This table represents the crosswalk mappings in ComplianceForge's NIST 800-171 Compliance Program (NCP), which contains the policies, standards and procedures to demonstrate compliance with both NIST 800-171 R2 and R3. The NCP contains coverage for both NIST 800-171 controls and NIST 800-171A Assessment Objectives (AOs), in addition to CMMC L1/L2 requirements.

The NCP enables an organization to demonstrate immediate compliance with NIST 800-171 R2 as they work towards implementing NIST 800-171 R3 requirements. The NCP includes one (1) year of updates.

#	NCP Policy Title	NCP Standard Title	NCP Standard #	NCP Procedure #	NIST 800-171 R2 Only	NIST 800-171 R3 Only	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US CMMC 2.0 Level 1	US CMMC 2.0 Level 2
1	Cybersecurity & Data Protection Governance	Cybersecurity & Data Protection Governance Program	GOV-01	P-GOV-01		x			03.15.01.a			
2	Cybersecurity & Data Protection Governance	Steering Committee & Program Oversight	GOV-01.1	P-GOV-01.1		x			03.12.03			
3	Cybersecurity & Data Protection Governance	Status Reporting To Governing Body	GOV-01.2	P-GOV-01.2		x			03.12.03			
4	Cybersecurity & Data Protection Governance	Publishing Cybersecurity & Data Protection Documentation	GOV-02	P-GOV-02	x	x		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]		
5	Cybersecurity & Data Protection Governance	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	P-GOV-03		x			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]		
6	Cybersecurity & Data Protection Governance	Measures of Performance	GOV-05	P-GOV-05		x			03.12.03			
7	Cybersecurity & Data Protection Governance	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	P-GOV-15		x			03.15.01.a 03.17.01.a	A.03.16.01		
8	Cybersecurity & Data Protection Governance	Select Controls	GOV-15.1	P-GOV-15.1		x			03.15.01.a 03.17.01.a			
9	Cybersecurity & Data Protection Governance	Implement Controls	GOV-15.2	P-GOV-15.2		x			03.15.01.a 03.17.01.a			
10	Cybersecurity & Data Protection Governance	Assess Controls	GOV-15.3	P-GOV-15.3		x			03.15.01.a 03.17.01.a			
11	Cybersecurity & Data Protection Governance	Authorize Systems, Applications & Services	GOV-15.4	P-GOV-15.4		x			03.15.01.a 03.17.01.a			
12	Cybersecurity & Data Protection Governance	Monitor Controls	GOV-15.5	P-GOV-15.5		x			03.15.01.a 03.17.01.a			
13	Asset Management	Asset Governance	AST-01	P-AST-01	x	x	3.4.1		03.01.03 03.01.18.a 03.04.11.a 03.07.04.a			CM.L2-3.4.1
14	Asset Management	Asset-Service Dependencies	AST-01.1	P-AST-01.1		x			03.01.03			
15	Asset Management	Approved Technologies	AST-01.4	P-AST-01.4		x				A.03.04.08.c		
16	Asset Management	Asset Inventories	AST-02	P-AST-02	x	x	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.03.04.10.ODP[01] A.03.04.10.a A.03.04.10.b[01] A.03.04.10.b[02]		CM.L2-3.4.1
17	Asset Management	Updates During Installations / Removals	AST-02.1	P-AST-02.1	x	x		3.4.1[f]	03.04.10.a 03.04.10.b 03.04.10.c	A.03.04.10.c[01] A.03.04.10.c[02] A.03.04.10.c[03]		
18	Asset Management	Component Duplication Avoidance	AST-02.3	P-AST-02.3	x		NFO - CM-8(5)					
19	Asset Management	Approved Baseline Deviations	AST-02.4	P-AST-02.4		x			03.04.02.b 03.04.06.a			
20	Asset Management	Data Action Mapping	AST-02.8	P-AST-02.8		x			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]		
21	Asset Management	Configuration Management Database (CMDB)	AST-02.9	P-AST-02.9		x			03.04.08.a 03.04.10.a 03.04.10.b 03.04.10.c			
22	Asset Management	Asset Ownership Assignment	AST-03	P-AST-03		x			03.09.02.a.03			
23	Asset Management	Accountability Information	AST-03.1	P-AST-03.1		x			03.09.02.a.03			
24	Asset Management	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	P-AST-04		x			03.01.03 03.04.11.a 03.04.11.b			
25	Asset Management	Asset Scope Classification	AST-04.1	P-AST-04.1		x			03.04.11.a 03.04.11.b			
26	Asset Management	Control Applicability Boundary Graphical Representation	AST-04.2	P-AST-04.2		x			03.04.11.a 03.04.11.b 03.15.02.a.04			
27	Asset Management	Compliance-Specific Asset Identification	AST-04.3	P-AST-04.3		x			03.01.03			
28	Asset Management	Security of Assets & Media	AST-05	P-AST-05	x	x	NFO - MP-1		03.07.04.a			
29	Asset Management	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	P-AST-09		x			03.07.04.c 03.08.03			
30	Asset Management	Return of Assets	AST-10	P-AST-10		x			03.09.02.a.03	A.03.09.02.a.03		
31	Asset Management	Use of Personal Devices	AST-12	P-AST-12		x			03.01.18.a			
32	Asset Management	Use of Third-Party Devices	AST-13	P-AST-13		x			03.01.18.a			
33	Asset Management	Usage Parameters	AST-14	P-AST-14		x			03.01.18.a			
34	Asset Management	Bring Your Own Device (BYOD) Usage	AST-16	P-AST-16		x			03.01.18.a			
35	Asset Management	Prohibited Equipment & Services	AST-17	P-AST-17		x			03.11.01.a 03.16.01			
36	Asset Management	Travel-Only Devices	AST-24	P-AST-24		x			03.04.12.a 03.04.12.b	A.03.04.12.a		
37	Asset Management	Re-Imaging Devices After Travel	AST-25	P-AST-25		x			03.04.12.b	A.03.04.12.b		
38	Asset Management	Jump Server	AST-27	P-AST-27		x			03.01.12.a 03.01.12.c			
39	Asset Management	Asset Categorization	AST-31	P-AST-31		x			03.01.03			
40	Business Continuity & Disaster Recovery	Data Backups	BCD-11	P-BCD-11	x	x	3.8.9	3.8.9	03.08.09.a			MP.L2-3.8.9
41	Business Continuity & Disaster Recovery	Cryptographic Protection	BCD-11.4	P-BCD-11.4	x	x	3.8.9	3.8.9	03.08.09.a 03.08.09.b	A.03.08.09.a A.03.08.09.b		MP.L2-3.8.9

#	NCP Policy Title	NCP Standard Title	NCP Standard #	NCP Procedure #	NIST 800-171 R2 Only	NIST 800-171 R3 Only	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US CMMC 2.0 Level 1	US CMMC 2.0 Level 2
42	Change Management	Change Management Program	CHG-01	P-CHG-01	x	x	3.4.3		03.04.02.b 03.04.03.a	A.03.04.03.d[01] A.03.04.03.d[02]		CM.L2-3.4.3
43	Change Management	Configuration Change Control	CHG-02	P-CHG-02	x	x	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	A.03.04.03.a A.03.04.03.c[01]		CM.L2-3.4.3
44	Change Management	Prohibition Of Changes	CHG-02.1	P-CHG-02.1		x			03.04.02.b 03.04.03.a	A.03.04.03.b[02] A.03.04.05[05]		
45	Change Management	Test, Validate & Document Changes	CHG-02.2	P-CHG-02.2	x	x	NFO - CM-3(2)		03.04.03.b 03.04.03.c 03.04.04.a 03.04.11.b	A.03.04.03.c[02]		
46	Change Management	Cybersecurity & Data Privacy Representative for Asset Lifecycle Changes	CHG-02.3	P-CHG-02.3		x			03.04.04.a			
47	Change Management	Security Impact Analysis for Changes	CHG-03	P-CHG-03	x	x	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		CM.L2-3.4.4
48	Change Management	Access Restriction For Change	CHG-04	P-CHG-04	x	x	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] 3.4.5[g] 3.4.5[h]	03.04.02.b 03.04.05			CM.L2-3.4.5
49	Change Management	Permissions To Implement Changes	CHG-04.4	P-CHG-04.4		x			03.04.05	A.03.04.05[06]		
50	Change Management	Stakeholder Notification of Changes	CHG-05	P-CHG-05	x	x	NFO - CM-9		03.04.11.b	A.03.04.11.b[01] A.03.04.11.b[02]		
51	Change Management	Control Functionality Verification	CHG-06	P-CHG-06		x			03.04.04.b	A.03.04.04.b		
52	Cloud Security	Cloud Services	CLD-01	P-CLD-01	x		NFO – PL-8					
53	Cloud Security	Cloud Security Architecture	CLD-02	P-CLD-02	x		NFO – PL-8					
54	Cloud Security	Cloud Infrastructure Security Subnet	CLD-03	P-CLD-03	x		3.13.2 NFO – PL-8					SC.L2-3.13.2
55	Compliance	Statutory, Regulatory & Contractual Compliance	CPL-01	P-CPL-01	x	x	NFO - PL-1		03.04.11.a 03.12.01			
56	Compliance	Non-Compliance Oversight	CPL-01.1	P-CPL-01.1		x			03.12.02.a.01			
57	Compliance	Compliance Scope	CPL-01.2	P-CPL-01.2		x			03.04.11.a 03.15.02.a.04			
58	Compliance	Cybersecurity & Data Protection Controls Oversight	CPL-02	P-CPL-02	x	x	3.12.1 3.12.3	3.12.1[a] 3.12.1[b] 3.12.3	03.12.01 03.12.03	A.03.12.03[01] A.03.12.03[03] A.03.12.03[04]		CA.L2-3.12.1 CA.L2-3.12.3
59	Compliance	Internal Audit Function	CPL-02.1	P-CPL-02.1	x	x	3.12.1		03.12.01	A.03.12.01.ODP[01]		CA.L2-3.12.1
60	Compliance	Cybersecurity & Data Protection Assessments	CPL-03	P-CPL-03	x	x	3.12.1		03.12.01 03.12.03	A.03.12.01		CA.L2-3.12.1
61	Compliance	Independent Assessors	CPL-03.1	P-CPL-03.1	x		NFO - CA-7(1)					
62	Compliance	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	P-CPL-03.2		x			03.04.08.c 03.12.03	A.03.12.03[02]		
63	Configuration Management	Configuration Management Program	CFG-01	P-CFG-01	x	x	NFO - CM-1 NFO - CM-9		03.04.01.a	A.03.04.03.a		
64	Configuration Management	System Hardening Through Baseline Configurations	CFG-02	P-CFG-02	x	x	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 03.01.08.a 03.01.08.b 03.01.09 03.01.10.a 03.01.10.b 03.01.10.c 03.01.11 03.01.12.a 03.01.16.a 03.01.18.a 03.04.01.a 03.04.02.a 03.04.06.a 03.04.06.b 03.04.06.d 03.05.07.d 03.05.07.e 03.05.07.f 03.05.12.d 03.08.07.a 03.13.12.b	A.03.01.03[01] A.03.01.16.a[03] A.03.01.16.c A.03.01.18.a[02] A.03.03.08.a[02] A.03.04.01.a[01] A.03.04.01.a[02] A.03.04.02.a[01] A.03.04.02.a[02] A.03.04.06.ODP[01] A.03.04.06.ODP[02] A.03.04.06.ODP[03] A.03.04.06.ODP[04] A.03.04.06.ODP[05] A.03.04.06.b[01] A.03.04.06.b[02] A.03.04.06.b[03] A.03.04.06.b[04] A.03.04.06.b[05] A.03.05.04[01] A.03.05.04[02] A.03.05.07.c A.03.05.07.d A.03.05.07.e A.03.05.07.f A.03.07.05.b[02]		CM.L2-3.4.1 CM.L2-3.4.2
65	Configuration Management	Reviews & Updates	CFG-02.1	P-CFG-02.1	x	x	NFO - CM-2(1)		03.04.01.b 03.04.02.b	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		
66	Configuration Management	Automated Central Management & Verification	CFG-02.2	P-CFG-02.2		x			03.04.02.b 03.04.03.d	A.03.04.03.d[01] A.03.04.03.d[02]		
67	Configuration Management	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	P-CFG-02.5	x	x	NFO - CM-2(7)		03.04.01.a 03.04.02.a 03.04.06.a 03.04.06.b 03.04.06.d 03.04.12.a	A.03.04.12.ODP[01] A.03.04.12.ODP[02]		
68	Configuration Management	Approved Configuration Deviations	CFG-02.7	P-CFG-02.7		x			03.04.01.a 03.04.02.b	A.03.04.02.b[01] A.03.04.02.b[02]		
69	Configuration Management	Baseline Tailoring	CFG-02.9	P-CFG-02.9		x			03.03.02.b 03.04.01.a 03.04.02.a 03.04.02.b 03.04.06.a 03.04.08.a 03.04.12.a 03.13.11	A.03.03.02.b		
70	Configuration Management	Least Functionality	CFG-03	P-CFG-03	x	x	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.03.04.06.d		CM.L2-3.4.6

