NIST 800-171 CSOP Procedure #	Procedure Description	NIST 800-171 rev 1	NIST 800-53 rev 4	Executive Leadership	Chief Information Officer (CIO)	Chief Data Security Officer (CDSO)	Enterprise Governance, Risk & Compliance (GRC)	Internal Audit	Legal	Procurement	Human Resources (HR)	Physical Security	Project Managers (PMs)	Line Managers / Supervisors	Security Governance, Risk & Compliance (GRC)	Security Architecture & Engineering	Identity & Access Management (IAM)	Change Control	Security Operations Center (SOC)	End User Computing (EUC)	Vulnerability Management	Incident Response	Threat Intelligence	Privacy	Service Desk	Asset Management	Mobile Device Administrators	Asset Custodian / Maintenance	Database Administrators	Application Developers	Website Eningeers	Business Continuity / Disaster Recovery	All Users
P-AST-01	Asset Governance	3.4.1 & 3.4.2	PM-5		X																				X							
P-AST-02	Asset Inventories	3.4.1 & 3.4.2	PM-5 & CM-8		X									X											X							
P-AST-02(a)	Updates During Installations / Removals	3.4.1 & 3.4.2	CM-8(1)													X									X							
P-AST-02(c)	Component Duplication Avoidance	NFO	CM-8(5)													X									X							
P-BCP-01	Contingency Plan	3.8.9	PM-8, CP-1 & CP-2	X	X	X	X			X		X		X	X	X															X	
P-BCP-10	Data Backups	3.8.9	CP-9		X	X	X								X																X	
P-CHG-01	Change Management Program	3.4.3 3.4.4 3.4.5	CM-3		X	X	X						X	X	X	X		X			X							X				X
P-CHG-02	Configuration Change Control	3.4.3	CM-3		X	X	X						X	X	X	X		X			X							X				X
P-CHG-02(b)	Test, Validate & Document Changes	NFO	CM-3(2)		X	X	X						X	X	X	X		X			X							X				
P-CHG-03	Security Impact Analysis for Changes	3.4.4	CM-4		X	X	X						X	X	X	X		X			X							X				
P-CHG-04	Access Restriction For Change	3.4.5	CM-5		X	X	X						X	X	X	X		X			X							X				
P-CPL-01	Statutory, Regulatory & Contractual Compliance	3.12.1, 3.12.2, 3.12.3 &	PM-8	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
P-CPL-02	Security Controls Oversight	3.12.1, 3.12.2, 3.12.3 &	PM-14, CA-7 & CA-7(1)	X	X	X	X	X	X	X	X	X	X	X	X										X							
P-CPL-03	Security Assessments	3.12.1, 3.12.2, 3.12.3 &	CA-2		X	X	X	X					X		X										X							
P-CPL-03(a)	Independent Assessors	NFO	CA-7(1)		X	X	X	X							X										X							
P-CFG-01	Configuration Management Program	NFO	CM-1 & CM-9		X	X	X	X		X			X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
P-CFG-02	System Hardening Through Baseline Configurations	3.4.1 & 3.4.2	CM-2 & CM-6											X	X	X										X		X				
P-CFG-02(a)	Reviews & Updates	NFO	CM-2(1)											X	X	X										X		X				
P-CFG-02(c)	Retention Of Previous Configurations	NFO	CM-2(3)											X	X	X										X		X				
P-CFG-02(e)	Configure Systems, Components or Devices for High-Risk Areas	NFO	CM-2(7)											X	X	X										X		X				

NIST 800-171 CSOP Procedure #	Procedure Description	NIST 800-171 rev 1	NIST 800-53 rev 4	Executive Leadership	Chief Information Officer (CIO)	Chief Data Security Officer (CDSO)	Enterprise Governance, Risk & Compliance (GRC)	Internal Audit	Legal	Procurement	Human Resources (HR)	Physical Security	Project Managers (PMs)	Line Managers / Supervisors	Security Governance, Risk & Compliance (GRC)	Security Architecture & Engineering	Identity & Access Management (IAM)	Change Control	Security Operations Center (SOC)	End User Computing (EUC)	Vulnerability Management	Incident Response	Threat Intelligence	Privacy	Service Desk	Asset Management	Mobile Device Administrators	Asset Custodian / Maintenance	Database Administrators	Application Developers	Website Eningeers	Business Continuity / Disaster Recovery	All Users
P-CFG-03	Least Functionality	3.4.6	CM-7											X	X	X											X					
P-CFG-03(a)	Periodic Review	3.4.7	CM-7(1)											X	X	X											X					
P-CFG-03(b)	Prevent Program Execution	3.4.7	CM-7(2)											X	X	X											X					
P-CFG-03(c)	Unauthorized or Authorized Software (Blacklisting or Whitelisting)	3.4.8	CM-7(4) & CM-7(5)											X	X	X											X					
