Policy Domain	Standard #	Standard Name	SCF CORE Fundamentals	US CMMC 2.0 Level 1	US FAR 52.204-21	US FAR 52.204-27	US FAR Section 889	Control Question	Possible Solutions & Considerations Micro-Small Business (<10 staff) BLS Firm Size Classes 1-2	Possible Solutions & Considerations Small Business (10-49 staff) BLS Firm Size Classes 3-4	Possible Solutions & Considerations Medium Business (50-249 staff) BLS Firm Size Classes 5-6	Possible Solutions & Considerations Large Business (250-999 staff) BLS Firm Size Classes 7-8	Possible Solutions & Considerations Enterprise (> 1,000 staff) BLS Firm Size Class 9	AICPA TSC 2017:2022 (used for SOC 2)	BSI Standard 200-1	CIS CSC v8.1	ISO 27001 v2022	ISO 27002 v2022	NIST 800-53 rev5	NIST 800-171 rev2	NIST 800-171 rev3	NIST CSF v2.0
Cybersecurity & Data Protection Governance	GOV-01	Cybersecurity & Data Protection Governance Program						Does the organization facilitate the implementation of cybersecurity and data protection governance controls?	· ComplianceForge - Cybersecurity & Data Protection Program (CDPP) (https://complianceforge.com)	· ComplianceForge - Cybersecurity & Data Protection Program (CDPP) (https://complianceforge.com)	· Steering committee · ComplianceForge - Digital Security Program (DSP) (https://complianceforge.com) · ComplianceForge - Cybersecurity & Data	· Steering committee · ComplianceForge - Digital Security Program (DSP) (https://complianceforge.com) · ComplianceForge - Cybersecurity & Data	· Steering committee · ComplianceForge - Digital Security Program (DSP) (https://complianceforge.com)	CC1.1 CC1.1-POF1 CC1.2 CC2.3-POF5	4 4.1 4.2 4.3 4.4		4.4 5.1 5.1(a) 5.1(b) 5.1(c)	5.1 5.4 5.37	PM-1		03.15.01.a	GV GV.RM-01 GV.RM-03 GV.RR-01 GV.SC
Cybersecurity & Data Protection Governance	GOV-02	Publishing Cybersecurity & Data Protection Documentation	GOV-02					Does the organization establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures?	· ComplianceForge - Cybersecurity & Data Protection Program (CDPP) (https://complianceforge.com) · SCFConnect (https://scfconnect.com)	· ComplianceForge - Cybersecurity & Data Protection Program (CDPP) (https://complianceforge.com) · SCFConnect (https://scfconnect.com)	· ComplianceForge - Digital Security Program (DSP) (https://complianceforge.com) · ComplianceForge - Cybersecurity & Data Protection Program (CDPP)	· ComplianceForge - Digital Security Program (DSP) (https://complianceforge.com) · ComplianceForge - Cybersecurity & Data Protection Program (CDPP)	· ComplianceForge - Digital Security Program (DSP) (https://complianceforge.com)	CC1.2-POF1 CC1.4-POF1 CC2.2-POF1 CC2.2-POF7 CC5.3	4.2 7.3		5.1(a) 5.2 5.2(a) 5.2(b) 5.2(c)	5.1 5.37	AC-1 AT-1 AU-1 CA-1 CM-1		03.15.01.a	GV.PO GV.PO-01 GV.SC-01 GV.SC-03 ID.RA
Cybersecurity & Data Protection Governance	GOV-04	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04					Does the organization assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and data protection program?	· Third-party advisors (e.g., virtual CISO, Managed Security Services Provider (MSSP), etc.)	· Third-party advisors (e.g., virtual CISO, Managed Security Services Provider (MSSP), etc.)	· Chief Information Security Officer (CISO)	· Chief Information Security Officer (CISO)	· Chief Information Security Officer (CISO)	CC1.1 CC1.3 CC5.3-POF2	4.1 4.1.1 4.1.2 4.1.3 4.1.4		5.1(f) 5.1(h) 5.3 5.3(a) 5.3(b)	5.2	PL-9 PM-2 PM-6 PM-29			GV.RM GV.RM-05 GV.RR-01 GV.RR-02
Cybersecurity & Data Protection Governance	GOV-15	Operationalizing Cybersecurity & Data Protection Practices	GOV-15					Does the organization compel data and/or process owners to operationalize cybersecurity and data protection practices for each Technology Asset, Application and/or Service (TAAS) under their control?	· ComplianceForge - Cybersecurity Standardized Operating Procedures (CSOP) (https://complianceforge.com)	· ComplianceForge - Cybersecurity Standardized Operating Procedures (CSOP) (https://complianceforge.com)	· ComplianceForge - Cybersecurity Standardized Operating Procedures (CSOP) (https://complianceforge.com)	· ComplianceForge - Cybersecurity Standardized Operating Procedures (CSOP) (https://complianceforge.com)	· ComplianceForge - Cybersecurity Standardized Operating Procedures (CSOP) (https://complianceforge.com)	CC2.1-POF1 CC2.1-POF2 CC2.1-POF3 CC2.1-POF4 CC3.1-POF5							03.15.01.a 03.17.01.a	
Asset Management	AST-01	Asset Governance		MP.L1-3.8.3	52.204-21(b)(1)(vii)			Does the organization facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls?	· IT Asset Management (ITAM) program	· IT Asset Management (ITAM) program	· IT Asset Management (ITAM) program · Configuration Management Database (CMDB)	· IT Asset Management (ITAM) program · Configuration Management Database (CMDB)	· IT Asset Management (ITAM) program · Configuration Management Database (CMDB)	CC2.1-POF6 CC2.1-POF9 CC3.3-POF1 CC6.1-POF1 CC6.1-POF9		1 2 2.1 2.2		5.30 5.31 7.9	PM-5	3.4.1 3.8.3	03.01.03 03.01.18.a 03.04.11.a 03.07.04.a	GV.SC-04 ID.AM ID.AM-08
Asset Management	AST-02	Asset Inventories	AST-02					Does the organization perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details;	· IT Asset Management (ITAM) program · Configuration Management Database (CMDB) · ManageEngine AssetExplorer (https://manageengine.com)	· IT Asset Management (ITAM) program · Configuration Management Database (CMDB) · ManageEngine AssetExplorer (https://manageengine.com)	· IT Asset Management (ITAM) program · Configuration Management Database (CMDB) · ManageEngine AssetExplorer (https://manageengine.com)	· IT Asset Management (ITAM) program · Configuration Management Database (CMDB) · ManageEngine AssetExplorer (https://manageengine.com)	· IT Asset Management (ITAM) program · Configuration Management Database (CMDB) · ManageEngine AssetExplorer (https://manageengine.com)	CC2.1-POF6 CC2.1-POF9 CC6.1-POF1		1 1.1 2 2.1 2.2		5.9	CM-8 PM-5	3.4.1	03.04.08.a 03.04.08.c 03.04.10.a 03.04.10.b 03.04.11.a	ID.AM ID.AM-01 ID.AM-02