#	NCP Policy Title	NCP Standard Title	NCP Standard #	NCP Procedure #	NIST 800-171 R2 Only	NIST 800-171 R3 Only	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US CMMC 2.0 Level 1	US CMMC 2.0 Level 2
71	Configuration Management	Periodic Review	CFG-03.1	P-CFG-03.1	x	x	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] 3.4.7[g] 3.4.7[h] 3.4.7[i] 3.4.7[j] 3.4.7[k] 3.4.7[l] 3.4.7[m] 3.4.7[n] 3.4.7[o]	03.04.06.c 03.04.08.c	A.03.04.06.ODP[06]		CM.L2-3.4.7
72	Configuration Management	Prevent Unauthorized Software Execution	CFG-03.2	P-CFG-03.2	x	x	3.4.7		03.04.08.b			CM.L2-3.4.7
73	Configuration Management	Explicitly Allow / Deny Applications	CFG-03.3	P-CFG-03.3	x	x	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.b[03]		CM.L2-3.4.8
74	Configuration Management	Split Tunneling	CFG-03.4	P-CFG-03.4	x		3.13.7	3.13.7				SC.L2-3.13.7
75	Configuration Management	Software Usage Restrictions	CFG-04	P-CFG-04		x			03.13.13.b			
76	Configuration Management	Open Source Software	CFG-04.1	P-CFG-04.1		x			03.13.13.b			
77	Configuration Management	User-Installed Software	CFG-05	P-CFG-05	x	x	3.4.9	3.4.9[b] 3.4.9[c]	03.13.13.b			CM.L2-3.4.9
78	Configuration Management	Configuration Enforcement	CFG-06	P-CFG-06		x			03.04.02.a 03.04.02.b 03.04.03.a			
79	Configuration Management	Sensitive / Regulated Data Access Enforcement	CFG-08	P-CFG-08		x			03.01.02	A.03.01.02[01]		
80	Continuous Monitoring	Continuous Monitoring	MON-01	P-MON-01	x	x	NFO - AU-1		03.03.01.a 03.12.03 03.14.06.a	A.03.14.06.a.01[01] A.03.14.06.a.01[02] A.03.14.06.a.02		
81	Continuous Monitoring	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	P-MON-01.1		x			03.13.01.a			
82	Continuous Monitoring	Inbound & Outbound Communications Traffic	MON-01.3	P-MON-01.3	x	x	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.c[01] A.03.14.06.c[02]		SI.L2-3.14.6
83	Continuous Monitoring	System Generated Alerts	MON-01.4	P-MON-01.4	x	x	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.03.03.02.a.01 A.03.03.03.a		
84	Continuous Monitoring	Reviews & Updates	MON-01.8	P-MON-01.8	x	x	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]	03.03.01.b 03.03.05.a	A.03.03.01.ODP[02] A.03.03.01.b[01] A.03.03.05.ODP[01] A.03.03.05.a		AU.L2-3.3.3 SI.L2-3.14.3
85	Continuous Monitoring	Automated Alerts	MON-01.12	P-MON-01.12		x			03.03.04.a 03.03.05.b	A.03.03.05.b		
86	Continuous Monitoring	Privileged User Oversight	MON-01.15	P-MON-01.15		x			03.01.07.b			
87	Continuous Monitoring	Centralized Collection of Security Event Logs	MON-02	P-MON-02	x	x	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]		AU.L2-3.3.1 AU.L2-3.3.3 AU.L2-3.3.5 AU.L2-3.3.6 AU.L2-3.3.8 AU.L2-3.3.9
88	Continuous Monitoring	Correlate Monitoring Information	MON-02.1	P-MON-02.1	x	x	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.c[02]		AU.L2-3.3.5 SI.L2-3.14.7
89	Continuous Monitoring	Central Review & Analysis	MON-02.2	P-MON-02.2		x			03.03.01.b 03.03.05.a 03.03.05.c			
90	Continuous Monitoring	Integration of Scanning & Other Monitoring Information	MON-02.3	P-MON-02.3		x			03.03.05.c			
91	Continuous Monitoring	System-Wide / Time-Correlated Audit Trail	MON-02.7	P-MON-02.7		x			03.03.01.a			
92	Continuous Monitoring	Content of Event Logs	MON-03	P-MON-03	x	x	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 03.03.02.a.05 03.03.02.a.06 03.03.02.b	A.03.03.01.ODP[01] A.03.03.01.a A.03.03.01.b[02] A.03.03.02.a.02 A.03.03.02.a.03 A.03.03.02.a.04 A.03.03.02.a.05 A.03.03.02.a.06 A.03.03.02.b		AU.L2-3.3.2
93	Continuous Monitoring	Sensitive Audit Information	MON-03.1	P-MON-03.1	x		3.3.8					AU.L2-3.3.8
94	Continuous Monitoring	Audit Trails	MON-03.2	P-MON-03.2	x	x		3.3.2[a] 3.3.1[c]	03.03.01.a			
95	Continuous Monitoring	Privileged Functions Logging	MON-03.3	P-MON-03.3		x			03.01.07.b	A.03.01.07.b		
96	Continuous Monitoring	Database Logging	MON-03.7	P-MON-03.7	x			3.3.2[a]				
97	Continuous Monitoring	Response To Event Log Processing Failures	MON-05	P-MON-05	x	x	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		AU.L2-3.3.4
98	Continuous Monitoring	Monitoring Reporting	MON-06	P-MON-06	x	x	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]		AU.L2-3.3.6
99	Continuous Monitoring	Time Stamps	MON-07	P-MON-07	x	x		3.3.7[a] 3.3.7[b]	03.03.02.a.02 03.03.07.a	A.03.03.07.ODP[01] A.03.03.07.a A.03.03.07.b[01]		
100	Continuous Monitoring	Synchronization With Authoritative Time Source	MON-07.1	P-MON-07.1	x	x	3.3.7	3.3.7[b] 3.3.7[c]	03.03.07.b	A.03.03.07.b[02]		AU.L2-3.3.7

