SCF Domain	SCF Control	SCF Control #	Secure Controls Framework (SCF) Control Description	CDPP Standard #	NIST CSF v1.1
Cybersecurity & Privacy Governance	Publishing Cybersecurity & Privacy Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and privacy policies, standards and procedures.	**GOV-02**	ID.GV-1
Cybersecurity & Privacy Governance	Assigned Cybersecurity & Privacy Responsibilities	GOV-04	Mechanisms exist to assign a qualified individual with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and privacy program.	**GOV-04**	ID.AM-6
Cybersecurity & Privacy Governance	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity and privacy program measures of performance.	**GOV-05**	PR.IP-8
Cybersecurity & Privacy Governance	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the mission of the organization.	**GOV-08**	ID.BE-1 ID.BE-2
Asset Management	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	**AST-01**	ID.AM-1
Asset Management	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: ▪ Accurately reflects the current systems, applications and services in use; ▪ Identifies authorized software products, including business justification details; ▪ Is at the level of granularity deemed necessary for tracking and	**AST-02**	ID.AM-1 ID.AM-2 ID.AM-4
Asset Management	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: ▪ Contain sufficient detail to assess the security of the network's architecture; ▪ Reflect the current architecture of the network environment; and ▪ Document all sensitive/regulated data flows.	**AST-04**	ID.AM-3
Asset Management	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	**AST-09**	PR.DS-3
Asset Management	Removal of Assets	AST-11	Mechanisms exist to authorize, control and track technology assets entering and exiting organizational facilities.	**AST-11**	PR.DS-3
Business Continuity & Disaster Recovery	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services.	**BCD-01**	ID.BE-5 PR.IP-9 RC.RP-1
Business Continuity & Disaster Recovery	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical systems, applications and services that support essential missions and business functions.	**BCD-02**	ID.AM-5 ID.BE-5

SCF Domain	SCF Control	SCF Control #	Secure Controls Framework (SCF) Control Description	CDPP Standard #	NIST CSF v1.1
Business Continuity & Disaster Recovery	Contingency Training	BCD-03	Mechanisms exist to adequately train contingency personnel and applicable stakeholders in their contingency roles and responsibilities.	**BCD-03**	PR.IP-10
Business Continuity & Disaster Recovery	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	**BCD-05**	RC.IM-1
Business Continuity & Disaster Recovery	Contingency Planning & Updates	BCD-06	Mechanisms exist to keep contingency plans current with business needs, technology changes and feedback from contingency plan testing activities.	**BCD-06**	RC.IM-2
Business Continuity & Disaster Recovery	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	**BCD-11**	PR.IP-4
Business Continuity & Disaster Recovery	Testing for Reliability & Integrity	BCD-11.1	Mechanisms exist to routinely test backups that verify the reliability of the backup process, as well as the integrity and availability of the data.	**BCD-11.1**	PR.IP-4
Business Continuity & Disaster Recovery	Test Restoration Using Sampling	BCD-11.5	Mechanisms exist to utilize sampling of available backups to test recovery capabilities as part of business continuity plan testing.	**BCD-11.5**	PR.IP-10
Business Continuity & Disaster Recovery	Information System Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of systems to a known state after a disruption, compromise or failure.	**BCD-12**	PR.IP-4
Business Continuity & Disaster Recovery	Failover Capability	BCD-12.2	Mechanisms exist to implement real-time or near-real-time failover capability to maintain availability of critical systems, applications and/or services.	**BCD-12.2**	PR.PT-5
Capacity & Performance Planning	Capacity & Performance Management	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	**CAP-01**	PR.DS-4
Capacity & Performance Planning	Capacity Planning	CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.	**CAP-03**	PR.DS-4
Change Management	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	**CHG-01**	PR.IP-3

SCF Domain	SCF Control	SCF Control #	Secure Controls Framework (SCF) Control Description	CDPP Standard #	NIST CSF v1.1
Change Management	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	**CHG-02**	PR.IP-3
Compliance	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	**CPL-01**	ID.GV-3 PR.IP-5 DE.DP-2
Compliance	Security & Privacy Controls Oversight	CPL-02	Mechanisms exist to provide a security & privacy controls oversight function that reports to the organization's executive leadership.	**CPL-02**	DE.DP-5 PR.IP-5 PR.IP-7
Configuration Management	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	**CFG-01**	PR.IP-1
Configuration Management	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	**CFG-02**	PR.IP-1 PR.IP-3
Configuration Management	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	**CFG-03**	PR.PT-3
Continuous Monitoring	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	**MON-01**	DE.CM-1 DE.DP-1 DE.DP-2 PR.PT-1
Continuous Monitoring	Inbound & Outbound Communications Traffic	MON-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	**MON-01.3**	DE.AE-1
Continuous Monitoring	File Integrity Monitoring (FIM)	MON-01.7	Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-detection technology, on critical assets to generate alerts for unauthorized modifications.	**MON-01.7**	PR.DS-8
Continuous Monitoring	Reviews & Updates	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	**MON-01.8**	PR.PT-1
Continuous Monitoring	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM) or similar automated tool, to support the centralized collection of security-related event logs.	**MON-02**	DE.AE-3

SCF Domain	SCF Control	SCF Control #	Secure Controls Framework (SCF) Control Description	CDPP Standard #	NIST CSF v1.1
Continuous Monitoring	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	**MON-02.1**	DE.AE-3
Continuous Monitoring	Monitoring Reporting	MON-06	Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.	**MON-06**	DE.DP-4
Continuous Monitoring	Anomalous Behavior	MON-16	Mechanisms exist to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	**MON-16**	DE.AE-1
Continuous Monitoring	Insider Threats	MON-16.1	Mechanisms exist to monitor internal personnel activity for potential security incidents.	**MON-16.1**	DE.CM-3
Continuous Monitoring	Third-Party Threats	MON-16.2	Mechanisms exist to monitor third-party personnel activity for potential security incidents.	**MON-16.2**	DE.CM-6
Continuous Monitoring	Unauthorized Activities	MON-16.3	Mechanisms exist to monitor for unauthorized activities, accounts, connections, devices and software.	**MON-16.3**	DE.CM-7
Cryptographic Protections	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	**CRY-01**	PR.DS-1 PR.DS-2
Cryptographic Protections	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	**CRY-03**	PR.DS-2
Cryptographic Protections	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	**CRY-04**	PR.DS-8
Cryptographic Protections	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	**CRY-05**	PR.DS-1
Data Classification & Handling	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	**DCH-01**	PR.DS-5