Asset Management	AST-02.8	Data Action Mapping	AST-02.8					Does the organization create and maintain a map of Technology Assets, Applications and/or Services (TAAS) where sensitive/regulated data is stored, transmitted or processed?	· Visio · LucidChart	· Visio · LucidChart	· Visio · LucidChart	· Visio · LucidChart	· Visio · LucidChart	CC2.1-POF5 CC2.1-POF9				5.9	CM-13		03.04.11.a 03.04.11.b	
Asset Management	AST-04	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04					Does the organization maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network	· High-Level Diagram (HLD) · Low-Level Diagram (LLD) · Data Flow Diagram (DFD)	· High-Level Diagram (HLD) · Low-Level Diagram (LLD) · Data Flow Diagram (DFD)	· High-Level Diagram (HLD) · Low-Level Diagram (LLD) · Data Flow Diagram (DFD)	· High-Level Diagram (HLD) · Low-Level Diagram (LLD) · Data Flow Diagram (DFD)	· High-Level Diagram (HLD) · Low-Level Diagram (LLD) · Data Flow Diagram (DFD)	C1.1-POF1 CC2.1 CC2.1-POF2 CC2.1-POF5		3.8 12.4		5.9 8.20	PL-2 SA-4(1) SA-4(2)		03.01.03 03.04.11.a 03.04.11.b	ID.AM-03
Asset Management	AST-09	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	MP.L1-3.8.3	52.204-21(b)(1)(vii)			Does the organization securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components?	· Shred-it (https://shredit.com) · IronMountain (https://ironmountain.com) · BitRaser (https://bitraser.com) · DBAN (https://dban.org) · DoD-strength data erasers	· Shred-it (https://shredit.com) · IronMountain (https://ironmountain.com) · BitRaser (https://bitraser.com) · DBAN (https://dban.org) · DoD-strength data erasers	· Shred-it (https://shredit.com) · IronMountain (https://ironmountain.com) · BitRaser (https://bitraser.com) · DBAN (https://dban.org) · DoD-strength data erasers	· Shred-it (https://shredit.com) · IronMountain (https://ironmountain.com) · BitRaser (https://bitraser.com) · DBAN (https://dban.org) · DoD-strength data erasers	· Shred-it (https://shredit.com) · IronMountain (https://ironmountain.com) · BitRaser (https://bitraser.com) · DBAN (https://dban.org) · DoD-strength data erasers	C1.2-POF2 CC6.5 CC6.5-POF2 P4.3-POF2 P4.3-POF3		3.5		7.14 8.10	SR-12	3.8.3	03.07.04.c 03.08.03	
Asset Management	AST-16	Bring Your Own Device (BYOD) Usage	AST-16					Does the organization implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace?	· Rules of Behavior (RoB) / Acceptable Use · Mobile Device Management (MDM) solution	· Rules of Behavior (RoB) / Acceptable Use · Mobile Device Management (MDM) solution	· Rules of Behavior (RoB) / Acceptable Use · Mobile Device Management (MDM) solution	· Rules of Behavior (RoB) / Acceptable Use · Mobile Device Management (MDM) solution	· Rules of Behavior (RoB) / Acceptable Use · Mobile Device Management (MDM) solution			4.11					03.01.18.a	
Asset Management	AST-17	Prohibited Equipment & Services				52.204-27(b)	889(a)(1)(A) 889(a)(1)(B)	Does the organization govern Supply Chain Risk Management (SCRM) sanctions that require the removal and prohibition of certain Technology Assets, Applications and/or Services (TAAS) that are designated as supply chain threats by a statutory or regulatory body?	· IT Asset Management (ITAM) program	· IT Asset Management (ITAM) program	· IT Asset Management (ITAM) program	· IT Asset Management (ITAM) program	· IT Asset Management (ITAM) program								03.11.01.a 03.16.01	
Business Continuity & Disaster Recovery	BCD-01	Business Continuity Management System (BCMS)						Does the organization facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks)?	· Continuity of Operations Plan (COOP) · Business Continuity Plan (BCP) · Disaster Recovery Plan (DRP) · Business Impact Analysis (BIA) · Criticality assessments	· Continuity of Operations Plan (COOP) · Business Continuity Plan (BCP) · Disaster Recovery Plan (DRP) · Business Impact Analysis (BIA) · Criticality assessments	· Continuity of Operations Plan (COOP) · Business Continuity Plan (BCP) · Disaster Recovery Plan (DRP) · Business Impact Analysis (BIA) · Criticality assessments	· Continuity of Operations Plan (COOP) · Business Continuity Plan (BCP) · Disaster Recovery Plan (DRP) · Business Impact Analysis (BIA) · Criticality assessments	· Continuity of Operations Plan (COOP) · Business Continuity Plan (BCP) · Disaster Recovery Plan (DRP) · Business Impact Analysis (BIA) · Criticality assessments	A1.2 A1.2-POF1 A1.2-POF10 A1.2-POF11 A1.2-POF2		11 11.1		5.29 5.30	CP-1 CP-2 IR-4(3) PM-8 CP-10			GV.SC-08 ID.IM-04 PR.IR-02 PR.IR-03 RC
Business Continuity & Disaster Recovery	BCD-04	Contingency Plan Testing & Exercises	BCD-04					Does the organization conduct tests and/or exercises to evaluate the contingency plan's effectiveness and its readiness to execute the plan?	· Tabletop exercises	· Tabletop exercises	· Tabletop exercises	· Tabletop exercises · Simulated events	· Tabletop exercises · Simulated events	A1.3 A1.3-POF1 A1.3-POF2 CC7.5 CC7.5-POF6				5.29 5.30	CP-4			