#	NCP Policy Title	NCP Standard Title	NCP Standard #	NCP Procedure #	NIST 800-171 R2 Only	NIST 800-171 R3 Only	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US CMMC 2.0 Level 1	US CMMC 2.0 Level 2
101	Continuous Monitoring	Protection of Event Logs	MON-08	P-MON-08	x	x	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	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		AU.L2-3.3.8
102	Continuous Monitoring	Event Log Backup on Separate Physical Systems / Components	MON-08.1	P-MON-08.1		x			03.03.08.a			
103	Continuous Monitoring	Access by Subset of Privileged Users	MON-08.2	P-MON-08.2	x	x	3.3.9	3.3.9[a] 3.3.9[b]	03.03.08.a 03.03.08.b	A.03.03.08.b		AU.L2-3.3.9
104	Continuous Monitoring	Cryptographic Protection of Event Log Information	MON-08.3	P-MON-08.3		x			03.03.08.a			
105	Continuous Monitoring	Event Log Retention	MON-10	P-MON-10	x	x	3.3.1	3.3.1[e] 3.3.1[f]	03.03.03.b	A.03.03.03.b		AU.L2-3.3.1
106	Continuous Monitoring	Monitoring For Information Disclosure	MON-11	P-MON-11		x			03.01.22.b			
107	Continuous Monitoring	Monitoring for Indicators of Compromise (IOC)	MON-11.3	P-MON-11.3		x			03.14.06.a.01 03.14.06.a.02 03.14.06.b 03.14.06.c			
108	Continuous Monitoring	Anomalous Behavior	MON-16	P-MON-16		x			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.03.14.06.b		
109	Cryptographic Protections	Use of Cryptographic Controls	CRY-01	P-CRY-01	x	x	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 A.03.13.11.ODP[01]		SC.L2-3.13.11
110	Cryptographic Protections	Alternate Physical Protection	CRY-01.1	P-CRY-01.1	x	x	3.13.8	3.13.8[b] 3.13.8[c]	03.13.08			SC.L2-3.13.8
111	Cryptographic Protections	Cryptographic Cipher Suites and Protocols Inventory	CRY-01.5	P-CRY-01.5		x			03.13.11			
112	Cryptographic Protections	Transmission Confidentiality	CRY-03	P-CRY-03	x	x	3.13.8	3.13.8[a] 3.13.11	03.13.08	A.03.13.08[01] A.03.13.11 A.03.13.11.ODP[01]		SC.L2-3.13.8
113	Cryptographic Protections	Transmission Integrity	CRY-04	P-CRY-04	x		NFO - SI-1					
114	Cryptographic Protections	Encrypting Data At Rest	CRY-05	P-CRY-05	x	x	3.8.6	3.8.6	03.13.08	A.03.13.08[02] A.03.13.11 A.03.13.11.ODP[01]		MP.L2-3.8.6
115	Cryptographic Protections	Storage Media	CRY-05.1	P-CRY-05.1		x			03.13.08			
116	Cryptographic Protections	Wireless Access Authentication & Encryption	CRY-07	P-CRY-07		x			03.01.16.a			
117	Cryptographic Protections	Public Key Infrastructure (PKI)	CRY-08	P-CRY-08	x	x	3.13.10	3.13.10[a] 3.13.10[b]	03.13.10			SC.L2-3.13.10
118	Cryptographic Protections	Cryptographic Key Management	CRY-09	P-CRY-09	x	x	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]		SC.L2-3.13.10
119	Cryptographic Protections	Cryptographic Key Loss or Change	CRY-09.3	P-CRY-09.3		x			03.13.10			
120	Cryptographic Protections	Control & Distribution of Cryptographic Keys	CRY-09.4	P-CRY-09.4		x			03.13.10			
121	Data Classification & Handling	Data Protection	DCH-01	P-DCH-01	x	x	3.8.1 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			MP.L2-3.8.1
122	Data Classification & Handling	Data Stewardship	DCH-01.1	P-DCH-01.1		x			03.08.01 03.08.05.a			
123	Data Classification & Handling	Sensitive / Regulated Data Protection	DCH-01.2	P-DCH-01.2		x			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 03.01.20.d 03.06.05.d 03.08.01 03.08.02 03.08.05.a 03.17.01.c			
124	Data Classification & Handling	Sensitive / Regulated Media Records	DCH-01.3	P-DCH-01.3		x			03.08.05.c			
125	Data Classification & Handling	Defining Access Authorizations for Sensitive/Regulated Data	DCH-01.4	P-DCH-01.4		x			03.01.02 03.01.03 03.01.04.b 03.08.01 03.08.02 03.10.01.a 03.15.02.c 03.17.01.c	A.03.15.02.c A.03.17.01.c		
126	Data Classification & Handling	Data & Asset Classification	DCH-02	P-DCH-02		x			03.04.11.a 03.08.01 03.08.04			
127	Data Classification & Handling	Media Access	DCH-03	P-DCH-03	x	x	3.1.3 3.8.2	3.1.3[c] 3.8.2	03.01.03 03.08.01 03.08.02	A.03.08.02		AC.L2-3.1.3 MP.L2-3.8.2
128	Data Classification & Handling	Disclosure of Information	DCH-03.1	P-DCH-03.1		x			03.01.22.a 03.15.02.c 03.17.01.c	A.03.15.02.c A.03.17.01.c		
129	Data Classification & Handling	Media Marking	DCH-04	P-DCH-04	x	x	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]		MP.L2-3.8.4
130	Data Classification & Handling	Media Storage	DCH-06	P-DCH-06	x	x	3.8.1		03.08.01	A.03.08.01[01] A.03.08.01[02]		MP.L2-3.8.1
131	Data Classification & Handling	Physically Secure All Media	DCH-06.1	P-DCH-06.1		x			03.08.01			
132	Data Classification & Handling	Sensitive Data Inventories	DCH-06.2	P-DCH-06.2		x			03.04.11.a 03.04.11.b			
133	Data Classification & Handling	Making Sensitive Data Unreadable In Storage	DCH-06.4	P-DCH-06.4		x			03.08.01			
134	Data Classification & Handling	Media Transportation	DCH-07	P-DCH-07	x	x	3.8.5	3.8.5[a] 3.8.5[b]	03.08.05.a 03.08.05.b	A.03.08.05.a[01] A.03.08.05.a[02] A.03.08.05.b A.03.08.05.c		MP.L2-3.8.5

#	NCP Policy Title	NCP Standard Title	NCP Standard #	NCP Procedure #	NIST 800-171 R2 Only	NIST 800-171 R3 Only	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US CMMC 2.0 Level 1	US CMMC 2.0 Level 2
135	Data Classification & Handling	Custodians	DCH-07.1	P-DCH-07.1		x			03.08.05.a 03.08.05.b			
136	Data Classification & Handling	Encrypting Data In Storage Media	DCH-07.2	P-DCH-07.2		x			03.08.05.a			
137	Data Classification & Handling	Physical Media Disposal	DCH-08	P-DCH-08		x			03.08.03			
138	Data Classification & Handling	System Media Sanitization	DCH-09	P-DCH-09	x	x	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.03.08.03	MP.L1-3.8.3	MA.L2-3.7.3 MP.L1-3.8.3
139	Data Classification & Handling	Media Use	DCH-10	P-DCH-10	x	x	3.8.7	3.8.7	03.08.07.a	A.03.08.07.ODP[01] A.03.08.07.a		MP.L2-3.8.7
140	Data Classification & Handling	Prohibit Use Without Owner	DCH-10.2	P-DCH-10.2	x	x	3.8.8	3.8.8	03.08.07.b	A.03.08.07.b		MP.L2-3.8.8
141	Data Classification & Handling	Removable Media Security	DCH-12	P-DCH-12		x			03.08.07.a			
142	Data Classification & Handling	Use of External Information Systems	DCH-13	P-DCH-13	x	x	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	AC.L1-3.1.20	AC.L1-3.1.20
143	Data Classification & Handling	Limits of Authorized Use	DCH-13.1	P-DCH-13.1	x	x	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		AC.L1-3.1.20	AC.L1-3.1.20
144	Data Classification & Handling	Portable Storage Devices	DCH-13.2	P-DCH-13.2	x	x	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.d		AC.L2-3.1.21
145	Data Classification & Handling	Protecting Sensitive Data on External Systems	DCH-13.3	P-DCH-13.3		x			03.01.20.b 03.01.20.c.01			
146	Data Classification & Handling	Non-Organizationally Owned Systems / Components / Devices	DCH-13.4	P-DCH-13.4		x			03.01.20.a 03.01.20.c.01 03.01.20.d			
147	Data Classification & Handling	Transfer Authorizations	DCH-14.2	P-DCH-14.2		x			03.01.20.b 03.01.20.c.02 03.12.05.a			
148	Data Classification & Handling	Data Access Mapping	DCH-14.3	P-DCH-14.3		x			03.01.03 03.01.20.c.02 03.12.05.a			
149	Data Classification & Handling	Publicly Accessible Content	DCH-15	P-DCH-15	x	x	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] A.03.01.22.b[02]	AC.L1-3.1.22	AC.L1-3.1.22
150	Data Classification & Handling	Ad-Hoc Transfers	DCH-17	P-DCH-17		x			03.01.20.a			
151	Data Classification & Handling	Media & Data Retention	DCH-18	P-DCH-18		x			03.01.20.c.02 03.14.08	A.03.14.08[01] A.03.14.08[02] A.03.14.08[03] A.03.14.08[04]		
152	Data Classification & Handling	Geographic Location of Data	DCH-19	P-DCH-19		x			03.04.11.a 03.04.11.b			
153	Data Classification & Handling	Information Disposal	DCH-21	P-DCH-21		x			03.08.03			
154	Data Classification & Handling	Information Location	DCH-24	P-DCH-24		x				A.03.04.11.a[01]		
155	Endpoint Security	Endpoint Security	END-01	P-END-01	x	x		3.4.1[a] 3.4.1[b] 3.4.1[c] 3.4.2[a] 3.4.2[b]	03.14.02.a	A.03.01.03[01]		
156	Endpoint Security	Endpoint Protection Measures	END-02	P-END-02	x		3.13.16	3.13.16				SC.L2-3.13.16
157	Endpoint Security	Prohibit Installation Without Privileged Status	END-03	P-END-03	x		3.4.9					CM.L2-3.4.9
158	Endpoint Security	Governing Access Restriction for Change	END-03.2	P-END-03.2	x			3.4.5[a] 3.4.5[b] 3.4.5[c] 3.4.5[d] 3.4.5[e] 3.4.5[f] 3.4.5[g] 3.4.5[h]				
159	Endpoint Security	Malicious Code Protection (Anti-Malware)	END-04	P-END-04	x	x	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.02	SI.L1-3.14.2	SI.L1-3.14.2
160	Endpoint Security	Automatic Antimalware Signature Updates	END-04.1	P-END-04.1	x	x	3.14.4	3.14.4	03.14.02.b	A.03.14.02.b	SI.L1-3.14.4	SI.L1-3.14.4
161	Endpoint Security	Centralized Management of Antimalware Technologies	END-04.3	P-END-04.3		x			03.14.02.a			
162	Endpoint Security	Always On Protection	END-04.7	P-END-04.7	x	x	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.c.01[01] A.03.14.02.c.01[02]	SI.L1-3.14.5	SI.L1-3.14.5
163	Endpoint Security	Host Intrusion Detection and Prevention Systems (HIDS / HIPS)	END-07	P-END-07		x			03.14.06.a.01 03.14.06.a.02 03.14.06.b 03.14.06.c			
164	Endpoint Security	Mobile Code	END-10	P-END-10	x	x	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[02] A.03.13.13.b[03]		SC.L2-3.13.13
165	Endpoint Security	Collaborative Computing Devices	END-14	P-END-14	x	x	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		SC.L2-3.13.12
166	Endpoint Security	Explicit Indication Of Use	END-14.6	P-END-14.6		x			03.13.12.b	A.03.13.12.b		
167	Human Resources Security	Human Resources Security Management	HRS-01	P-HRS-01	x	x	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]		
168	Human Resources Security	Position Categorization	HRS-02	P-HRS-02		x			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 03.09.01.b			

