R2 & R3	Threat Management	THR-06	P-THR-06	Vulnerability Disclosure Program (VDP)	THR-06	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of Technology Assets, Applications and/or Services (TAAS) that receives unsolicited input from the public about vulnerabilities in organizational TAAS.			03.14.01.a	A.03.14.01.a[01] A.03.14.01.a[02]									Annual	E-TDA-16
	R3	R2 & R3	Threat Management	THR-09	P-THR-09	Threat Catalog	THR-09	Mechanisms exist to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade.			03.15.02.a.03									Annual	E-THR-06
	R3	R2 & R3	Threat Management	THR-10	P-THR-10	Threat Analysis	THR-10	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.			03.14.03.b	A.03.14.03.a									Annual	E-THR-07
R2	R3	R2 & R3	Vulnerability & Patch Management	VPM-01	P-VPM-01	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	3.14.1	3.14.1[a] 3.14.1[b] 3.14.1[c] 3.14.1[d] 3.14.1[e] 3.14.1[f]	03.11.02.a 03.14.01.a	A.03.11.02.ODP[03] A.03.11.02.a[01] A.03.14.01.a[01]		52.204-21(b)(1)(xii)			SI.L1-B.1.XII	SI.L1-B.1.XII[a] SI.L1-B.1.XII[b] SI.L1-B.1.XII[c] SI.L1-B.1.XII[d] SI.L1-B.1.XII[e] SI.L1-B.1.XII[f]	SIL2.-3.14.1	Annual	E-MNT-03 E-THR-05 E-VPM-01
	R3	R2 & R3	Vulnerability & Patch Management	VPM-01.1	P-VPM-01.1	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.			03.11.02.a 03.14.01.a	A.03.11.02.a[01] A.03.14.01.a[01]								Annual	E-VPM-06
R2	R3	R2 & R3	Vulnerability & Patch Management	VPM-02	P-VPM-02	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	3.14.1	3.11.3[a] 3.11.3[b]	03.11.02.b 03.12.02.a.02 03.14.01.a	A.03.11.02.ODP[03] A.03.11.02.b A.03.12.02.a.02		52.204-21(b)(1)(xii)			SI.L1-B.1.XII		SIL2.-3.14.1	Annual	E-RSK-03 E-RSK-04 E-VPM-01 E-VPM-09
	R3	R2 & R3	Vulnerability & Patch Management	VPM-03	P-VPM-03	Vulnerability Ranking	VPM-03	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.			03.11.02.a	A.03.11.02.a[01]								Annual	E-RSK-03 E-RSK-04 E-VPM-01 E-VPM-10
R2	R3	R2 & R3	Vulnerability & Patch Management	VPM-04	P-VPM-04	Continuous Vulnerability Remediation Activities	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	3.11.3		03.11.02.b 03.14.01.a	A.03.11.02.b A.03.14.01.a[03]							RAL2.-3.11.3	Annual	E-MNT-03 E-THR-05

Applies To NIST 800-171 R2 & CMMC L2	Applies To NIST 800-171 R3	Applies To Both 171 R2 & R3	NCP SCRP Policy	NCP SCRP Standard #	NCP CSOP Procedure #	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US DFARS Cybersecurity	US FAR 52.204-21	US FAR 52.204-25	US FAR 52.204-27	US CMMC 2.0 Level 1	US CMMC 2.0 Level 1 AOs	US CMMC 2.0 Level 2	Conformity Validation Cadence	Evidence Request List (ERL) #
R2	R3	R2 & R3	Vulnerability & Patch Management	VPM-05	P-VPM-05	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	3.11.3 3.14.1		03.11.02.b 03.12.02.a.02 03.14.01.a 03.14.01.b	A.03.11.02.b A.03.12.02.a.02 A.03.14.01.ODP[01] A.03.14.01.ODP[02] A.03.14.01.a[03] A.03.14.01.b[01]		52.204-21(b)(1)(xii)			SI.L1-B.1.XII		RAL2.-3.11.3 SIL2.-3.14.1	Quarterly	E-MNT-03 E-VPM-10
R2	R3	R2 & R3	Vulnerability & Patch Management	VPM-06	P-VPM-06	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	3.11.2	3.11.2[a] 3.11.2[b] 3.11.2[c] 3.11.2[d] 3.11.2[e]	03.11.02.a 03.14.01.a	A.03.11.02.ODP[01] A.03.11.02.ODP[02] A.03.11.02.ODP[04] A.03.11.02.a[01] A.03.11.02.a[02] A.03.11.02.a[03]							RAL2.-3.11.2	Semi-Annual	E-VPM-05 E-VPM-11
R2	R3	R2 & R3	Vulnerability & Patch Management	VPM-06.1	P-VPM-06.1	Update Tool Capability	VPM-06.1	Mechanisms exist to update vulnerability scanning tools.	NFO - RA-5(1) NFO - RA-5(2)		03.11.02.c	A.03.11.02.ODP[04] A.03.11.02.c[01] A.03.11.02.c[02]								Annual	
R2		R2 & R3	Vulnerability & Patch Management	VPM-06.3	P-VPM-06.3	Privileged Access	VPM-06.3	Mechanisms exist to implement privileged access authorization for selected vulnerability scanning activities.	3.11.2										RAL2.-3.11.2	Semi-Annual	
R2	R3	R2 & R3	Web Security	WEB-01	P-WEB-01	Web Security	WEB-01	Mechanisms exist to facilitate the implementation of an enterprise-wide web management policy, as well as associated standards, controls and procedures.	3.1.22		03.01.22.a	A.03.01.22.a		52.204-21(b)(1)(iv)			AC.L1-B.1.IV		ACL2.-3.1.22	Annual	
R2	R3	R2 & R3	Web Security	WEB-02	P-WEB-02	Use of Demilitarized Zones (DMZ)	WEB-02	Mechanisms exist to utilize a Demilitarized Zone (DMZ) to restrict inbound traffic to authorized Technology Assets, Applications and/or Services (TAAS) on certain services, protocols and ports.	3.1.22	3.1.22[a] 3.1.22[b] 3.1.22[c] 3.1.22[d] 3.1.22[e]				52.204-21(b)(1)(iv)			AC.L1-B.1.IV		ACL2.-3.1.22	Annual	
R2	R3	R2 & R3	Web Security	WEB-04	P-WEB-04	Client-Facing Web Services	WEB-04	Mechanisms exist to deploy reasonably-expected security, compliance and resilience controls to protect the confidentiality and availability of client data that is stored, transmitted or processed by the Internet-based service.	3.1.22	3.1.22[a] 3.1.22[b] 3.1.22[c] 3.1.22[d] 3.1.22[e]				52.204-21(b)(1)(iv)			AC.L1-B.1.IV		ACL2.-3.1.22	Annual	
	R3	R2 & R3	Web Security	WEB-14	P-WEB-14	Publicly Accessible Content Reviews	WEB-14	Mechanisms exist to routinely review the content on publicly accessible systems for sensitive and/or regulated data and remove such information, if discovered.			03.01.22.b	A.03.01.22.b[02]								Annual	E-DCH-12