Business Continuity & Disaster Recovery	BCD-11	Data Backups	BCD-11					Does the organization create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs)?	· Disaster Recovery Plan (DRP) · On-site data backup solution · Off-site data backup service	· Disaster Recovery Plan (DRP) · On-site data backup solution · Off-site data backup service	· Disaster Recovery Plan (DRP) · On-site data backup solution · Off-site data backup service	· Disaster Recovery Plan (DRP) · On-site data backup solution · Off-site data backup service	· Disaster Recovery Plan (DRP) · On-site data backup solution · Off-site data backup service	A1.2 A1.2-POF7 A1.2-POF8 CC7.5		11.2		8.13	CP-9 SC-28(2)	3.8.9	03.08.09.a	PR.DS-11
Change Management	CHG-01	Change Management Program						Does the organization facilitate the implementation of a change management program?	· VisibleOps (https://itpi.org) · ITIL 4 (https://axelos.com)	· VisibleOps (https://itpi.org) · ITIL 4 (https://axelos.com)	· VisibleOps (https://itpi.org) · ITIL 4 (https://axelos.com)	· VisibleOps (https://itpi.org) · ITIL 4 (https://axelos.com)	· VisibleOps (https://itpi.org) · ITIL 4 (https://axelos.com)	CC2.2-POF13 CC3.4 CC3.4-POF4 CC6.8-POF3 CC8.1			6.3	8.19 8.32	CM-3	3.4.3	03.04.02.b 03.04.03.a	ID.RA-07
Change Management	CHG-02	Configuration Change Control	CHG-02					Does the organization govern the technical configuration change control processes?	· Change Control Board (CCB) · Configuration Management Database (CMDB) · VisibleOps (https://itpi.org) · ITIL 4 (https://axelos.com)	· Change Control Board (CCB) · Configuration Management Database (CMDB) · VisibleOps (https://itpi.org) · ITIL 4 (https://axelos.com)	· Change Control Board (CCB) · Configuration Management Database (CMDB) · VisibleOps (https://itpi.org) · ITIL 4 (https://axelos.com)	· Change Control Board (CCB) · Configuration Management Database (CMDB) · VisibleOps (https://itpi.org) · ITIL 4 (https://axelos.com)	· Change Control Board (CCB) · Configuration Management Database (CMDB) · VisibleOps (https://itpi.org) · ITIL 4 (https://axelos.com)	CC2.2-POF13 CC3.4 CC3.4-POF4 CC6.8-POF3 CC8.1				8.19 8.32	CM-3 SA-8(31)	3.4.3	03.04.02.b 03.04.03.a 03.04.03.b 03.04.03.c	ID.RA-07
Change Management	CHG-03	Security Impact Analysis for Changes	CHG-03					Does the organization analyze proposed changes for potential security impacts, prior to the implementation of the change?	· Change Control Board (CCB) · VisibleOps (https://itpi.org)	· Change Control Board (CCB) · VisibleOps (https://itpi.org)	· Change Control Board (CCB) · VisibleOps (https://itpi.org)	· Change Control Board (CCB) · VisibleOps (https://itpi.org)	· Change Control Board (CCB) · VisibleOps (https://itpi.org)	CC3.4 CC3.4-POF4 CC8.1-POF10 CC8.1-POF3					CM-4	3.4.4	03.04.03.b 03.04.04.a 03.04.11.b	ID.RA-07
Cloud Security	CLD-01	Cloud Services	CLD-01	AC.L1-3.1.22	52.204-21(b)(1)(iv)			Does the organization facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices?	· SCF Integrated Controls Management (ICM) model (https://securecontrolsframework.com/integrated-controls-management) · Data Protection Impact Assessment	· SCF Integrated Controls Management (ICM) model (https://securecontrolsframework.com/integrated-controls-management) · Data Protection Impact Assessment	· SCF Integrated Controls Management (ICM) model (https://securecontrolsframework.com/integrated-controls-management) · Data Protection Impact Assessment	· SCF Integrated Controls Management (ICM) model (https://securecontrolsframework.com/integrated-controls-management) · Data Protection Impact Assessment	· SCF Integrated Controls Management (ICM) model (https://securecontrolsframework.com/integrated-controls-management) · Data Protection Impact Assessment	CC6.1-POF5				5.23		NFO–PL-8		
Cloud Security	CLD-02	Cloud Security Architecture		AC.L1-3.1.22	52.204-21(b)(1)(iv)			Does the organization ensure the cloud security architecture supports its technology strategy to securely design, configure and maintain cloud employments?	· System Security & Privacy Plan (SSPP)	· System Security & Privacy Plan (SSPP)	· Architectural review board · System Security & Privacy Plan (SSPP) · Security architecture roadmaps	· Steering committee · Architectural review board · System Security & Privacy Plan (SSPP) · Security architecture roadmaps	· Steering committee · Architectural review board · System Security & Privacy Plan (SSPP) · Security architecture roadmaps					5.23		NFO–PL-8		
Cloud Security	CLD-06	Multi-Tenant Environments		AC.L1-3.1.22	52.204-21(b)(1)(iv)			Does the organization ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users?	· System Security & Privacy Plan (SSPP)	· System Security & Privacy Plan (SSPP)	· Architectural review board · System Security & Privacy Plan (SSPP) · Security architecture roadmaps	· Steering committee · Architectural review board · System Security & Privacy Plan (SSPP) · Security architecture roadmaps	· Steering committee · Architectural review board · System Security & Privacy Plan (SSPP) · Security architecture roadmaps					5.23		3.1.22		
Cloud Security	CLD-10	Sensitive Data In Public Cloud Providers	CLD-10	AC.L1-3.1.22	52.204-21(b)(1)(iv)			Does the organization limit and manage the storage of sensitive/regulated data in public cloud providers?	· Data Protection Impact Assessment (DPIA) · Security and network architecture diagrams · Data Flow Diagram (DFD)	· Data Protection Impact Assessment (DPIA) · Security and network architecture diagrams · Data Flow Diagram (DFD)	· Data Protection Impact Assessment (DPIA) · Security and network architecture diagrams · Data Flow Diagram (DFD)	· Data Protection Impact Assessment (DPIA) · Security and network architecture diagrams · Data Flow Diagram (DFD)	· Data Protection Impact Assessment (DPIA) · Security and network architecture diagrams · Data Flow Diagram (DFD)							3.1.22		