P-CFG-05	User-Installed Software	3.4.9	CM-11								X			X	X	X											X					X
P-MON-01	Continuous Monitoring	NFO	AU-1											X	X	X																
P-MON-01(c)	Inbound & Outbound Communications Traffic	3.14.6	SI-4(4)													X			X													
P-MON-01(d)	System Generated Alerts	NFO	SI-4(5)													X			X													
P-MON-01(f)	Correlate Monitoring Information	3.3.5	AU-6(3) & SI-4(16)													X			X													
P-MON-01(i)	Reviews & Updates	3.3.3	AU-2(3)													X			X													
P-MON-02	Centralized Event Log Collection	3.3.1, 3.3.2, 3.14.6 & 3.14.7	AU-2 AU-2(2) AU-6 &													X			X													
P-MON-03	Content of Audit Records	3.3.1 & 3.3.2	AU-3												X	X			X													
P-MON-03(a)	Additional Audit Information	3.3.1 & 3.3.2	AU-3(1) & AU-6(1)												X	X			X													
P-MON-05	Response To Audit Processing Failures	3.3.4	AU-5				X	X	X						X	X			X													
P-MON-06	Monitoring Reporting	3.3.6	AU-7 & AU-7(1)		X	X	X	X	X						X	X			X													
P-MON-06(a)	System-Level Audit Generation	3.3.1 & 3.3.2	AU-12												X	X																
P-MON-07	Time Stamps	3.3.7	AU-8												X	X												X				
P-MON-07(a)	Synchronization With Authoritative Time Source	3.3.7	AU-8(1)												X	X												X				
P-MON-08	Protection of Audit Information	3.3.8	AU-9												X	X												X				
P-MON-08(b)	Access by Subset of Privileged Users	3.3.9	AU-9(4)												X	X												X				

NIST 800-171 CSOP Procedure #	Procedure Description	NIST 800-171 rev 1	NIST 800-53 rev 4	Executive Leadership	Chief Information Officer (CIO)	Chief Data Security Officer (CDSO)	Enterprise Governance, Risk & Compliance (GRC)	Internal Audit	Legal	Procurement	Human Resources (HR)	Physical Security	Project Managers (PMs)	Line Managers / Supervisors	Security Governance, Risk & Compliance (GRC)	Security Architecture & Engineering	Identity & Access Management (IAM)	Change Control	Security Operations Center (SOC)	End User Computing (EUC)	Vulnerability Management	Incident Response	Threat Intelligence	Privacy	Service Desk	Asset Management	Mobile Device Administrators	Asset Custodian / Maintenance	Database Administrators	Application Developers	Website Eningeers	Business Continuity / Disaster Recovery	All Users
P-CRY-01	Use of Cryptographic Controls	3.13.11	SC-13				X		X						X	X				X				X		X	X						X
P-CRY-01(a)	Alternate Physical Protection	3.13.8	SC-8(1)				X		X						X	X				X													X
P-CRY-03	Transmission Confidentiality	3.13.8	SC-8												X	X				X													
P-CRY-04	Transmission Integrity	3.13.8 & 3.13.16	SC-8 & SC-28(1)												X	X				X													
P-CRY-05	Encrypting Data At Rest	3.13.11	SC-13												X	X				X						X	X						X
P-CRY-08	Public Key Infrastructure (PKI)	3.13.10	SC-12 & SC-17													X	X																
P-CRY-09	Cryptographic Key Management	3.13.10	SC-12													X	X																
P-CRY-09(a)	Symmetric Keys	3.13.10	SC-12(2)													X	X																
P-CRY-09(b)	Asymmetric Keys	3.13.10	SC-12(3)													X	X																
P-CRY-09(c)	Cryptographic Key Loss or Change	3.13.10														X	X																
P-CRY-09(d)	Control & Distribution of Cryptographic Keys	3.13.10														X	X																
P-CRY-09(e)	Assigned Owners	3.13.10														X	X																
P-DCH-01	Data Protection	NFO	MP-1	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
P-DCH-01(a)	Data Stewardship	3.8.1, 3.8.2 & 3.8.3					X		X					X	X	X	X			X													X
P-DCH-02	Data & Asset Classification	3.8.1, 3.8.2 & 3.8.3			X	X	X		X					X	X	X	X			X													X
P-DCH-03	Media Access	3.8.1, 3.8.2 & 3.8.3	MP-2											X	X	X	X			X													X
P-DCH-04	Media Marking	3.8.4	MP-3											X	X	X	X			X													X
P-DCH-05	Media Storage	3.8.1, 3.8.2 & 3.8.3	MP-4											X	X	X	X			X													X
P-DCH-06	Media Transportation	3.8.5	MP-5											X	X	X	X			X													X