#	NCP Policy Title	NCP Standard Title	NCP Standard #	NCP Procedure #	NIST 800-171 R2 Only	NIST 800-171 R3 Only	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US CMMC 2.0 Level 1	US CMMC 2.0 Level 2
169	Human Resources Security	Users With Elevated Privileges	HRS-02.1	P-HRS-02.1		x			03.01.02			
170	Human Resources Security	Roles & Responsibilities	HRS-03	P-HRS-03		x			03.01.22.a 03.06.04.a 03.06.05.d 03.07.06.a 03.08.02 03.15.03.b 03.16.03.b	A.03.06.05.d		
171	Human Resources Security	User Awareness	HRS-03.1	P-HRS-03.1		x			03.01.22.a 03.15.03.b			
172	Human Resources Security	Competency Requirements for Security-Related Positions	HRS-03.2	P-HRS-03.2		x			03.07.06.d			
173	Human Resources Security	Personnel Screening	HRS-04	P-HRS-04	x	x	3.9.1	3.9.1	03.09.01.a	A.03.09.01.ODP[01] A.03.09.01.a A.03.09.01.b		PS.L2-3.9.1
174	Human Resources Security	Roles With Special Protection Measures	HRS-04.1	P-HRS-04.1		x			03.01.22.a 03.02.02.a.01 03.09.01.a 03.09.01.b	A.03.09.01.ODP[01]		
175	Human Resources Security	Formal Indoctrination	HRS-04.2	P-HRS-04.2		x			03.01.22.a 03.02.02.a.01 03.06.04.a 03.06.04.a.01 03.15.03.b			
176	Human Resources Security	Terms of Employment	HRS-05	P-HRS-05	x	x	NFO - PL-4		03.01.01.h 03.01.22.a 03.15.03.a	A.03.15.03.b		
177	Human Resources Security	Rules of Behavior	HRS-05.1	P-HRS-05.1	x	x	NFO - PL-4		03.01.12.a 03.01.18.a 03.01.22.a 03.15.03.a	A.03.15.03.ODP[01] A.03.15.03.a A.03.15.03.d[01] A.03.15.03.d[02]		
178	Human Resources Security	Social Media & Social Networking Restrictions	HRS-05.2	P-HRS-05.2	x	x	NFO - PL-4(1)		03.15.03.a	A.03.15.03.a		
179	Human Resources Security	Use of Communications Technology	HRS-05.3	P-HRS-05.3		x			03.01.01.h 03.01.12.a 03.01.18.a 03.15.03.a	A.03.15.03.a		
180	Human Resources Security	Use of Critical Technologies	HRS-05.4	P-HRS-05.4		x			03.15.03.a			
181	Human Resources Security	Use of Mobile Devices	HRS-05.5	P-HRS-05.5		x			03.01.18.a 03.15.03.a	A.03.15.03.a		
182	Human Resources Security	Policy Familiarization & Acknowledgement	HRS-05.7	P-HRS-05.7		x			03.15.03.b 03.15.03.c 03.15.03.d	A.03.15.03.c		
183	Human Resources Security	Access Agreements	HRS-06	P-HRS-06	x	x	NFO - PS-6		03.01.18.a 03.12.05.a 03.15.03.b 03.15.03.c			
184	Human Resources Security	Confidentiality Agreements	HRS-06.1	P-HRS-06.1		x			03.12.05.a 03.15.03.c			
185	Human Resources Security	Personnel Sanctions	HRS-07	P-HRS-07	x	x	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			
186	Human Resources Security	Workplace Investigations	HRS-07.1	P-HRS-07.1		x			03.01.01.f.04 03.01.01.f.05			
187	Human Resources Security	Personnel Transfer	HRS-08	P-HRS-08	x	x	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	A.03.09.02.ODP[01] A.03.09.02.b.01[01] A.03.09.02.b.01[02] A.03.09.02.b.02		PS.L2-3.9.2
188	Human Resources Security	Personnel Termination	HRS-09	P-HRS-09	x	x	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.03 03.09.02.b.01	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] A.03.09.02.a.03		PS.L2-3.9.2
189	Human Resources Security	Asset Collection	HRS-09.1	P-HRS-09.1		x			03.09.02.a.03	A.03.09.02.a.03		
190	Human Resources Security	High-Risk Terminations	HRS-09.2	P-HRS-09.2		x			03.09.02.a.01 03.09.02.a.02 03.09.02.b.01			
191	Human Resources Security	Automated Employment Status Notifications	HRS-09.4	P-HRS-09.4		x			03.01.01.g.02 03.09.02.a.01 03.09.02.a.02			
192	Human Resources Security	Third-Party Personnel Security	HRS-10	P-HRS-10	x	x	NFO - PS-7		03.16.03.b			
193	Human Resources Security	Separation of Duties (SoD)	HRS-11	P-HRS-11	x	x	3.1.4	3.1.4[a] 3.1.4[b] 3.1.4[c]	03.01.04.a	A.03.01.04.a		AC.L2-3.1.4
194	Human Resources Security	Incompatible Roles	HRS-12	P-HRS-12		x			03.01.04.a			
195	Identification & Authentication	Identity & Access Management (IAM)	IAC-01	P-IAC-01	x	x	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.e			
196	Identification & Authentication	Authenticate, Authorize and Audit (AAA)	IAC-01.2	P-IAC-01.2		x			03.05.01.a 03.05.02 03.05.05.d 03.05.07.a 03.05.07.b 03.05.07.c 03.05.07.d 03.05.07.e 03.05.12.d 03.05.12.f 03.07.05.a	A.03.01.01.d.01 A.03.01.01.d.02 A.03.01.16.b A.03.05.01.a[01] A.03.05.01.a[02]		
197	Identification & Authentication	Identification & Authentication for Organizational Users	IAC-02	P-IAC-02	x	x	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	A.03.05.01.a[03]	IA.L1-3.5.1 IA.L1-3.5.2	IA.L1-3.5.1 IA.L1-3.5.2
198	Identification & Authentication	Replay-Resistant Authentication	IAC-02.2	P-IAC-02.2	x	x	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]		IA.L2-3.5.4
199	Identification & Authentication	Identification & Authentication for Non-Organizational Users	IAC-03	P-IAC-03		x			03.05.01.a			

#	NCP Policy Title	NCP Standard Title	NCP Standard #	NCP Procedure #	NIST 800-171 R2 Only	NIST 800-171 R3 Only	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US CMMC 2.0 Level 1	US CMMC 2.0 Level 2
200	Identification & Authentication	Identification & Authentication for Devices	IAC-04	P-IAC-04	x	x	3.5.2		03.01.18.b 03.05.02	A.03.05.02.ODP[01] A.03.05.02[01] A.03.05.02[02]	IA.L1-3.5.2	IA.L1-3.5.2
201	Identification & Authentication	Identification & Authentication for Third Party Systems & Services	IAC-05	P-IAC-05		x			03.05.01.a 03.05.02			
202	Identification & Authentication	Privileged Access by Non-Organizational Users	IAC-05.2	P-IAC-05.2		x			03.07.05.a			
203	Identification & Authentication	Multi-Factor Authentication (MFA)	IAC-06	P-IAC-06	x	x	3.5.3		03.05.03 03.07.05.b	A.03.05.03[01] A.03.05.03[02] A.03.07.05.b[01]		IA.L2-3.5.3
204	Identification & Authentication	Network Access to Privileged Accounts	IAC-06.1	P-IAC-06.1	x	x	3.5.3	3.5.3[a] 3.5.3[c]	03.05.03			IA.L2-3.5.3
205	Identification & Authentication	Network Access to Non-Privileged Accounts	IAC-06.2	P-IAC-06.2	x	x	3.5.3	3.5.3[d]	03.05.03			IA.L2-3.5.3
206	Identification & Authentication	Local Access to Privileged Accounts	IAC-06.3	P-IAC-06.3	x	x	3.5.3	3.5.3[a] 3.5.3[b]	03.05.03			IA.L2-3.5.3
207	Identification & Authentication	Out-of-Band Multi-Factor Authentication	IAC-06.4	P-IAC-06.4		x				A.03.05.03[01] A.03.05.03[02]		
208	Identification & Authentication	User Provisioning & De-Provisioning	IAC-07	P-IAC-07		x			03.01.01.g.01 03.01.01.g.02 03.01.01.g.03 03.05.05.a 03.09.02.a.01 03.09.02.a.02	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.03.05.05.a		
209	Identification & Authentication	Change of Roles & Duties	IAC-07.1	P-IAC-07.1		x			03.01.01.g.01 03.01.01.g.02 03.01.01.g.03 03.05.05.a 03.09.02.b.02			
210	Identification & Authentication	Termination of Employment	IAC-07.2	P-IAC-07.2		x			03.09.02.a.01 03.09.02.a.02			
211	Identification & Authentication	Role-Based Access Control (RBAC)	IAC-08	P-IAC-08	x	x	3.1.1 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 03.01.12.a 03.03.08.b 03.04.05 03.06.05.d 03.07.06.a	A.03.01.01.c.02 A.03.01.01.c.03 A.03.01.05.ODP[01] A.03.01.05.ODP[02] A.03.01.05.b[01] A.03.01.05.b[02] A.03.04.05[04] A.03.06.05.d		AC.L2-3.1.3
212	Identification & Authentication	Identifier Management (User Names)	IAC-09	P-IAC-09	x	x	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		IA.L2-3.5.5
213	Identification & Authentication	User Identity (ID) Management	IAC-09.1	P-IAC-09.1		x			03.05.05.b			
214	Identification & Authentication	Identity User Status	IAC-09.2	P-IAC-09.2		x			03.05.05.d	A.03.05.05.ODP[02] A.03.05.05.d		
215	Identification & Authentication	Privileged Account Identifiers	IAC-09.5	P-IAC-09.5		x			03.01.07.b 03.05.05.d			
216	Identification & Authentication	Authenticator Management	IAC-10	P-IAC-10	x	x	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 03.05.12.a 03.05.12.b 03.05.12.c 03.05.12.d 03.05.12.e 03.05.12.f	A.03.05.12.ODP[01] A.03.05.12.ODP[02] A.03.05.12.a A.03.05.12.b A.03.05.12.c[01] A.03.05.12.c[02] A.03.05.12.c[03] A.03.05.12.c[04] A.03.05.12.c[05] A.03.05.12.c[06] A.03.05.12.d A.03.05.12.e A.03.05.12.f[01] A.03.05.12.f[02]		IA.L2-3.5.8 IA.L2-3.5.9
217	Identification & Authentication	Password-Based Authentication	IAC-10.1	P-IAC-10.1	x	x	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.c 03.05.12.d 03.05.12.e 03.05.12.f	A.03.05.07.ODP[02] A.03.05.07.f		IA.L2-3.5.7
218	Identification & Authentication	In-Person or Trusted Third-Party Registration	IAC-10.3	P-IAC-10.3		x			03.05.12.a			
219	Identification & Authentication	Automated Support For Password Strength	IAC-10.4	P-IAC-10.4		x			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		
220	Identification & Authentication	Protection of Authenticators	IAC-10.5	P-IAC-10.5	x	x	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]		IA.L2-3.5.10
221	Identification & Authentication	No Embedded Unencrypted Static Authenticators	IAC-10.6	P-IAC-10.6		x			03.05.07.d			
222	Identification & Authentication	Vendor-Supplied Defaults	IAC-10.8	P-IAC-10.8		x			03.05.07.e 03.05.12.d			
223	Identification & Authentication	Password Managers	IAC-10.11	P-IAC-10.11		x			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		
224	Identification & Authentication	Authenticator Feedback	IAC-11	P-IAC-11	x	x	3.5.11	3.5.11	03.05.11	A.03.05.11		IA.L2-3.5.11
225	Identification & Authentication	Re-Authentication	IAC-14	P-IAC-14		x			03.05.01.b	A.03.05.01.ODP[01] A.03.05.01.b		