Compliance	CPL-01	Statutory, Regulatory & Contractual Compliance	CPL-01					Does the organization facilitate the identification and implementation of relevant statutory, regulatory and contractual controls?	· SCF Integrated Controls Management (ICM) model (https://securecontrolsframework.com/integrated-controls-management) · Governance, Risk and Compliance (GRC)	· SCF Integrated Controls Management (ICM) model (https://securecontrolsframework.com/integrated-controls-management) · Governance, Risk and Compliance (GRC)	· SCF Integrated Controls Management (ICM) model (https://securecontrolsframework.com/integrated-controls-management) · Governance, Risk and Compliance (GRC)	· SCF Integrated Controls Management (ICM) model (https://securecontrolsframework.com/integrated-controls-management) · Governance, Risk and Compliance (GRC)	· SCF Integrated Controls Management (ICM) model (https://securecontrolsframework.com/integrated-controls-management) · Governance, Risk and Compliance (GRC)	CC1.5 CC2.2 CC2.3 CC2.3-POF5 CC3.1-POF14	7.1 9		4.1 9.1 9.2 9.2.1 9.2.2	5.31 8.34	PL-1 PM-8	NFO-PL-1	03.04.11.a 03.12.01	GV.OC GV.OC-03 GV.SC-05 PR
Configuration Management	CFG-01	Configuration Management Program						Does the organization facilitate the implementation of configuration management controls?	· Configuration Management (CM) program · Change control program	· Configuration Management (CM) program · Change control program	· Configuration Management (CM) program · Change control program	· Configuration Management (CM) program · Change control program	· Configuration Management (CM) program · Change control program	CC7.1 CC7.1-POF1 CC8.1-POF12 CC8.1-POF6		2 4 4.1 4.2		8.3 8.9 8.12	CM-1 CM-9	NFO-CM-1 NFO-CM-9	03.04.01.a	PR.PS PR.PS-01 PR.PS-05

Policy Domain	Standard #	Standard Name	SCF CORE Fundamentals	US CMMC 2.0 Level 1	US FAR 52.204-21	US FAR 52.204-27	US FAR Section 889	Control Question
Configuration Management	CFG-02	Secure Baseline Configurations	CFG-02					Does the organization develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards?
Configuration Management	CFG-03	Least Functionality	CFG-03					Does the organization configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services?
Continuous Monitoring	MON-01	Continuous Monitoring						Does the organization facilitate the implementation of enterprise-wide monitoring controls?
Continuous Monitoring	MON-01.8	Security Event Monitoring	MON-01.8					Does the organization review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures?
Continuous Monitoring	MON-03	Content of Event Logs	MON-03					Does the organization configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred;
Continuous Monitoring	MON-16	Anomalous Behavior	MON-16					Does the organization utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities?
Cryptographic Protections	CRY-01	Use of Cryptographic Controls						Does the organization facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies?
Cryptographic Protections	CRY-03	Transmission Confidentiality	CRY-03					Are cryptographic mechanisms utilized to protect the confidentiality of data being transmitted?
Cryptographic Protections	CRY-05	Encrypting Data At Rest	CRY-05					Are cryptographic mechanisms utilized to prevent unauthorized disclosure of data at rest?
Cryptographic Protections	CRY-09	Cryptographic Key Management	CRY-09					Does the organization facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys?
Data Classification & Handling	DCH-01	Data Protection		MP.L1-3.8.3	52.204-21(b)(1) 52.204-21(b)(1)(vii)			Does the organization facilitate the implementation of data protection controls?
Data Classification & Handling	DCH-01.2	Sensitive / Regulated Data Protection	DCH-01.2		52.204-21(b)(1)			Does the organization protect sensitive/regulated data wherever it is stored?
Data Classification & Handling	DCH-01.4	Defining Access Authorizations for Sensitive / Regulated Data	DCH-01.4					Does the organization explicitly define authorizations for specific individuals and/or roles for logical and /or physical access to sensitive/regulated data?
Data Classification & Handling	DCH-02	Data & Asset Classification	DCH-02					Does the organization ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements?
Data Classification & Handling	DCH-08	Physical Media Disposal		MP.L1-3.8.3	52.204-21(b)(1)(vii)			Does the organization securely dispose of media when it is no longer required, using formal procedures?
Data Classification & Handling	DCH-09	System Media Sanitization		MP.L1-3.8.3	52.204-21(b)(1)(vii)			Does the organization sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse?
Data Classification & Handling	DCH-13	Use of External Technology Assets, Applications and/or Services (TAAS)	DCH-13	AC.L1-3.1.20	52.204-21(b)(1)(iii)			Does the organization govern how external parties, including Technology Assets, Applications and/or Services (TAAS), are used to securely store, process and transmit data?
Data Classification & Handling	DCH-13.1	Limits of Authorized Use		AC.L1-3.1.20	52.204-21(b)(1)(iii)			Does the organization prohibit external parties, including Technology Assets, Applications and/or Services (TAAS), from storing, processing and transmitting data unless authorized individuals first: (1) Verifying the implementation of required security
Data Classification & Handling	DCH-15	Publicly Accessible Content		AC.L1-3.1.22	52.204-21(b)(1)(iv)			Does the organization control publicly-accessible content?