P-DCH-06(a)	Custodians	3.8.5												X	X	X	X			X													X

NIST 800-171 CSOP Procedure #	Procedure Description	NIST 800-171 rev 1	NIST 800-53 rev 4	Executive Leadership	Chief Information Officer (CIO)	Chief Data Security Officer (CDSO)	Enterprise Governance, Risk & Compliance (GRC)	Internal Audit	Legal	Procurement	Human Resources (HR)	Physical Security	Project Managers (PMs)	Line Managers / Supervisors	Security Governance, Risk & Compliance (GRC)	Security Architecture & Engineering	Identity & Access Management (IAM)	Change Control	Security Operations Center (SOC)	End User Computing (EUC)	Vulnerability Management	Incident Response	Threat Intelligence	Privacy	Service Desk	Asset Management	Mobile Device Administrators	Asset Custodian / Maintenance	Database Administrators	Application Developers	Website Eningeers	Business Continuity / Disaster Recovery	All Users
P-DCH-06(b)	Cryptographic Protection	3.8.6	MP-5(4)											X	X	X	X			X												X
P-DCH-07	Physical Media Disposal	3.8.1, 3.8.2 & 3.8.3	MP-6							X				X	X	X				X												X
P-DCH-08	Digital Media Sanitization	3.8.1, 3.8.2 & 3.8.3	MP-6							X				X	X	X				X												X
P-DCH-09	Media Use	3.8.7	MP-7											X	X	X				X												X
P-DCH-09(a)	Prohibit Use Without Owner	3.8.8	MP-7(1)											X	X	X				X												
P-DCH-13	Use of External Information Systems	3.1.20	AC-20				X		X	X				X	X	X				X												X
P-DCH-13(a)	Limits of Authorized Use	3.1.20	AC-20(1)				X		X					X	X	X				X												
P-DCH-13(b)	Portable Storage Devices	3.1.21	AC-20(2)				X		X					X	X	X				X												
P-DCH-15	Publicly Accessible Content	3.1.22	AC-22				X		X					X	X																	X
P-DCH-18	Media & Data Retention	3.8.7	SI-12				X		X		X			X	X					X												X
P-END-01	Workstation Security	3.13.16	MP-2	X	X	X	X		X		X				X					X						X		X				X
P-END-02	Endpoint Protection Measures	3.13.16	SC-28												X	X		X		X								X				X
P-END-04	Malicious Code Protection (Anti-Malware)	3.14.1, 3.14.2, 3.14.3,	SI-3												X	X				X								X				X
P-END-04(a)	Automatic Updates	3.14.1, 3.14.2, 3.14.3,	SI-3(2)												X	X				X								X				
P-END-04(e)	Malware Protection Mechanism Testing	3.14.1, 3.14.2, 3.14.3,	SI-3(6)												X	X				X								X				
P-END-10	Mobile Code	3.13.13	SC-18 & SC-27												X	X				X								X				
P-END-14	Collaborative Computing Devices	3.13.12	SC-15												X	X				X								X				
P-HRS-01	Human Resources Security Management	NFO	PS-1			X	X		X		X			X	X																	X
P-HRS-02	Position Categorization	3.9.1 & 3.9.2	PS-2			X	X		X		X			X	X																	X
P-HRS-02(a)	Users With Elevated Privileges	3.9.1 & 3.9.2				X	X		X		X			X	X																	X

NIST 800-171 CSOP Procedure #	Procedure Description	NIST 800-171 rev 1	NIST 800-53 rev 4	Executive Leadership	Chief Information Officer (CIO)	Chief Data Security Officer (CDSO)	Enterprise Governance, Risk & Compliance (GRC)	Internal Audit	Legal	Procurement	Human Resources (HR)	Physical Security	Project Managers (PMs)	Line Managers / Supervisors	Security Governance, Risk & Compliance (GRC)	Security Architecture & Engineering	Identity & Access Management (IAM)	Change Control	Security Operations Center (SOC)	End User Computing (EUC)	Vulnerability Management	Incident Response	Threat Intelligence	Privacy	Service Desk	Asset Management	Mobile Device Administrators	Asset Custodian / Maintenance	Database Administrators	Application Developers	Website Eningeers	Business Continuity / Disaster Recovery	All Users
P-HRS-02(b)	Competency Requirements for Security-Related Positions	3.9.1 & 3.9.2	PS-2			X	X		X		X			X	X																	X
P-HRS-03	Roles & Responsibilities	3.9.1 & 3.9.2	PM-13			X	X		X		X			X	X																	X
P-HRS-04	Personnel Screening	3.9.1 & 3.9.2	PS-3			X	X		X		X			X	X																	X
P-HRS-05	Terms of Employment	3.9.1 & 3.9.2				X	X		X		X			X	X																	X
P-HRS-05(a)	Rules of Behavior	NFO	PL-4 & PL-4(1)			X	X		X		X			X	X																	X