#	NCP Policy Title	NCP Standard Title	NCP Standard #	NCP Procedure #	NIST 800-171 R2 Only	NIST 800-171 R3 Only	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US CMMC 2.0 Level 1	US CMMC 2.0 Level 2
226	Identification & Authentication	Account Management	IAC-15	P-IAC-15	x	x	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 03.01.01.e 03.01.01.f.01 03.01.01.f.03 03.01.01.f.04 03.01.01.f.05 03.01.01.g.01 03.01.01.g.02 03.01.01.g.03 03.01.02 03.01.05.b 03.01.05.c 03.01.05.d	A.03.01.01.ODP[01] A.03.01.01.a[01] A.03.01.01.a[02] A.03.01.01.c.01 A.03.01.01.e A.03.01.01.f.01 A.03.01.01.f.02 A.03.01.01.f.03 A.03.01.01.f.04 A.03.01.01.f.05 A.03.01.01.g.01 A.03.01.01.g.02 A.03.01.01.g.03 A.03.05.07.e	AC.L1-3.1.2	AC.L1-3.1.2
227	Identification & Authentication	Automated System Account Management (Directory Services)	IAC-15.1	P-IAC-15.1	x	x	3.1.1		03.05.05.b 03.05.05.c 03.05.05.d 03.05.07.c 03.05.07.d 03.05.07.e 03.05.07.f 03.05.12.d 03.05.12.e 03.05.12.f			
228	Identification & Authentication	Disable Inactive Accounts	IAC-15.3	P-IAC-15.3	x	x	3.5.6	3.5.6[a] 3.5.6[b]	03.01.01.f.02	A.03.01.01.f.02		IA.L2-3.5.6
229	Identification & Authentication	Restrictions on Shared Groups / Accounts	IAC-15.5	P-IAC-15.5		x			03.01.01.c.01			
230	Identification & Authentication	Account Disabling for High Risk Individuals	IAC-15.6	P-IAC-15.6		x			03.01.01.f.04 03.01.01.f.05			
231	Identification & Authentication	System Account Reviews	IAC-15.7	P-IAC-15.7		x			03.01.01.e 03.01.05.c	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] A.03.01.01.b[04] A.03.01.01.b[05] A.03.01.01.c.01		
232	Identification & Authentication	Privileged Account Management (PAM)	IAC-16	P-IAC-16	x	x	3.1.5		03.01.06.a 03.01.07.a 03.01.07.b			AC.L2-3.1.5
233	Identification & Authentication	Privileged Account Inventories	IAC-16.1	P-IAC-16.1	x		3.1.5					AC.L2-3.1.5
234	Identification & Authentication	Periodic Review of Account Privileges	IAC-17	P-IAC-17		x			03.01.01.g.03 03.01.05.c 03.01.05.d 03.10.01.c 03.10.01.d	A.03.01.05.ODP[03] A.03.01.05.c A.03.01.05.d		
235	Identification & Authentication	Access Enforcement	IAC-20	P-IAC-20	x	x	3.1.1	3.1.1[a] 3.1.1[b] 3.1.1[c] 3.1.1[d] 3.1.1[e] 3.1.1[f]	03.01.01.c.03 03.01.01.d.01 03.01.01.d.02 03.01.02 03.01.03 03.01.04.b 03.01.05.a 03.01.05.b 03.01.06.a 03.09.02.b.02		AC.L1-3.1.1	AC.L1-3.1.1
236	Identification & Authentication	Access To Sensitive / Regulated Data	IAC-20.1	P-IAC-20.1		x			03.01.01.c.03 03.01.01.d.01 03.01.01.d.02 03.01.02 03.01.03 03.01.04.b 03.01.05.a 03.06.05.d 03.10.01.a	A.03.01.05.b[01] A.03.01.05.b[02] A.03.06.05.d		
237	Identification & Authentication	Least Privilege	IAC-21	P-IAC-21	x	x	3.1.5	3.1.5[a] 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 03.01.04.b 03.01.05.a 03.01.05.b 03.01.06.a 03.01.07.a 03.03.08.a 03.03.08.b 03.04.05	A.03.01.02[02] A.03.01.05.a		AC.L2-3.1.5
238	Identification & Authentication	Authorize Access to Security Functions	IAC-21.1	P-IAC-21.1	x		3.1.5					AC.L2-3.1.5
239	Identification & Authentication	Non-Privileged Access for Non-Security Functions	IAC-21.2	P-IAC-21.2	x	x	3.1.6	3.1.6[a] 3.1.6[b]	03.01.06.b	A.03.01.06.b		AC.L2-3.1.6
240	Identification & Authentication	Privileged Accounts	IAC-21.3	P-IAC-21.3	x	x	3.1.5		03.01.06.a 03.01.07.a	A.03.01.06.ODP[01] A.03.01.06.a		AC.L2-3.1.5
241	Identification & Authentication	Auditing Use of Privileged Functions	IAC-21.4	P-IAC-21.4	x	x	3.1.7		03.01.07.b			AC.L2-3.1.7
242	Identification & Authentication	Prohibit Non-Privileged Users from Executing Privileged Functions	IAC-21.5	P-IAC-21.5	x	x	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		AC.L2-3.1.7
243	Identification & Authentication	Account Lockout	IAC-22	P-IAC-22	x	x	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		AC.L2-3.1.8
244	Identification & Authentication	Session Lock	IAC-24	P-IAC-24	x	x	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		AC.L2-3.1.10
245	Identification & Authentication	Pattern-Hiding Displays	IAC-24.1	P-IAC-24.1	x	x	3.1.10		03.01.10.c	A.03.01.10.c		AC.L2-3.1.10

#	NCP Policy Title	NCP Standard Title	NCP Standard #	NCP Procedure #	NIST 800-171 R2 Only	NIST 800-171 R3 Only	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US CMMC 2.0 Level 1	US CMMC 2.0 Level 2
246	Identification & Authentication	Session Termination	IAC-25	P-IAC-25	x	x	3.1.11	3.1.11[a] 3.1.11[b]	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 A.03.01.11.ODP[01] A.03.07.05.c[01] A.03.07.05.c[01]		AC.L2-3.1.11
247	Identification & Authentication	Identity Proofing (Identity Verification)	IAC-28	P-IAC-28		x			03.05.12.a 03.05.12.c			
248	Identification & Authentication	Management Approval For New or Changed Accounts	IAC-28.1	P-IAC-28.1		x			03.01.01.b 03.05.05.a			
249	Incident Response	Incident Response Operations	IRO-01	P-IRO-01	x	x	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]		
250	Incident Response	Incident Handling	IRO-02	P-IRO-02	x	x	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] 3.6.1[f] 3.6.1[g] 3.6.2[a] 3.6.2[b] 3.6.2[c] 3.6.2[d] 3.6.2[e] 3.6.2[f]	03.03.04.b 03.06.01 03.06.02.a 03.06.02.b 03.06.02.c 03.06.02.d	A.03.06.01[02] A.03.06.01[03] A.03.06.01[04] A.03.06.01[05] A.03.06.01[06] A.03.06.02.b		IR.L2-3.6.1 IR.L2-3.6.2
251	Incident Response	Incident Response Plan (IRP)	IRO-04	P-IRO-04	x	x	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 03.06.05.a.04 03.06.05.a.05 03.06.05.a.06 03.06.05.b	A.03.06.02.ODP[01] A.03.06.02.ODP[02] A.03.06.05.a.01 A.03.06.05.a.02 A.03.06.05.a.03 A.03.06.05.a.04 A.03.06.05.a.05 A.03.06.05.a.06 A.03.06.05.b[01] A.03.06.05.b[02]		
252	Incident Response	IRP Update	IRO-04.2	P-IRO-04.2	x	x	NFO - IR-1		03.06.04.b 03.06.05.c	A.03.06.05.c		
253	Incident Response	Continuous Incident Response Improvements	IRO-04.3	P-IRO-04.3		x			03.06.04.b			
254	Incident Response	Incident Response Training	IRO-05	P-IRO-05	x	x	3.6.1		03.06.04.a 03.06.04.a.03	A.03.06.04.ODP[01] A.03.06.04.ODP[02] A.03.06.04.ODP[03] A.03.06.04.ODP[04] A.03.06.04.a.01 A.03.06.04.b[01] A.03.06.04.b[02] A.03.06.04.b[03] A.03.06.04.b[04]		IR.L2-3.6.1
255	Incident Response	Incident Response Testing	IRO-06	P-IRO-06	x	x	3.6.3	3.6.3	03.06.03	A.03.06.03 A.03.06.03.ODP[01]		IR.L2-3.6.3
256	Incident Response	Integrated Security Incident Response Team (ISIRT)	IRO-07	P-IRO-07		x				A.03.06.02.b A.03.06.02.d		
257	Incident Response	Situational Awareness For Incidents	IRO-09	P-IRO-09		x			03.06.02.a 03.06.02.b	A.03.06.02.a[01] A.03.06.02.a[02]		
258	Incident Response	Incident Stakeholder Reporting	IRO-10	P-IRO-10		x			03.06.02.b 03.06.02.c	A.03.06.02.ODP[01] A.03.06.02.b A.03.06.02.c A.03.06.02.d		
259	Incident Response	Cyber Incident Reporting for Sensitive Data	IRO-10.2	P-IRO-10.2		x			03.06.02.b 03.06.02.c	A.03.06.02.ODP[02]		
260	Incident Response	Incident Reporting Assistance	IRO-11	P-IRO-11		x			03.06.02.d	A.03.06.02.d		
261	Incident Response	Information Spillage Response	IRO-12	P-IRO-12		x			03.06.01	A.03.01.22.b[02]		
262	Incident Response	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	P-IRO-13	x	x	NFO - IR-1		03.06.04.b			
263	Incident Response	Regulatory & Law Enforcement Contacts	IRO-14	P-IRO-14		x			03.06.02.c	A.03.06.02.ODP[02]		
264	Information Assurance	Information Assurance (IA) Operations	IAO-01	P-IAO-01	x	x	NFO - CA-1		03.12.01			
265	Information Assurance	Assessment Boundaries	IAO-01.1	P-IAO-01.1		x			03.12.01			
266	Information Assurance	Assessments	IAO-02	P-IAO-02	x		3.12.1					CA.L2-3.12.1
267	Information Assurance	Assessor Independence	IAO-02.1	P-IAO-02.1	x		NFO - CA-2(1)					
268	Information Assurance	System Security & Privacy Plan (SSPP)	IAO-03	P-IAO-03	x	x	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] 3.12.4[g] 3.12.4[h]	03.04.11.b 03.15.02.a 03.15.02.a.01 03.15.02.a.02 03.15.02.a.03 03.15.02.a.04 03.15.02.a.05 03.15.02.a.06 03.15.02.a.07 03.15.02.a.08 03.15.02.b	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] A.03.15.02.a.01 A.03.15.02.a.02 A.03.15.02.a.03 A.03.15.02.a.04 A.03.15.02.a.05 A.03.15.02.a.06 A.03.15.02.a.07 A.03.15.02.a.08 A.03.15.02.b[01] A.03.15.02.b[02] A.03.15.02.c		CA.L2-3.12.4
269	Information Assurance	Plan / Coordinate with Other Organizational Entities	IAO-03.1	P-IAO-03.1	x		NFO - PL-2(3)					
270	Information Assurance	Adequate Security for Sensitive / Regulated Data In Support of Contracts	IAO-03.2	P-IAO-03.2	x		3.12.4					CA.L2-3.12.4