Data Classification & Handling	DCH-17	Ad-Hoc Transfers	DCH-17	AC.L1-3.1.20	52.204-21(b)(1)(iii)			Does the organization secure ad-hoc exchanges of large digital files with internal or external parties?
Endpoint Security	END-01	Endpoint Device Management (EDM)		SI.L1-3.14.2	52.204-21(b)(1)(xiii)			Does the organization facilitate the implementation of Endpoint Device Management (EDM) controls?
Endpoint Security	END-04	Malicious Code Protection (Anti-Malware)	END-04	SI.L1-3.14.2	52.204-21(b)(1)(xiii)			Does the organization utilize antimalware technologies to detect and eradicate malicious code?
Endpoint Security	END-04.1	Automatic Antimalware Signature Updates		SI.L1-3.14.4	52.204-21(b)(1)(xiv)			Does the organization automatically update antimalware technologies, including signature definitions?

Standard #	Possible Solutions & Considerations Micro-Small Business (<10 staff) BLS Firm Size Classes 1-2	Possible Solutions & Considerations Small Business (10-49 staff) BLS Firm Size Classes 3-4	Possible Solutions & Considerations Medium Business (50-249 staff) BLS Firm Size Classes 5-6	Possible Solutions & Considerations Large Business (250-999 staff) BLS Firm Size Classes 7-8	Possible Solutions & Considerations Enterprise (> 1,000 staff) BLS Firm Size Class 9
CFG-02	· Secure Baseline Configurations (SBC) · Defense Information Security Agency (DISA) Secure Technology Implementation Guides (STIGs) · Center for Internet Security (CIS)	· Secure Baseline Configurations (SBC) · Defense Information Security Agency (DISA) Secure Technology Implementation Guides (STIGs) · Center for Internet Security (CIS)	· Secure Baseline Configurations (SBC) · Defense Information Security Agency (DISA) Secure Technology Implementation Guides (STIGs) · Center for Internet Security (CIS)	· Secure Baseline Configurations (SBC) · Defense Information Security Agency (DISA) Secure Technology Implementation Guides (STIGs) · Center for Internet Security (CIS)	· Secure Baseline Configurations (SBC) · Defense Information Security Agency (DISA) Secure Technology Implementation Guides (STIGs) · Center for Internet Security (CIS)
CFG-03	· Secure Baseline Configurations (SBC) · Defense Information Security Agency (DISA) Secure Technology Implementation Guides (STIGs) · Center for Internet Security (CIS)	· Secure Baseline Configurations (SBC) · Defense Information Security Agency (DISA) Secure Technology Implementation Guides (STIGs) · Center for Internet Security (CIS)	· Secure Baseline Configurations (SBC) · Defense Information Security Agency (DISA) Secure Technology Implementation Guides (STIGs) · Center for Internet Security (CIS)	· Secure Baseline Configurations (SBC) · Defense Information Security Agency (DISA) Secure Technology Implementation Guides (STIGs) · Center for Internet Security (CIS)	· Secure Baseline Configurations (SBC) · Defense Information Security Agency (DISA) Secure Technology Implementation Guides (STIGs) · Center for Internet Security (CIS)
MON-01	· Centralized event logging · Managed Security Services Provider (MSSP)	· Centralized event logging · Security Incident Event Manager (SIEM) · Managed Security Services Provider (MSSP)	· Centralized event logging · Security Incident Event Management (SIEM) · Managed Security Services Provider (MSSP)	· Centralized event logging · Security Incident Event Management (SIEM) · Managed Security Services Provider (MSSP)	· Centralized event logging · Security Incident Event Management (SIEM) · Managed Security Services Provider (MSSP)
MON-01.8	· Managed Security Services Provider (MSSP)	· Security Incident Event Manager (SIEM) · Managed Security Services Provider (MSSP)	· Security Incident Event Manager (SIEM) · Managed Security Services Provider (MSSP)	· Security Incident Event Manager (SIEM) · Managed Security Services Provider (MSSP)	· Security Incident Event Manager (SIEM) · Managed Security Services Provider (MSSP)
MON-03	· Secure Baseline Configurations (SBC)	· Secure Baseline Configurations (SBC)	· Secure Baseline Configurations (SBC)	· Secure Baseline Configurations (SBC)	· Secure Baseline Configurations (SBC)
MON-16	· Indicators of Compromise (IoC) · Indicators of Exposure (IoE) · Managed Security Services Provider (MSSP)	· Indicators of Compromise (IoC) · Indicators of Exposure (IoE) · Security Incident Event Manager (SIEM) · Managed Security Services Provider (MSSP)	· Indicators of Compromise (IoC) · Indicators of Exposure (IoE) · Security Incident Event Manager (SIEM) · Extended Detection and Response (XDR) · Managed Security Services Provider	· Indicators of Compromise (IoC) · Indicators of Exposure (IoE) · Security Incident Event Manager (SIEM) · Extended Detection and Response (XDR) · Managed Security Services Provider	· Indicators of Compromise (IoC) · Indicators of Exposure (IoE) · Security Incident Event Manager (SIEM) · Extended Detection and Response (XDR) · Managed Security Services Provider
CRY-01	· IT Asset Management (ITAM) program · Configuration Management (CM) program · Secure Baseline Configurations (SBC)	· IT Asset Management (ITAM) program · Configuration Management (CM) program · Secure Baseline Configurations (SBC)	· IT Asset Management (ITAM) program · Configuration Management (CM) program · Secure Baseline Configurations (SBC)	· IT Asset Management (ITAM) program · Configuration Management (CM) program · Secure Baseline Configurations (SBC)	· IT Asset Management (ITAM) program · Configuration Management (CM) program · Secure Baseline Configurations (SBC)