P-HRS-05(b)	Social Media & Social Networking Restrictions	NFO	PL-4(1)			X	X		X		X			X	X																	X
P-HRS-05(c)	Use of Communications Technology	3.13.14	SC-19			X	X		X		X			X	X																	X
P-HRS-05(f)	Confidentiality Agreements	NFO	PS-6			X	X		X		X			X	X																	X
P-HRS-06	Access Agreements	3.9.1 & 3.9.2	PS-6			X	X		X		X			X	X																	X
P-HRS-07	Personnel Sanctions	NFO	PS-8			X	X		X		X			X	X																	X
P-HRS-08	Personnel Transfer	3.9.1 & 3.9.2	PS-5			X	X		X		X			X	X		X															X
P-HRS-09	Personnel Termination	3.9.1 & 3.9.2	PS-4			X	X		X		X			X	X		X															X
P-HRS-09(a)	Asset Collection	3.9.1 & 3.9.2				X	X		X		X			X	X		X															
P-HRS-09(b)	High-Risk Terminations	3.9.1 & 3.9.2				X	X		X		X			X	X		X															
P-HRS-10	Third-Party Personnel Security	NFO	PS-7			X	X		X		X			X	X		X															
P-HRS-11	Separation of Duties	3.1.4	AC-5			X	X		X		X			X	X		X															
P-IAC-01	Identity & Access Management (IAM)	NFO	AC-1 & IA-1											X	X	X	X															X
P-IAC-02	Identification & Authentication for Organizational Users	3.5.1 & 3.5.2	IA-2											X	X	X	X															
P-IAC-02(a)	Network Access to Privileged Accounts	3.5.3	IA-2(1)											X	X	X	X															
P-IAC-02(b)	Network Access to Non-Privileged Accounts	3.5.3	IA-2(2)											X	X	X	X															

NIST 800-171 CSOP Procedure #	Procedure Description	NIST 800-171 rev 1	NIST 800-53 rev 4	Executive Leadership	Chief Information Officer (CIO)	Chief Data Security Officer (CDSO)	Enterprise Governance, Risk & Compliance (GRC)	Internal Audit	Legal	Procurement	Human Resources (HR)	Physical Security	Project Managers (PMs)	Line Managers / Supervisors	Security Governance, Risk & Compliance (GRC)	Security Architecture & Engineering	Identity & Access Management (IAM)	Change Control	Security Operations Center (SOC)	End User Computing (EUC)	Vulnerability Management	Incident Response	Threat Intelligence	Privacy	Service Desk	Asset Management	Mobile Device Administrators	Asset Custodian / Maintenance	Database Administrators	Application Developers	Website Eningeers	Business Continuity / Disaster Recovery	All Users
P-IAC-02(c)	Local Access to Privileged Accounts	3.5.3	IA-2(3)											X	X	X	X															
P-IAC-02(e)	Network Access to Privileged Accounts - Replay Resistant	3.5.4	IA-2(8)											X	X	X	X															
P-IAC-02(f)	Network Access to Non-Privileged Accounts - Replay Resistant	3.5.4	IA-2(9)											X	X	X	X															
P-IAC-03	Identification & Authentication for Non-Organizational Users	3.5.1	IA-8											X	X	X	X															
P-IAC-05	Identification & Authentication for Third Parties	3.5.1	IA-9											X	X	X	X															
P-IAC-06	Multifactor Authentication	3.5.3	IA-2(11)											X	X	X	X															
P-IAC-07	User Provisioning & De-Provisioning	3.5.1	IA-5(3)											X	X	X	X															X
P-IAC-07(b)	Termination of Employment	3.5.1	AC-2(10)											X	X	X	X															X
P-IAC-08	Role-Based Access Control (RBAC)	3.5.1	AC-2(7)											X	X	X	X															
P-IAC-09	Identifier Management (User Names)	3.5.5 & 3.5.6	IA-4											X	X	X	X															X
P-IAC-09(e)	Privileged Account Identifiers	3.1.6												X	X	X	X															X
P-IAC-10	Authenticator Management (Passwords)	3.5.1 & 3.5.2	IA-5 & IA-5(4)											X	X	X	X															X
P-IAC-10(a)	Password-Based Authentication	3.5.7, 3.5.8 & 3.5.9	IA-5(1)											X	X	X	X															
P-IAC-10(h)	Vendor-Supplied Defaults	3.5.7, 3.5.8 & 3.5.9	IA-5											X	X	X	X															X
P-IAC-11	Authenticator Feedback	3.5.11	IA-6											X	X	X	X															
P-IAC-15	Account Management	3.1.1 & 3.1.2	AC-2											X	X	X	X															X
P-IAC-15(b)	Removal of Temporary / Emergency Accounts	3.1.1 & 3.1.2	AC-2(2)											X	X	X	X															
P-IAC-15(c)	Disable Inactive Accounts	3.1.1 & 3.1.2	AC-2(3)											X	X	X	X															