#	NCP Policy Title	NCP Standard Title	NCP Standard #	NCP Procedure #	NIST 800-171 R2 Only	NIST 800-171 R3 Only	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US CMMC 2.0 Level 1	US CMMC 2.0 Level 2
271	Information Assurance	Plan of Action & Milestones (POA&M)	IAO-05	P-IAO-05	x	x	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 03.12.02.b.02 03.12.02.b.03 03.14.01.a	A.03.12.02.a.01 A.03.12.02.a.02 A.03.12.02.b.01 A.03.12.02.b.02 A.03.12.02.b.03		CA.L2-3.12.2
272	Maintenance	Maintenance Operations	MNT-01	P-MNT-01	x	x	NFO - MA-1		03.04.03.c 03.07.04.a 03.07.06.a			
273	Maintenance	Controlled Maintenance	MNT-02	P-MNT-02	x	x	3.7.1	3.7.1	03.04.03.c 03.07.04.a 03.07.05.a	A.03.04.03.c[01]		MA.L2-3.7.1
274	Maintenance	Timely Maintenance	MNT-03	P-MNT-03		x			03.07.04.a			
275	Maintenance	Preventative Maintenance	MNT-03.1	P-MNT-03.1		x			03.07.04.a			
276	Maintenance	Maintenance Tools	MNT-04	P-MNT-04	x	x	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]		MA.L2-3.7.2
277	Maintenance	Inspect Tools	MNT-04.1	P-MNT-04.1	x	x	3.7.1		03.07.04.b			MA.L2-3.7.1
278	Maintenance	Inspect Media	MNT-04.2	P-MNT-04.2	x	x	3.7.4	3.7.4		A.03.07.04.b		MA.L2-3.7.4
279	Maintenance	Prevent Unauthorized Removal	MNT-04.3	P-MNT-04.3		x			03.07.04.c	A.03.07.04.c		
280	Maintenance	Remote Maintenance	MNT-05	P-MNT-05	x	x	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.03.07.05.a[01] A.03.07.05.a[02]		MA.L2-3.7.5
281	Maintenance	Auditing Remote Maintenance	MNT-05.1	P-MNT-05.1		x			03.07.05.a			
282	Maintenance	Remote Maintenance Notifications	MNT-05.2	P-MNT-05.2	x		NFO - MA-4(2)					
283	Maintenance	Remote Maintenance Cryptographic Protection	MNT-05.3	P-MNT-05.3		x			03.07.05.b	A.03.07.05.b[02]		
284	Maintenance	Remote Maintenance Disconnect Verification	MNT-05.4	P-MNT-05.4		x			03.07.05.c	A.03.07.05.c[01]		
285	Maintenance	Remote Maintenance Pre-Approval	MNT-05.5	P-MNT-05.5		x			03.07.05.a			
286	Maintenance	Authorized Maintenance Personnel	MNT-06	P-MNT-06	x	x	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] A.03.07.06.d[02]		MA.L2-3.7.6
287	Maintenance	Maintenance Personnel Without Appropriate Access	MNT-06.1	P-MNT-06.1		x			03.07.06.a 03.07.06.c 03.07.06.d	A.03.07.06.c		
288	Maintenance	Non-System Related Maintenance	MNT-06.2	P-MNT-06.2		x			03.07.06.a 03.07.06.c	A.03.07.06.c		
289	Maintenance	Off-Site Maintenance	MNT-09	P-MNT-09		x			03.07.04.a			
290	Mobile Device Management	Centralized Management Of Mobile Devices	MDM-01	P-MDM-01	x	x	3.1.18		03.01.18.a 03.01.20.d	A.03.01.18.a[01]		AC.L2-3.1.18
291	Mobile Device Management	Access Control For Mobile Devices	MDM-02	P-MDM-02	x	x	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.b		AC.L2-3.1.18
292	Mobile Device Management	Full Device & Container-Based Encryption	MDM-03	P-MDM-03	x	x	3.1.19	3.1.19[a] 3.1.19[b]	03.01.18.c	A.03.01.18.c		AC.L2-3.1.19
293	Mobile Device Management	Mobile Device Tampering	MDM-04	P-MDM-04		x			03.04.12.b			
294	Mobile Device Management	Personally-Owned Mobile Devices	MDM-06	P-MDM-06	x	x	3.1.18		03.01.18.a 03.01.18.b			AC.L2-3.1.18
295	Mobile Device Management	Organization-Owned Mobile Devices	MDM-07	P-MDM-07	x	x	3.1.18		03.01.18.a 03.01.18.b 03.01.20.d			AC.L2-3.1.18
296	Mobile Device Management	Restricting Access To Authorized Devices	MDM-11	P-MDM-11		x			03.01.18.b			
297	Network Security	Network Security Controls (NSC)	NET-01	P-NET-01	x	x	NFO - SC-1		03.01.12.a 03.01.16.a 03.01.16.b 03.01.18.a 03.13.01.a			
298	Network Security	Layered Network Defenses	NET-02	P-NET-02		x			03.13.01.b			
299	Network Security	Boundary Protection	NET-03	P-NET-03	x	x	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] 3.13.1[g] 3.13.1[h]	03.01.12.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.c	SC.L1-3.13.1	SC.L1-3.13.1
300	Network Security	Limit Network Connections	NET-03.1	P-NET-03.1	x		NFO - SC-7(3)					
301	Network Security	External Telecommunications Services	NET-03.2	P-NET-03.2	x		NFO - SC-7(4)					
302	Network Security	Separate Subnet for Connecting to Different Security Domains	NET-03.8	P-NET-03.8		x			03.13.01.b			
303	Network Security	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	P-NET-04	x	x	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]		AC.L2-3.1.3
304	Network Security	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	P-NET-04.1	x	x	3.13.6 NFO - CA-3(5)	3.13.6[a] 3.13.6[b]	03.13.01.a 03.13.06	A.03.13.06[01] A.03.13.06[02]		SC.L2-3.13.6
305	Network Security	Interconnection Security Agreements (ISAs)	NET-05	P-NET-05	x	x	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.03.12.05.ODP[01] A.03.12.05.ODP[02] A.03.12.05.a[01] A.03.12.05.a[02] A.03.12.05.b[01] A.03.12.05.b[02] A.03.12.05.b[03] A.03.12.05.c[01] A.03.12.05.c[02]		
306	Network Security	Internal System Connections	NET-05.2	P-NET-05.2	x	x	NFO - CA-9		03.01.03 03.12.05.a 03.12.05.b 03.12.05.c			
307	Network Security	Network Segmentation (macrosegementation)	NET-06	P-NET-06	x	x	3.13.5	3.13.5[a] 3.13.5[b]	03.13.01.b	A.03.13.01.b	SC.L1-3.13.5	SC.L1-3.13.5

#	NCP Policy Title	NCP Standard Title	NCP Standard #	NCP Procedure #	NIST 800-171 R2 Only	NIST 800-171 R3 Only	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US CMMC 2.0 Level 1	US CMMC 2.0 Level 2
308	Network Security	Sensitive / Regulated Data Enclave (Secure Zone)	NET-06.3	P-NET-06.3		x			03.13.01.b			
309	Network Security	Network Connection Termination	NET-07	P-NET-07	x	x	3.13.9	3.13.9[a] 3.13.9[b] 3.13.9[c]	03.13.09	A.03.07.05.c[02] A.03.13.09 A.03.13.09.ODP[01]		SC.L2-3.13.9
310	Network Security	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-08	P-NET-08	x	x	3.14.6		03.13.01.a 03.14.06.c			SI.L2-3.14.6
311	Network Security	DMZ Networks	NET-08.1	P-NET-08.1		x			03.13.01.b			
312	Network Security	Session Integrity	NET-09	P-NET-09	x	x	3.13.15	3.13.15	03.13.15	A.03.13.15		SC.L2-3.13.15
313	Network Security	Domain Name Service (DNS) Resolution	NET-10	P-NET-10	x		NFO - SC-20					
314	Network Security	Architecture & Provisioning for Name / Address Resolution Service	NET-10.1	P-NET-10.1	x		NFO - SC-22					
315	Network Security	Secure Name / Address Resolution Service (Recursive or Caching Resolver)	NET-10.2	P-NET-10.2	x		NFO - SC-21					
316	Network Security	Electronic Messaging	NET-13	P-NET-13	x		3.13.14	3.13.14[a] 3.13.14[b]				SC.L2-3.13.14
317	Network Security	Remote Access	NET-14	P-NET-14	x	x	3.1.12		03.01.12.a 03.01.12.b 03.01.12.c 03.01.12.d	A.03.01.12.a[01] A.03.01.12.a[02] A.03.01.12.a[03] A.03.01.12.a[04] A.03.01.12.b A.03.01.12.c[01] A.03.01.12.c[02] A.03.01.12.d[1] A.03.01.12.d[2]		AC.L2-3.1.12
318	Network Security	Automated Monitoring & Control	NET-14.1	P-NET-14.1	x	x	3.1.12	3.1.12[a] 3.1.12[b] 3.1.12[c] 3.1.12[d]	03.01.12.b			AC.L2-3.1.12
319	Network Security	Protection of Confidentiality / Integrity Using Encryption	NET-14.2	P-NET-14.2	x	x	3.1.13	3.1.13[a] 3.1.13[b]	03.01.12.a			AC.L2-3.1.13
320	Network Security	Managed Access Control Points	NET-14.3	P-NET-14.3	x	x	3.1.14	3.1.14[a] 3.1.14[b]	03.01.12.b 03.01.12.c			AC.L2-3.1.14
321	Network Security	Remote Privileged Commands & Sensitive Data Access	NET-14.4	P-NET-14.4	x	x	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
322	Network Security	Work From Anywhere (WFA) - Telecommuting Security	NET-14.5	P-NET-14.5	x	x	3.1.12 3.10.6		03.01.12.a 03.01.12.c 03.10.06.a 03.10.06.b	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
323	Network Security	Wireless Networking	NET-15	P-NET-15	x	x	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]		AC.L2-3.1.16
324	Network Security	Authentication & Encryption	NET-15.1	P-NET-15.1	x	x	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.d[01] A.03.01.16.d[02]		AC.L2-3.1.17
325	Network Security	Disable Wireless Networking	NET-15.2	P-NET-15.2		x			03.01.16.c			
326	Network Security	Restrict Configuration By Users	NET-15.3	P-NET-15.3		x			03.01.16.a 03.01.16.c			
327	Network Security	DNS & Content Filtering	NET-18	P-NET-18	x	x	3.1.3		03.14.06.c			AC.L2-3.1.3
328	Physical & Environmental Security	Physical & Environmental Protections	PES-01	P-PES-01	x	x	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			PE.L2-3.10.2
329	Physical & Environmental Security	Physical Access Authorizations	PES-02	P-PES-02	x	x	3.10.1	3.10.1[a] 3.10.1[b] 3.10.1[c] 3.10.1[d]	03.08.01 03.08.02 03.10.01.a 03.10.01.b 03.10.01.c 03.10.01.d 03.10.07.a	A.03.04.05[02] A.03.10.01.ODP[01] A.03.10.01.a[01] A.03.10.01.a[02] A.03.10.01.a[03] A.03.10.01.c A.03.10.01.d A.03.10.07.a.01	PE.L1-3.10.1	PE.L1-3.10.1
330	Physical & Environmental Security	Role-Based Physical Access	PES-02.1	P-PES-02.1		x			03.08.01 03.08.02 03.10.01.b 03.10.01.d	A.03.04.05[01] A.03.10.01.ODP[01] A.03.10.01.b		
331	Physical & Environmental Security	Physical Access Control	PES-03	P-PES-03	x	x	3.10.5	3.10.5[a] 3.10.5[b] 3.10.5[c]	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.03.10.07.a.02 A.03.10.07.d	PE.L1-3.10.5	PE.L1-3.10.5
332	Physical & Environmental Security	Controlled Ingress & Egress Points	PES-03.1	P-PES-03.1		x			03.10.02.a 03.10.07.a 03.10.07.a.02			
333	Physical & Environmental Security	Physical Access Logs	PES-03.3	P-PES-03.3	x	x	3.10.4 NFO - PE-8	3.10.4	03.10.02.a 03.10.07.b	A.03.10.07.b	PE.L1-3.10.4	PE.L1-3.10.4
334	Physical & Environmental Security	Access To Information Systems	PES-03.4	P-PES-03.4		x			03.10.07.a.01 03.10.07.a.02			
335	Physical & Environmental Security	Physical Security of Offices, Rooms & Facilities	PES-04	P-PES-04	x	x	3.10.5		03.08.01 03.08.02 03.10.07.a.01 03.10.07.a.02 03.10.07.d		PE.L1-3.10.5	PE.L1-3.10.5
336	Physical & Environmental Security	Working in Secure Areas	PES-04.1	P-PES-04.1		x			03.08.01 03.08.02 03.10.07.a.01 03.10.07.a.02 03.10.07.d			
337	Physical & Environmental Security	Monitoring Physical Access	PES-05	P-PES-05	x	x	3.10.2		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
338	Physical & Environmental Security	Intrusion Alarms / Surveillance Equipment	PES-05.1	P-PES-05.1	x	x	3.10.2 NFO - PE-6(1)		03.10.02.a 03.10.02.b			PE.L2-3.10.2
339	Physical & Environmental Security	Monitoring Physical Access To Information Systems	PES-05.2	P-PES-05.2	x	x	3.10.2		03.10.02.a 03.10.02.b			PE.L2-3.10.2