CRY-03	· NIST Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov) · Transport Layer Security (TLS) · IPSec encryption · Encrypted Multiprotocol Label Switching	· NIST Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov) · Transport Layer Security (TLS) · IPSec encryption · Encrypted Multiprotocol Label Switching	· NIST Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov) · Transport Layer Security (TLS) · IPSec encryption · Encrypted Multiprotocol Label Switching	· NIST Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov) · Transport Layer Security (TLS) · IPSec encryption · Encrypted Multiprotocol Label Switching	· NIST Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov) · Transport Layer Security (TLS) · IPSec encryption · Encrypted Multiprotocol Label Switching
CRY-05	· NIST Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov) · Microsoft BitLocker (https://microsoft.com)	· NIST Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov) · Microsoft BitLocker (https://microsoft.com)	· NIST Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov) · Microsoft BitLocker (https://microsoft.com)	· NIST Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov) · Microsoft BitLocker (https://microsoft.com)	· NIST Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov) · Microsoft BitLocker (https://microsoft.com)
CRY-09	· Cryptographic governance program	· Cryptographic governance program	· Cryptographic governance program	· Cryptographic governance program	· Cryptographic governance program
DCH-01	· Logical Access Control (LAC) · Physical Access Control (PAC)	· Logical Access Control (LAC) · Physical Access Control (PAC)	· Logical Access Control (LAC) · Physical Access Control (PAC) · Data governance program	· Logical Access Control (LAC) · Physical Access Control (PAC) · Data governance program · Chief Data Officer (CDO)	· Logical Access Control (LAC) · Physical Access Control (PAC) · Data governance program · Chief Data Officer (CDO)
DCH-01.2	· Logical Access Control (LAC) · Physical Access Control (PAC)	· Logical Access Control (LAC) · Physical Access Control (PAC)	· Logical Access Control (LAC) · Physical Access Control (PAC) · Data governance program	· Logical Access Control (LAC) · Physical Access Control (PAC) · Data governance program	· Logical Access Control (LAC) · Physical Access Control (PAC) · Data governance program
DCH-01.4	· Logical Access Control (LAC) · Physical Access Control (PAC)	· Logical Access Control (LAC) · Physical Access Control (PAC)	· Logical Access Control (LAC) · Physical Access Control (PAC) · Data governance program	· Logical Access Control (LAC) · Physical Access Control (PAC) · Data governance program	· Logical Access Control (LAC) · Physical Access Control (PAC) · Data governance program
DCH-02	· Data classification program · IT Asset Management (ITAM) program	· Data classification program · IT Asset Management (ITAM) program	· Data classification program · IT Asset Management (ITAM) program · Data governance program	· Data classification program · IT Asset Management (ITAM) program · Data governance program	· Data classification program · IT Asset Management (ITAM) program · Data governance program
DCH-08	· Shred-it (https://shredit.com) · IronMountain (https://ironmountain.com) · BitRaser (https://bitraser.com) · DBAN (https://dban.org) · DoD-strength data erasers	· Shred-it (https://shredit.com) · IronMountain (https://ironmountain.com) · BitRaser (https://bitraser.com) · DBAN (https://dban.org) · DoD-strength data erasers	· Shred-it (https://shredit.com) · IronMountain (https://ironmountain.com) · BitRaser (https://bitraser.com) · DBAN (https://dban.org) · DoD-strength data erasers	· Shred-it (https://shredit.com) · IronMountain (https://ironmountain.com) · BitRaser (https://bitraser.com) · DBAN (https://dban.org) · DoD-strength data erasers	· Shred-it (https://shredit.com) · IronMountain (https://ironmountain.com) · BitRaser (https://bitraser.com) · DBAN (https://dban.org) · DoD-strength data erasers
DCH-09	· Shred-it (https://shredit.com) · IronMountain (https://ironmountain.com) · BitRaser (https://bitraser.com) · DBAN (https://dban.org) · DoD-strength data erasers	· Shred-it (https://shredit.com) · IronMountain (https://ironmountain.com) · BitRaser (https://bitraser.com) · DBAN (https://dban.org) · DoD-strength data erasers	· Shred-it (https://shredit.com) · IronMountain (https://ironmountain.com) · BitRaser (https://bitraser.com) · DBAN (https://dban.org) · DoD-strength data erasers	· Shred-it (https://shredit.com) · IronMountain (https://ironmountain.com) · BitRaser (https://bitraser.com) · DBAN (https://dban.org) · DoD-strength data erasers	· Shred-it (https://shredit.com) · IronMountain (https://ironmountain.com) · BitRaser (https://bitraser.com) · DBAN (https://dban.org) · DoD-strength data erasers