P-IAC-15(e)	Inactivity Logout	3.5.6	AC-2(5)											X	X	X	X															X
P-IAC-17	Periodic Review	3.1.1 & 3.1.2												X	X	X	X															

NIST 800-171 CSOP Procedure #	Procedure Description	NIST 800-171 rev 1	NIST 800-53 rev 4	Executive Leadership	Chief Information Officer (CIO)	Chief Data Security Officer (CDSO)	Enterprise Governance, Risk & Compliance (GRC)	Internal Audit	Legal	Procurement	Human Resources (HR)	Physical Security	Project Managers (PMs)	Line Managers / Supervisors	Security Governance, Risk & Compliance (GRC)	Security Architecture & Engineering	Identity & Access Management (IAM)	Change Control	Security Operations Center (SOC)	End User Computing (EUC)	Vulnerability Management	Incident Response	Threat Intelligence	Privacy	Service Desk	Asset Management	Mobile Device Administrators	Asset Custodian / Maintenance	Database Administrators	Application Developers	Website Eningeers	Business Continuity / Disaster Recovery	All Users
P-IAC-20	Access Enforcement	3.1.1 & 3.1.2	AC-3											X	X	X	X															X
P-IAC-21	Least Privilege	3.1.5	AC-6											X	X	X	X															X
P-IAC-21(a)	Authorize Access to Security Functions	3.1.5	AC-6(1)											X	X	X	X															
P-IAC-21(b)	Non-Privileged Access for Non-Security Functions	3.1.6	AC-6(2)											X	X	X	X															
P-IAC-21(c)	Privileged Accounts	3.1.5	AC-6(5)											X	X	X	X															
P-IAC-21(d)	Auditing Use of Privileged Functions	3.1.7	AC-6(9)											X	X	X	X															
P-IAC-21(e)	Prohibit Non-Privileged Users from Executing Privileged Functions	3.1.7	AC-6(10)											X	X	X	X															
P-IAC-22	Account Lockout	3.1.8	AC-7											X	X	X	X															X
P-IAC-24	Session Lock	3.1.10	AC-11											X	X	X	X															X
P-IAC-24(a)	Pattern-Hiding Displays	3.1.10	AC-11(1)											X	X	X	X															
P-IAC-25	Session Termination	3.1.11	AC-12											X	X	X	X															X
P-IRO-01	Management of Security Incidents	NFO	IR-1			X			X			X		X	X				X			X										
P-IRO-02	Incident Handling	3.6.1 & 3.6.2	IR-4			X			X			X		X	X				X			X										X
P-IRO-04	Incident Response Plan (IRP)	NFO	IR-8			X			X			X		X	X				X			X										
P-IRO-05	Incident Response Training	3.6.1 & 3.6.2	IR-2			X			X			X		X	X				X			X										
P-IRO-06	Incident Response Testing	3.6.3	IR-3			X			X			X		X	X				X			X										
P-IRO-06(a)	Coordination with Related Plans	3.6.3	IR-3(2)			X			X			X		X	X				X			X										
P-IRO-07	Integrated Incident Response Team	3.6.1, 3.6.2 & 3.6.3	IR-7(2)			X			X			X		X	X				X			X										
P-IRO-08	Chain of Custody & Forensics	3.6.1, 3.6.2 & 3.6.3				X			X			X		X	X				X			X										
P-IRO-09	Incident Monitoring	3.6.1 & 3.6.2	IR-5			X			X			X		X	X				X			X										

NIST 800-171 CSOP Procedure #	Procedure Description	NIST 800-171 rev 1	NIST 800-53 rev 4	Executive Leadership	Chief Information Officer (CIO)	Chief Data Security Officer (CDSO)	Enterprise Governance, Risk & Compliance (GRC)	Internal Audit	Legal	Procurement	Human Resources (HR)	Physical Security	Project Managers (PMs)	Line Managers / Supervisors	Security Governance, Risk & Compliance (GRC)	Security Architecture & Engineering	Identity & Access Management (IAM)	Change Control	Security Operations Center (SOC)	End User Computing (EUC)	Vulnerability Management	Incident Response	Threat Intelligence	Privacy	Service Desk	Asset Management	Mobile Device Administrators	Asset Custodian / Maintenance	Database Administrators	Application Developers	Website Eningeers	Business Continuity / Disaster Recovery	All Users
P-IRO-10	Incident Reporting	3.6.1 & 3.6.2	IR-6			X			X			X		X	X				X			X										X
P-IRO-10(b)	Cyber Incident Reporting for Covered Defense Information (CDI)	3.6.1, 3.6.2 & 3.6.3				X			X			X		X	X				X			X										
P-IRO-11	Incident Reporting Assistance	3.6.1 & 3.6.2	IR-7			X			X			X		X	X				X			X										
P-IRO-13	IRP - Root Cause Analysis (RCA) & Lessons Learned	3.6.1, 3.6.2 & 3.6.3	IR-1			X			X			X		X	X				X			X										