#	NCP Policy Title	NCP Standard Title	NCP Standard #	NCP Procedure #	NIST 800-171 R2 Only	NIST 800-171 R3 Only	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US CMMC 2.0 Level 1	US CMMC 2.0 Level 2
340	Physical & Environmental Security	Visitor Control	PES-06	P-PES-06	x	x	3.10.3	3.10.3[a] 3.10.3[b]	03.10.02.b 03.10.07.c	A.03.10.07.c[01] A.03.10.07.c[02]	PE.L1-3.10.3	PE.L1-3.10.3
341	Physical & Environmental Security	Identification Requirement	PES-06.2	P-PES-06.2		x			03.10.07.c			
342	Physical & Environmental Security	Restrict Unescorted Access	PES-06.3	P-PES-06.3	x	x	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]	PE.L1-3.10.3	PE.L1-3.10.3
343	Physical & Environmental Security	Visitor Access Revocation	PES-06.6	P-PES-06.6		x			03.10.07.c			
344	Physical & Environmental Security	Supporting Utilities	PES-07	P-PES-07		x			03.10.08			
345	Physical & Environmental Security	Delivery & Removal	PES-10	P-PES-10	x		NFO - PE-16					
346	Physical & Environmental Security	Alternate Work Site	PES-11	P-PES-11	x	x	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		PE.L2-3.10.6
347	Physical & Environmental Security	Equipment Siting & Protection	PES-12	P-PES-12	x	x	3.10.1		03.10.07.e 03.10.08		PE.L1-3.10.1	PE.L1-3.10.1
348	Physical & Environmental Security	Transmission Medium Security	PES-12.1	P-PES-12.1	x	x	3.10.1		03.10.08	A.03.10.08	PE.L1-3.10.1	PE.L1-3.10.1
349	Physical & Environmental Security	Access Control for Output Devices	PES-12.2	P-PES-12.2	x	x	3.10.1		03.10.07.e	A.03.10.07.e	PE.L1-3.10.1	PE.L1-3.10.1
350	Project & Resource Management	Cybersecurity & Data Privacy Portfolio Management	PRM-01	P-PRM-01	x	x	NFO - PL-1		03.16.01			
351	Project & Resource Management	Allocation of Resources	PRM-03	P-PRM-03	x		NFO - SA-2					
352	Project & Resource Management	Cybersecurity & Data Privacy Requirements Definition	PRM-05	P-PRM-05		x			03.16.01			
353	Project & Resource Management	Secure Development Life Cycle (SDLC) Management	PRM-07	P-PRM-07	x		NFO - SA-3					
354	Risk Management	Risk Management Program	RSK-01	P-RSK-01	x	x	NFO - RA-1		03.11.01.a 03.17.01.a	A.03.17.03.b		
355	Risk Management	Risk Framing	RSK-01.1	P-RSK-01.1		x			03.11.01.a	A.03.11.01.a		
356	Risk Management	Risk-Based Security Categorization	RSK-02	P-RSK-02		x			03.11.01.a			
357	Risk Management	Impact-Level Prioritization	RSK-02.1	P-RSK-02.1		x			03.11.01.a 03.14.03.b			
358	Risk Management	Risk Identification	RSK-03	P-RSK-03		x			03.11.01.a	A.03.11.01.a		
359	Risk Management	Risk Catalog	RSK-03.1	P-RSK-03.1		x			03.15.02.a.03	A.03.11.01.a		
360	Risk Management	Risk Assessment	RSK-04	P-RSK-04	x	x	3.11.1	3.11.1[a] 3.11.1[b]	03.11.01.a	A.03.11.01.a A.03.11.01.b		RA.L2-3.11.1
361	Risk Management	Risk Register	RSK-04.1	P-RSK-04.1		x			03.12.02.a.01 03.12.02.a.02			
362	Risk Management	Risk Ranking	RSK-05	P-RSK-05		x			03.11.01.a			
363	Risk Management	Risk Remediation	RSK-06	P-RSK-06	x	x	3.11.3		03.11.02.b 03.12.02.a.02			RA.L2-3.11.3
364	Risk Management	Risk Response	RSK-06.1	P-RSK-06.1		x			03.11.02.b 03.11.04	A.03.11.04[01] A.03.11.04[02] A.03.11.04[03]		
365	Risk Management	Compensating Countermeasures	RSK-06.2	P-RSK-06.2		x			03.11.02.b			
366	Risk Management	Risk Assessment Update	RSK-07	P-RSK-07		x			03.11.01.b	A.03.11.01.ODP[01] A.03.11.01.b		
367	Risk Management	Supply Chain Risk Management (SCRM) Plan	RSK-09	P-RSK-09		x			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] A.03.17.01.a[05] A.03.17.01.a[06] A.03.17.01.a[07] A.03.17.01.a[08] A.03.17.01.a[09] A.03.17.01.a[10] A.03.17.01.b[01] A.03.17.01.b[02] A.03.17.01.c A.03.17.03.ODP[01] A.03.17.03.a[01] A.03.17.03.a[02] A.03.17.03.b		
368	Risk Management	Supply Chain Risk Assessment	RSK-09.1	P-RSK-09.1		x			03.11.01.a 03.11.01.b 03.17.03.a			
369	Secure Engineering & Architecture	Secure Engineering Principles	SEA-01	P-SEA-01	x	x	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.b 03.01.16.c 03.01.18.a 03.13.01.c 03.16.01	A.03.16.01.ODP[01]		SC.L2-3.13.2
370	Secure Engineering & Architecture	Alignment With Enterprise Architecture	SEA-02	P-SEA-02	x	x	NFO - PL-8		03.01.12.a 03.01.16.a 03.01.18.a 03.13.01.c 03.16.01			
371	Secure Engineering & Architecture	Defense-In-Depth (DiD) Architecture	SEA-03	P-SEA-03	x		3.13.2					SC.L2-3.13.2
372	Secure Engineering & Architecture	Application Partitioning	SEA-03.2	P-SEA-03.2	x		3.13.3	3.13.3[a] 3.13.3[b] 3.13.3[c]				SC.L2-3.13.3
373	Secure Engineering & Architecture	Process Isolation	SEA-04	P-SEA-04	x		NFO - SC-39					
374	Secure Engineering & Architecture	Information In Shared Resources	SEA-05	P-SEA-05	x	x	3.13.4	3.13.4	03.13.04	A.03.13.04[01] A.03.13.04[02]		SC.L2-3.13.4
375	Secure Engineering & Architecture	Predictable Failure Analysis	SEA-07	P-SEA-07	x	x	NFO - SA-3		03.16.02.b			
376	Secure Engineering & Architecture	Technology Lifecycle Management	SEA-07.1	P-SEA-07.1	x	x	NFO - SA-3		03.16.02.a 03.16.02.b			