DCH-13	· Secure Baseline Configurations (SBC) · Cybersecurity Supply Chain Risk Management (C-SCRM) program	· Secure Baseline Configurations (SBC) · Cybersecurity Supply Chain Risk Management (C-SCRM) program	· Secure Baseline Configurations (SBC) · Cybersecurity Supply Chain Risk Management (C-SCRM) program	· Secure Baseline Configurations (SBC) · Cybersecurity Supply Chain Risk Management (C-SCRM) program	· Secure Baseline Configurations (SBC) · Cybersecurity Supply Chain Risk Management (C-SCRM) program
DCH-13.1	· Cybersecurity Supply Chain Risk Management (C-SCRM) program	· Cybersecurity Supply Chain Risk Management (C-SCRM) program	· Cybersecurity Supply Chain Risk Management (C-SCRM) program	· Cybersecurity Supply Chain Risk Management (C-SCRM) program	· Cybersecurity Supply Chain Risk Management (C-SCRM) program
DCH-15					
DCH-17	· Data classification program · Secure Baseline Configurations (SBC) · Content / DNS filtering	· Data classification program · Secure Baseline Configurations (SBC) · Content / DNS filtering	· Data classification program · Secure Baseline Configurations (SBC) · Content / DNS filtering	· Data classification program · Secure Baseline Configurations (SBC) · Content / DNS filtering· Data governance program	· Data classification program · Secure Baseline Configurations (SBC) · Content / DNS filtering· Data governance program
END-01	· Secure Baseline Configurations (SBC) · IT Asset Management (ITAM) program · Configuration Management (CM) program · Change control program	· Secure Baseline Configurations (SBC) · IT Asset Management (ITAM) program · Configuration Management (CM) program · Change control program	· Secure Baseline Configurations (SBC) · IT Asset Management (ITAM) program · Configuration Management (CM) program · Change control program	· Secure Baseline Configurations (SBC) · IT Asset Management (ITAM) program · Configuration Management (CM) program · Change control program	· Secure Baseline Configurations (SBC) · IT Asset Management (ITAM) program · Configuration Management (CM) program · Change control program
END-04	· Antimalware software	· Antimalware software	· Antimalware software	· Antimalware software	· Antimalware software
END-04.1	· Secure Baseline Configurations (SBC)	· Secure Baseline Configurations (SBC)	· Secure Baseline Configurations (SBC)	· Secure Baseline Configurations (SBC)	· Secure Baseline Configurations (SBC)

Standard #	AICPA TSC 2017:2022 (used for SOC 2)	BSI Standard 200-1	CIS CSC v8.1	ISO 27001 v2022	ISO 27002 v2022	NIST 800-53 rev5	NIST 800-171 rev2	NIST 800-171 rev3	NIST CSF v2.0
CFG-02	CC6.1-POF7 CC6.7-POF1 CC7.1 CC7.1-POF1 CC8.1		4.1 4.2 4.3 4.4 4.5		8.3 8.5 8.9 8.12 8.25	AU-2 CM-2 CM-6 PL-10 SA-8	3.3.3 3.4.1 3.4.2	03.01.01.h 03.01.08.a 03.01.08.b 03.01.09 03.01.10.a	PR.DS-10 PR.PS PR.PS-05
CFG-03	CC5.2-POF3 CC6.1-POF7 CC6.7-POF1		4 4.6 4.8		8.3 8.9 8.12	CM-7	3.4.6	03.04.02.a 03.04.06.a 03.04.06.b 03.04.06.d 03.04.08.a	PR.PS-05
MON-01	CC7.2 CC7.2-POF1		8 8.2 13 13.6		8.15 8.16	AU-1 PM-31 SI-4	NFO-AU-1	03.03.01.a 03.12.03 03.14.06.a	DE.AE DE.CM-01 DE.CM-03 DE.CM-06 DE.CM-09
MON-01.8	CC7.2 CC7.2-POF4		8.1		8.16	AU-2	3.3.3 3.14.3	03.03.01.b 03.03.05.a	DE.AE DE.AE-06 DE.CM-01
MON-03	PI1.4		3.14 8.2 8.5		8.15	AU-2 AU-3	3.3.2	03.03.01.a 03.03.02.a 03.03.02.a.01 03.03.02.a.02 03.03.02.a.03	PR.PS-04
MON-16	CC7.2 CC7.2-POF2 CC7.2-POF3					AC-2(12) IR-4(13) SI-4(11)		03.01.01.e 03.03.05.a 03.14.06.a.01 03.14.06.a.02 03.14.06.b	DE.CM DE.CM-03
CRY-01	CC6.1 CC6.1-POF10 CC6.1-POF11 CC6.6-POF2 CC6.7-POF2		3.6 3.9 3.10 3.11		8.24 8.26	SC-8(1) SC-8(2) SC-13 SI-7(6)	3.13.11	03.13.08 03.13.11	PR.DS-01 PR.DS-02 PR.DS-10
CRY-03	CC6.1 CC6.1-POF10 CC6.7 CC6.7-POF2		3.10		5.14 8.24 8.26	SC-8 SC-8(1)	3.13.8	03.13.08	PR.DS-02
CRY-05	CC6.1 CC6.1-POF10 CC6.7 CC6.7-POF2 CC6.7-POF3		3.6 3.9 3.11		8.24	SC-13 SC-28 SC-28(1)	3.8.6	03.13.08	PR.DS-01
CRY-09	CC6.1 CC6.1-POF10 CC6.1-POF11				8.24	SC-28(3)	3.13.10	03.13.10	
DCH-01	A1.2-POF7 C1.1 C1.1-POF2 CC2.1 CC6.5		3 3.1 3.3 11 11.3		5.9 5.10 5.12 5.33 7.10	MP-1	3.8.1 3.8.3 NFO-MP-1	03.01.01.d.01 03.01.01.d.02 03.08.01	ID.AM-08 PR.DS PR.DS-01 PR.DS-02 PR.DS-10
DCH-01.2	A1.2-POF7 C1.1-POF2 CC8.1-POF17		3.1					03.01.01.d.01 03.01.01.d.02 03.01.02 03.01.20.a 03.01.20.b	PR.DS
DCH-01.4			3.1 3.3					03.01.02 03.01.03 03.01.04.b 03.08.01 03.08.02	PR.DS
DCH-02	C1.1 CC2.1 CC2.1-POF7 CC6.1-POF1		3.1 3.7		5.9 5.12			03.04.11.a 03.08.01 03.08.04	ID.AM-05 PR.DS
DCH-08	C1.2-POF2 CC6.5 CC6.5-POF2 P4.3-POF2 P4.3-POF3		3.1 3.5		7.10 8.10	MP-6	3.8.3	03.08.03	
DCH-09	C1.2-POF2 CC6.5 CC6.5-POF2		3.1 3.5		8.10	MP-6 MP-6(3)	3.7.3 3.8.3	03.07.04.c 03.08.03	
DCH-13	CC6.7					AC-20	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	
DCH-13.1			3.3			AC-20(1)	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	
DCH-15						AC-22	3.1.22	03.01.22.a 03.01.22.b	
DCH-17	CC6.7 CC6.7-POF1				5.14		3.1.20	03.01.20.a	
END-01	CC6.7-POF4		10		7.7 8.1 8.5	MP-2	3.14.2	03.14.02.a	DE.CM-09
END-04	CC6.8 CC6.8-POF4		10 10.1 10.4		8.7	SI-3	3.14.2	03.14.02.c 03.14.02.c.01 03.14.02.c.02	DE.CM-09
END-04.1			10.2		8.7	SI-2 SI-3	3.14.4	03.14.02.b	