P-IAO-01	Information Assurance (IA) Operations	NFO	PM-10 & CA-1			X	X	X	X				X	X	X	X						X						X					X
P-IAO-02	Security Assessments	3.12.1, 3.12.2, 3.12.3 &	CA-2			X	X	X	X				X	X	X	X						X						X					X
P-IAO-02(a)	Independent Assessors	NFO	CA-2(1)			X	X	X	X				X	X	X	X						X						X					
P-IAO-02(b)	Specialized Assessments	3.12.1, 3.12.2, 3.12.3 &	CA-2(2)			X	X	X	X				X	X	X	X						X						X					
P-IAO-03	System Security Plans (SSP)	3.12.1, 3.12.2, 3.12.3 &	PL-2			X	X	X	X				X	X	X	X						X						X					
P-IAO-03(a)	Plan / Coordinate with Other Organizational Entities	NFO	PL-2(3)			X	X	X	X				X	X	X	X						X						X					
P-IAO-04	System Security Plan Update	3.12.1, 3.12.2, 3.12.3 &	PL-3			X	X	X	X				X	X	X	X						X						X					
P-IAO-06	Plan of Action & Milestones (POA&M)	3.12.1, 3.12.2, 3.12.3 &	PM-4 & CA-5			X	X	X	X				X	X	X	X						X						X					
P-MNT-01	Maintenance Operations	NFO	MA-1		X	X	X							X	X	X				X	X							X					X
P-MNT-02	Controlled Maintenance	3.7.1, 3.7.2 & 3.7.3	MA-2		X	X	X							X	X	X				X	X							X					X
P-MNT-04	Maintenance Tools	3.7.1 & 3.7.2	MA-3											X	X	X				X	X							X					
P-MNT-04(a)	Inspect Tools	3.7.1 & 3.7.2	MA-3(1)											X	X	X				X	X							X					
P-MNT-04(b)	Inspect Media	3.7.1, 3.7.2 & 3.7.4	MA-3(2)											X	X	X				X	X							X					
P-MNT-05	Non-Local Maintenance	3.7.5	MA-4											X	X	X				X	X							X					
P-MNT-05(b)	Document Non-Local Maintenance	NFO	MA-4(2)											X	X	X				X	X							X					
P-MNT-06	Maintenance Personnel	3.7.6	MA-5						X		X			X	X	X				X	X							X					

NIST 800-171 CSOP Procedure #	Procedure Description	NIST 800-171 rev 1	NIST 800-53 rev 4	Executive Leadership	Chief Information Officer (CIO)	Chief Data Security Officer (CDSO)	Enterprise Governance, Risk & Compliance (GRC)	Internal Audit	Legal	Procurement	Human Resources (HR)	Physical Security	Project Managers (PMs)	Line Managers / Supervisors	Security Governance, Risk & Compliance (GRC)	Security Architecture & Engineering	Identity & Access Management (IAM)	Change Control	Security Operations Center (SOC)	End User Computing (EUC)	Vulnerability Management	Incident Response	Threat Intelligence	Privacy	Service Desk	Asset Management	Mobile Device Administrators	Asset Custodian / Maintenance	Database Administrators	Application Developers	Website Eningeers	Business Continuity / Disaster Recovery	All Users
P-MDM-01	Centralized Management Of Mobile Devices	3.1.18							X		X			X	X	X				X						X	X	X					X
P-MDM-02	Access Control For Mobile Devices	3.1.18	AC-19						X		X			X	X	X				X						X	X	X					
P-MDM-03	Full Device & Container-Based Encryption	3.1.19	AC-19(5)						X		X			X	X	X				X						X	X	X					
P-MDM-05	Remote Purging	3.1.18 & 3.1.19	MP-6(8)						X		X			X	X	X				X						X	X	X					
P-NET-01	Network Security Management	NFO	SC-1		X	X	X								X	X			X		X		X					X			X		X
P-NET-02(b)	Partitioning	3.13.3	SC-2												X	X			X		X		X					X			X		
P-NET-02(c)	Guest Networks	3.13.1, 3.13.2 & 3.13.5													X	X			X		X		X					X			X		
P-NET-03	Boundary Protection	3.13.1, 3.13.2 & 3.13.5	SC-7												X	X			X		X		X					X			X		
P-NET-03(a)	Access Points	NFO	SC-7(3)												X	X			X		X		X					X			X		
P-NET-03(b)	External Telecommunications Services	NFO	SC-7(4)												X	X			X		X		X					X			X		
P-NET-03(c)	Prevent Split Tunneling for Remote Devices	3.13.7	SC-7(7)												X	X			X		X		X					X			X		
P-NET-03(e)	Proxy Server	3.13.6													X	X			X		X		X					X			X		
P-NET-04	Data Flow Enforcement – Access Control Lists (ACLs)	3.1.3	AC-4												X	X			X		X		X					X			X		
P-NET-04(a)	Deny Traffic by Default & Allow Traffic by Exception	3.13.6	SC-7(5)												X	X		X	X		X		X					X			X		
P-NET-05	Information System Connections	NFO	CA-3												X	X			X		X		X					X			X		
P-NET-05(b)	Restrictions on External System Connections	NFO	CA-3(5)												X	X			X		X		X					X			X		