#	NCP Policy Title	NCP Standard Title	NCP Standard #	NCP Procedure #	NIST 800-171 R2 Only	NIST 800-171 R3 Only	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US CMMC 2.0 Level 1	US CMMC 2.0 Level 2
377	Secure Engineering & Architecture	Memory Protection	SEA-10	P-SEA-10	x		NFO - SI-16					
378	Secure Engineering & Architecture	System Use Notification (Logon Banner)	SEA-18	P-SEA-18	x	x	3.1.9	3.1.9[a] 3.1.9[b]	03.01.09	A.03.01.09		AC.L2-3.1.9
379	Secure Engineering & Architecture	Standardized Microsoft Windows Banner	SEA-18.1	P-SEA-18.1	x	x	3.1.9	3.1.9[a] 3.1.9[b]	03.01.09	A.03.01.09		AC.L2-3.1.9
380	Secure Engineering & Architecture	Truncated Banner	SEA-18.2	P-SEA-18.2	x	x	3.1.9	3.1.9[a] 3.1.9[b]	03.01.09	A.03.01.09		AC.L2-3.1.9
381	Secure Engineering & Architecture	Clock Synchronization	SEA-20	P-SEA-20	x		3.3.7					AU.L2-3.3.7
382	Security Operations	Operations Security	OPS-01	P-OPS-01		x			03.15.01.a 03.15.01.b			
383	Security Operations	Standardized Operating Procedures (SOP)	OPS-01.1	P-OPS-01.1		x			03.15.01.a	A.03.15.01.a[03] A.03.15.01.a[04] A.03.15.01.b[01] A.03.15.01.b[02]		
384	Security Operations	Service Delivery (Business Process Support)	OPS-03	P-OPS-03		x			03.15.01.b			
385	Security Awareness & Training	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	P-SAT-01	x	x	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] A.03.02.01.a.01[02]		
386	Security Awareness & Training	Cybersecurity & Data Privacy Awareness Training	SAT-02	P-SAT-02	x	x	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 03.02.01.b 03.06.04.a.03	A.03.02.01.ODP[03] A.03.02.01.ODP[04]		AT.L2-3.2.1
387	Security Awareness & Training	Social Engineering & Mining	SAT-02.2	P-SAT-02.2		x			03.02.01.a.03	A.03.02.01.a.03[03] A.03.02.01.a.03[04] A.03.02.01.a.03[05] A.03.02.01.a.03[06]		
388	Security Awareness & Training	Role-Based Cybersecurity & Data Privacy Training	SAT-03	P-SAT-03	x	x	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 03.02.02.b 03.06.04.a 03.06.04.a.01 03.06.04.a.02 03.06.04.b	A.03.02.02.ODP[01] A.03.02.02.ODP[02] A.03.02.02.ODP[03] A.03.02.02.ODP[04] A.03.02.02.a.01[01] A.03.02.02.a.01[02] A.03.02.02.a.01[03] A.03.02.02.a.02 A.03.02.02.b[01] A.03.02.02.b[02] A.03.06.04.a.01 A.03.06.04.a.02 A.03.06.04.a.03		AT.L2-3.2.2
389	Security Awareness & Training	Sensitive Information Storage, Handling & Processing	SAT-03.3	P-SAT-03.3		x			03.01.22.a 03.02.01.a.01 03.02.02.a.01			
390	Security Awareness & Training	Privileged Users	SAT-03.5	P-SAT-03.5		x			03.02.01.a.01 03.02.02.a.01			
391	Security Awareness & Training	Cyber Threat Environment	SAT-03.6	P-SAT-03.6		x			03.02.01.a.01 03.02.01.a.02 03.02.01.a.03 03.02.01.b 03.02.02.a.01 03.02.02.a.02 03.02.02.b 03.06.04.a.02	A.03.02.01.a.02 A.03.02.01.b[01] A.03.02.01.b[02]		
392	Security Awareness & Training	Continuing Professional Education (CPE) - Cybersecurity & Data Privacy Personnel	SAT-03.7	P-SAT-03.7		x			03.06.04.b			
393	Security Awareness & Training	Cybersecurity & Data Privacy Training Records	SAT-04	P-SAT-04	x		NFO - AT-4					
394	Technology Development & Acquisition	Technology Development & Acquisition	TDA-01	P-TDA-01	x	x	NFO - SA-4		03.12.01 03.12.03 03.14.01.a 03.16.01 03.17.02	A.03.16.01.ODP[01] A.03.17.02[04] A.03.17.02[05] A.03.17.02[06]		
395	Technology Development & Acquisition	Product Management	TDA-01.1	P-TDA-01.1		x			03.12.03			
396	Technology Development & Acquisition	Minimum Viable Product (MVP) Security Requirements	TDA-02	P-TDA-02	x		NFO - SA-4					
397	Technology Development & Acquisition	Ports, Protocols & Services In Use	TDA-02.1	P-TDA-02.1	x		NFO - SA-4(9)					
398	Technology Development & Acquisition	Information Assurance Enabled Products	TDA-02.2	P-TDA-02.2	x		NFO - SA-4(10)					
399	Technology Development & Acquisition	Development Methods, Techniques & Processes	TDA-02.3	P-TDA-02.3		x			03.16.01			
400	Technology Development & Acquisition	Pre-Established Secure Configurations	TDA-02.4	P-TDA-02.4		x			03.16.01			
401	Technology Development & Acquisition	Commercial Off-The-Shelf (COTS) Security Solutions	TDA-03	P-TDA-03		x			03.16.01			
402	Technology Development & Acquisition	Documentation Requirements	TDA-04	P-TDA-04	x		NFO - SA-5					
403	Technology Development & Acquisition	Functional Properties	TDA-04.1	P-TDA-04.1	x		NFO - SA-4(1) NFO - SA-4(2)					
404	Technology Development & Acquisition	Developer Architecture & Design	TDA-05	P-TDA-05		x			03.16.01			
405	Technology Development & Acquisition	Secure Coding	TDA-06	P-TDA-06	x	x	NFO - SA-1	3.13.2[b] 3.13.2[e]	03.16.01			
406	Technology Development & Acquisition	Separation of Development, Testing and Operational Environments	TDA-08	P-TDA-08	x		3.4.5					CM.L2-3.4.5
407	Technology Development & Acquisition	Cybersecurity & Data Privacy Testing Throughout Development	TDA-09	P-TDA-09	x	x	NFO - SA-11		03.12.01 03.12.03 03.14.01.a			

#	NCP Policy Title	NCP Standard Title	NCP Standard #	NCP Procedure #	NIST 800-171 R2 Only	NIST 800-171 R3 Only	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US CMMC 2.0 Level 1	US CMMC 2.0 Level 2
408	Technology Development & Acquisition	Continuous Monitoring Plan	TDA-09.1	P-TDA-09.1		x			03.12.03			
409	Technology Development & Acquisition	Developer Configuration Management	TDA-14	P-TDA-14	x		NFO - SA-10					
410	Technology Development & Acquisition	Unsupported Systems	TDA-17	P-TDA-17		x			03.16.02.a	A.03.16.02.a		
411	Technology Development & Acquisition	Alternate Sources for Continued Support	TDA-17.1	P-TDA-17.1		x			03.16.02.b	A.03.16.02.b		
412	Third-Party Management	Third-Party Management	TPM-01	P-TPM-01	x	x	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.03.17.03.ODP[01]		
413	Third-Party Management	Third-Party Inventories	TPM-01.1	P-TPM-01.1		x			03.07.06.a			
414	Third-Party Management	Third-Party Criticality Assessments	TPM-02	P-TPM-02		x			03.11.01.a 03.17.03.a			
415	Third-Party Management	Supply Chain Protection	TPM-03	P-TPM-03		x			03.11.01.a 03.17.01.a 03.17.03.a 03.17.03.b			
416	Third-Party Management	Acquisition Strategies, Tools & Methods	TPM-03.1	P-TPM-03.1		x			03.17.01.a 03.17.02 03.17.03.a 03.17.03.b	A.03.17.02[01] A.03.17.02[02] A.03.17.02[03]		
417	Third-Party Management	Limit Potential Harm	TPM-03.2	P-TPM-03.2		x			03.17.03.a 03.17.03.b			
418	Third-Party Management	Processes To Address Weaknesses or Deficiencies	TPM-03.3	P-TPM-03.3		x			03.17.03.a 03.17.03.b			
419	Third-Party Management	Third-Party Services	TPM-04	P-TPM-04	x	x	NFO -SA-9		03.16.03.a 03.16.03.c 03.17.02 03.17.03.a 03.17.03.b			
420	Third-Party Management	Third-Party Risk Assessments & Approvals	TPM-04.1	P-TPM-04.1		x			03.11.01.a 03.17.02 03.17.03.a 03.17.03.b	A.03.17.03.a[01]		
421	Third-Party Management	External Connectivity Requirements - Identification of Ports, Protocols & Services	TPM-04.2	P-TPM-04.2	x		NFO - SA-9(2)					
422	Third-Party Management	Third-Party Processing, Storage and Service Locations	TPM-04.4	P-TPM-04.4		x			03.16.03.a			
423	Third-Party Management	Third-Party Contract Requirements	TPM-05	P-TPM-05	x	x	3.1.1		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 03.16.03.c 03.17.02 03.17.03.b	A.03.16.03.ODP[01] A.03.16.03.a	AC.L1-3.1.1	AC.L1-3.1.1
424	Third-Party Management	Security Compromise Notification Agreements	TPM-05.1	P-TPM-05.1		x			03.17.02			
425	Third-Party Management	Contract Flow-Down Requirements	TPM-05.2	P-TPM-05.2	x	x	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]	AC.L1-3.1.1	AC.L1-3.1.1
426	Third-Party Management	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	P-TPM-05.4		x			03.07.06.a 03.16.03.b	A.03.16.03.b		
427	Third-Party Management	Third-Party Scope Review	TPM-05.5	P-TPM-05.5		x			03.16.03.c 03.17.02 03.17.03.a 03.17.03.b	A.03.16.03.c		
428	Third-Party Management	First-Party Declaration (1PD)	TPM-05.6	P-TPM-05.6		x			03.01.20.c.01 03.16.03.c	A.03.16.03.c		
429	Third-Party Management	Break Clauses	TPM-05.7	P-TPM-05.7		x			03.17.01.a 03.17.02 03.17.03.b			
430	Third-Party Management	Third-Party Attestation	TPM-05.8	P-TPM-05.8		x			03.01.20.a 03.01.20.b 03.01.20.c.01 03.16.03.a 03.16.03.c	A.03.16.03.c		
431	Third-Party Management	Review of Third-Party Services	TPM-08	P-TPM-08		x			03.16.03.c 03.17.02	A.03.16.03.c		
432	Third-Party Management	Third-Party Deficiency Remediation	TPM-09	P-TPM-09		x			03.17.02			
433	Third-Party Management	Managing Changes To Third-Party Services	TPM-10	P-TPM-10	x	x	NFO - SA-4		03.16.01 03.17.02			
434	Threat Management	Threat Intelligence Program	THR-01	P-THR-01	x	x	3.12.3 3.14.3		03.11.02.a 03.14.03.a			CA.L2-3.12.3 SI.L2-3.14.3
435	Threat Management	Threat Intelligence	THR-03	P-THR-03	x	x	3.14.3		03.02.01.a.02 03.02.01.a.03 03.02.01.b 03.02.02.b 03.11.02.a 03.14.03.a	A.03.14.03.a		SI.L2-3.14.3
436	Threat Management	Threat Intelligence Reporting	THR-03.1	P-THR-03.1		x			03.14.03.b	A.03.14.03.b[01] A.03.14.03.b[02]		
437	Threat Management	Insider Threat Awareness	THR-05	P-THR-05	x	x	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
438	Threat Management	Threat Catalog	THR-09	P-THR-09		x			03.15.02.a.03			
439	Threat Management	Threat Analysis	THR-10	P-THR-10		x			03.14.03.b			
440	Vulnerability & Patch Management	Vulnerability & Patch Management Program (VPMP)	VPM-01	P-VPM-01	x	x	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]	SI.L1-3.14.1	SI.L1-3.14.1
441	Vulnerability & Patch Management	Attack Surface Scope	VPM-01.1	P-VPM-01.1		x			03.11.02.a 03.14.01.a	A.03.11.02.a[01]		

#	NCP Policy Title	NCP Standard Title	NCP Standard #	NCP Procedure #	NIST 800-171 R2 Only	NIST 800-171 R3 Only	NIST 800-171 R2	NIST 800-171A	NIST 800-171 R3	NIST 800-171A R3	US CMMC 2.0 Level 1	US CMMC 2.0 Level 2
442	Vulnerability & Patch Management	Vulnerability Remediation Process	VPM-02	P-VPM-02	x	x		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]		
443	Vulnerability & Patch Management	Vulnerability Ranking	VPM-03	P-VPM-03		x			03.11.02.a			
444	Vulnerability & Patch Management	Continuous Vulnerability Remediation Activities	VPM-04	P-VPM-04		x			03.11.02.b 03.14.01.a 03.14.01.b	A.03.11.02.b		
445	Vulnerability & Patch Management	Software & Firmware Patching	VPM-05	P-VPM-05	x	x	3.11.3		03.11.02.b 03.12.02.a.02 03.14.01.a 03.14.01.b	A.03.11.02.b A.03.14.01.ODP[01] A.03.14.01.ODP[02] A.03.14.01.a[01] A.03.14.01.a[02] A.03.14.01.a[03] A.03.14.01.b[01] A.03.14.01.b[02]		RA.L2-3.11.3
446	Vulnerability & Patch Management	Vulnerability Scanning	VPM-06	P-VPM-06	x	x	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	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] A.03.11.02.a[04] A.03.11.02.c[01] A.03.11.02.c[02]		RA.L2-3.11.2
447	Vulnerability & Patch Management	Update Tool Capability	VPM-06.1	P-VPM-06.1	x	x	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]		
448	Vulnerability & Patch Management	Privileged Access	VPM-06.3	P-VPM-06.3	x		3.11.2					RA.L2-3.11.2