P-NET-05(c)	Restrictions on Internal System Connections	NFO	CA-9												X	X			X		X		X					X			X		
P-NET-07	Network Disconnect	3.13.9	SC-10												X	X												X					
P-NET-09	Session Authenticity	3.13.15	SC-23												X	X																	
P-NET-10	Domain Name Service (DNS) Resolution	NFO	SC-20												X	X																	

NIST 800-171 CSOP Procedure #	Procedure Description	NIST 800-171 rev 1	NIST 800-53 rev 4	Executive Leadership	Chief Information Officer (CIO)	Chief Data Security Officer (CDSO)	Enterprise Governance, Risk & Compliance (GRC)	Internal Audit	Legal	Procurement	Human Resources (HR)	Physical Security	Project Managers (PMs)	Line Managers / Supervisors	Security Governance, Risk & Compliance (GRC)	Security Architecture & Engineering	Identity & Access Management (IAM)	Change Control	Security Operations Center (SOC)	End User Computing (EUC)	Vulnerability Management	Incident Response	Threat Intelligence	Privacy	Service Desk	Asset Management	Mobile Device Administrators	Asset Custodian / Maintenance	Database Administrators	Application Developers	Website Eningeers	Business Continuity / Disaster Recovery	All Users
P-NET-10(a)	Architecture & Provisioning for Name / Address Resolution Service	NFO	SC-22												X	X																
P-NET-10(b)	Secure Name / Address Resolution Service (Recursive or Caching Resolver)	NFO	SC-21												X	X																
P-NET-14	Remote Access	3.1.1 & 3.1.2	AC-17												X	X																X
P-NET-14(a)	Automated Monitoring & Control	3.1.12	AC-17(1)												X	X																
P-NET-14(b)	Protection of Confidentiality / Integrity Using Encryption	3.1.13	AC-17(2)												X	X																
P-NET-14(c)	Managed Access Control Points	3.1.14	AC-17(3)												X	X																
P-NET-14(d)	Privileged Commands & Access	3.1.15	AC-17(4)												X	X																
P-NET-15	Wireless Networking	3.1.16	AC-18												X	X																
P-NET-15(a)	Authentication & Encryption	3.1.17	AC-18(1)												X	X																
P-PES-01	Physical & Environmental Protections	NFO	PE-1								X	X			X	X	X														X	X
P-PES-02	Physical Access Authorizations	3.10.1 & 3.10.2	PE-2								X	X			X	X	X														X	X
P-PES-02(a)	Role-Based Physical Access	3.10.1 & 3.10.2	PE-2(1)								X	X			X	X	X														X	X
P-PES-03	Physical Access Control	3.10.3, 3.10.4 & 3.10.5	PE-3								X	X			X	X	X														X	X
P-PES-03(a)	Controlled Ingress & Egress Points	3.10.3, 3.10.4 & 3.10.5									X	X			X	X	X														X	X
P-PES-03(b)	Lockable Physical Casings	3.10.3, 3.10.4 & 3.10.5	PE-3(4)								X	X			X	X	X														X	
P-PES-03(c)	Laptop Storage In Automobiles	3.10.3, 3.10.4 & 3.10.5									X	X			X	X	X														X	X
P-PES-03(d)	Physical Access Logs	NFO	PE-8								X	X			X	X	X														X	
P-PES-05	Monitoring Physical Access	3.10.1 & 3.10.2	PE-6								X	X			X	X	X														X	
P-PES-05(a)	Intrusion Alarms / Surveillance Equipment	NFO	PE-6(1)								X	X			X	X	X														X	
P-PES-10	Delivery & Removal	NFO	PE-16									X			X	X									X						X	

NIST 800-171 CSOP Procedure #	Procedure Description	NIST 800-171 rev 1	NIST 800-53 rev 4	Executive Leadership	Chief Information Officer (CIO)	Chief Data Security Officer (CDSO)	Enterprise Governance, Risk & Compliance (GRC)	Internal Audit	Legal	Procurement	Human Resources (HR)	Physical Security	Project Managers (PMs)	Line Managers / Supervisors	Security Governance, Risk & Compliance (GRC)	Security Architecture & Engineering	Identity & Access Management (IAM)	Change Control	Security Operations Center (SOC)	End User Computing (EUC)	Vulnerability Management	Incident Response	Threat Intelligence	Privacy	Service Desk	Asset Management	Mobile Device Administrators	Asset Custodian / Maintenance	Database Administrators	Application Developers	Website Eningeers	Business Continuity / Disaster Recovery	All Users
P-PES-11	Alternate Work Site	3.10.6	PE-17									X			X	X															X	
P-PES-12(a)	Access Control for Transmission Medium	NFO	PE-4									X			X	X									X						X	
P-PES-12(b)	Access Control for Output Devices	3.10.1 & 3.10.2	PE-5									X			X	X									X						X	
P-PRM-01	Security Portfolio Management	NFO	PL-1			X	X		X						X	X								X								X
P-PRM-03	Allocation of Resources	NFO	SA-2			X	X		X						X	X								X								
P-PRM-07	System Development Life Cycle (SDLC)	NFO	SA-3			X	X		X						X	X								X								
P-RSK-01	Risk Management Program (RMP)	NFO	PM-9 & RA-1	X	X	X	X	X	X					X	X																	X
P-RSK-04	Risk Assessment	3.11.1	RA-3				X							X	X																	X
P-SEA-01	Security Engineering Principles	3.13.1 & 3.13.2	SA-8, SC-7(18) & SI-1				X	X						X	X	X				X	X											X
P-SEA-02	Alignment With Enterprise Architecture	NFO	PL-8 & PM-7				X	X						X	X	X				X	X											X
P-SEA-06	Process Isolation	NFO	SC-39				X	X						X	X	X				X	X											
P-SEA-08	Information In Shared Resources	3.13.4	SC-4				X	X						X	X	X				X	X											
P-SEA-15	Memory Protection	NFO	SI-16											X	X	X				X	X											
P-SEA-24	System Use Notification (Logon Banner)	3.1.9	AC-8											X	X	X				X	X											X
P-SAT-01	Security-Minded Workforce	NFO	PM-13 & AT-1			X			X		X			X	X																	X
P-SAT-02	Security Awareness	3.2.1 & 3.2.2	AT-2			X			X		X			X	X																	X
P-SAT-02(b)	Insider Threat	3.2.3	AT-2(2)			X			X		X			X	X																	
P-SAT-03	Security Training	3.2.1 & 3.2.2	AT-3			X			X		X			X	X																	X
P-SAT-04	Security Training Records	NFO	AT-4			X			X		X			X	X																	X
P-TDA-01	Technology Development & Acquisition	NFO	SA-1				X		X	X				X	X															X		X

NIST 800-171 CSOP Procedure #	Procedure Description	NIST 800-171 rev 1	NIST 800-53 rev 4	Executive Leadership	Chief Information Officer (CIO)	Chief Data Security Officer (CDSO)	Enterprise Governance, Risk & Compliance (GRC)	Internal Audit	Legal	Procurement	Human Resources (HR)	Physical Security	Project Managers (PMs)	Line Managers / Supervisors	Security Governance, Risk & Compliance (GRC)	Security Architecture & Engineering	Identity & Access Management (IAM)	Change Control	Security Operations Center (SOC)	End User Computing (EUC)	Vulnerability Management	Incident Response	Threat Intelligence	Privacy	Service Desk	Asset Management	Mobile Device Administrators	Asset Custodian / Maintenance	Database Administrators	Application Developers	Website Eningeers	Business Continuity / Disaster Recovery	All Users
P-TDA-02	Security Requirements	NFO	SA-4				X		X	X				X	X														X			X
P-TDA-02(a)	Ports, Protocols &Services In Use	NFO	SA-4(9)				X		X	X				X	X														X			
P-TDA-02(b)	Use of Approved PIV Products	NFO	SA-4(10) & IA-5(11)				X		X	X				X	X														X			
P-TDA-04	Design & Implementation of Security Controls	NFO	SA-4(2)				X		X	X				X	X														X			
P-TDA-05	Functional Properties of Security Controls	NFO	SA-4(1)				X		X	X				X	X														X			
P-TDA-06	Secure Development	NFO	SA-1				X		X	X				X	X														X			X
P-TDA-12	Security Testing Throughout Development	NFO	SA-11				X		X	X				X	X														X			X
P-TDA-17	Developer Configuration Management	NFO	SA-10				X		X	X				X	X														X			X
P-THR-03	Threat Intelligence Feeds	3.14.1, 3.14.2 & 3.14.3	SI-5			X	X								X								X									
P-TPM-05	Third-Party Services	NFO	SA-9				X		X	X			X		X	X							X						X			X
P-TPM-05(b)	Identification of Functions, Ports, Protocols & Services	NFO	SA-9(2)				X		X	X			X		X	X							X						X			
P-VPM-05	Software Patching	3.14.1, 3.14.2 & 3.14.3	SI-2			X	X								X				X		X		X									X
P-VPM-06	Vulnerability Scanning	3.11.2 & 3.11.3	RA-5			X	X								X				X		X		X									X
P-VPM-06(a)	Update Tool Capability	NFO	RA-5(1)			X	X								X				X		X		X									
P-VPM-06(b)	Update by Frequency / Prior to New Scan / When Identified	NFO	RA-5(2)			X	X								X				X		X		X									
P-VPM-06(d)	Privileged Access	3.11.2	RA-5(5)			X	X								X				X		X		X									