Policy Domain	Standard #	Standard Name	SCF CORE Fundamentals	US CMMC 2.0 Level 1	US FAR 52.204-21	US FAR 52.204-27	US FAR Section 889	Control Question	Possible Solutions & Considerations Micro-Small Business (<10 staff) BLS Firm Size Classes 1-2	Possible Solutions & Considerations Small Business (10-49 staff) BLS Firm Size Classes 3-4	Possible Solutions & Considerations Medium Business (50-249 staff) BLS Firm Size Classes 5-6	Possible Solutions & Considerations Large Business (250-999 staff) BLS Firm Size Classes 7-8	Possible Solutions & Considerations Enterprise (> 1,000 staff) BLS Firm Size Class 9	AICPA TSC 2017:2022 (used for SOC 2)	BSI Standard 200-1	CIS CSC v8.1	ISO 27001 v2022	ISO 27002 v2022	NIST 800-53 rev5	NIST 800-171 rev2	NIST 800-171 rev3	NIST CSF v2.0
Endpoint Security	END-04.7	Always On Protection		SI.L1-3.14.5	52.204-21(b)(1)(xv)			Does the organization ensure that anti-malware technologies are continuously running in real-time and cannot be disabled or altered by non-privileged users, unless specifically authorized by management on a case-by-case basis for a limited time period?	· Antimalware software	· Antimalware software	· Antimalware software	· Antimalware software	· Antimalware software	CC6.8-POF5		10.4				3.14.5	03.14.02.a 03.14.02.c.01 03.14.02.c.02	
Endpoint Security	END-08	Phishing & Spam Protection	END-08					Does the organization utilize anti-phishing and spam protection technologies to detect and take action on unsolicited messages transported by electronic mail?	· Anti-spam / phishing solution	· Anti-spam / phishing solution	· Anti-spam / phishing solution	· Anti-spam / phishing solution	· Anti-spam / phishing solution			9 9.6 9.7			SI-8			
Human Resources Security	HRS-01	Human Resources Security Management		AC.L1-3.1.22	52.204-21(b)(1)(iv)			Does the organization facilitate the implementation of personnel security controls?						CC1.1 CC1.1-POF1 CC1.1-POF3 CC1.2-POF1 CC1.2-POF2	6		7.3 7.3(a) 7.3(b) 7.3(c) 7.2(d)	5.4	PS-1	3.1.22 NFO-PS-1	03.01.01.g.02 03.15.03.a 03.15.03.d	GV.RR-04 ID.AM
Human Resources Security	HRS-04	Personnel Screening	HRS-04					Does the organization manage personnel security risk by screening individuals prior to authorizing access?	· Criminal, education and employment background checks · Professional references · Education / certification transcripts	· Criminal, education and employment background checks · Professional references · Education / certification transcripts	· Criminal, education and employment background checks · Professional references · Education / certification transcripts	· Criminal, education and employment background checks · Professional references · Education / certification transcripts	· Criminal, education and employment background checks · Professional references · Education / certification transcripts	CC1.4-POF5			7.2(b) 7.2(c)	6.1	PS-3	3.9.1	03.09.01.a 03.09.01.b	
Human Resources Security	HRS-05	Terms of Employment	HRS-05	AC.L1-3.1.22	52.204-21(b)(1)(iv)			Does the organization require all employees and contractors to apply cybersecurity and data protection principles in their daily work?	· Formal onboarding training · Acceptable Use / Rules of Behavior (RoB)	· Formal onboarding training · Acceptable Use / Rules of Behavior (RoB)	· Formal onboarding training · Acceptable Use / Rules of Behavior (RoB)	· Formal onboarding training · Acceptable Use / Rules of Behavior (RoB)	· Formal onboarding training · Acceptable Use / Rules of Behavior (RoB)				7.3 7.3(a) 7.3(b) 7.3(c)	5.4 5.14 6.2	PL-4	3.1.22 NFO-PL-4	03.01.01.h 03.01.22.a 03.15.03.a	ID.AM
Human Resources Security	HRS-05.1	Rules of Behavior		AC.L1-3.1.22	52.204-21(b)(1)(iv)			Does the organization define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior?	· Formal onboarding training · Acceptable Use / Rules of Behavior (RoB)	· Formal onboarding training · Acceptable Use / Rules of Behavior (RoB)	· Formal onboarding training · Acceptable Use / Rules of Behavior (RoB)	· Formal onboarding training · Acceptable Use / Rules of Behavior (RoB)	· Formal onboarding training · Acceptable Use / Rules of Behavior (RoB)	CC1.1		9.4	7.3 7.3(a) 7.3(b) 7.3(c)	5.4 5.10 5.14 6.2	PL-4	3.1.22 NFO-PL-4	03.01.12.a 03.01.18.a 03.01.22.a 03.15.03.a 03.15.03.d	ID.AM
Human Resources Security	HRS-05.2	Social Media & Social Networking Restrictions		AC.L1-3.1.22	52.204-21(b)(1)(iv)			Does the organization define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information?	· Formal onboarding training · Acceptable Use / Rules of Behavior (RoB)	· Formal onboarding training · Acceptable Use / Rules of Behavior (RoB)	· Formal onboarding training · Acceptable Use / Rules of Behavior (RoB)	· Formal onboarding training · Acceptable Use / Rules of Behavior (RoB)	· Formal onboarding training · Acceptable Use / Rules of Behavior (RoB)	CC1.1 CC1.1-POF2		9	7.3 7.3(a) 7.3(b) 7.3(c)	5.4 5.10 6.2	PL-4(1)	3.1.22 NFO-PL-4(1)	03.15.03.a	
Identification & Authentication	IAC-01	Identity & Access Management (IAM)		AC.L1-3.1.1	52.204-21(b)(1)(i)			Does the organization facilitate the implementation of identification and access management controls?			· Identity & Access Management (IAM) program	· Identity & Access Management (IAM) program	· Identity & Access Management (IAM) program	CC6.1 CC6.1-POF3 CC6.1-POF7 CC6.1-POF8 CC6.1-POF9		4.7 5 5.6 6 6.6		5.15 5.18	AC-1 IA-1	3.1.1 NFO-AC-1 NFO-IA-1	03.01.01.a 03.01.18.b 03.05.01.a 03.05.05.a 03.05.12.e	PR.AA PR.AA-05
Identification & Authentication	IAC-01.3	User & Service Account Inventories	IAC-01.3					Does the organization maintain a current list of authorized users and service accounts?	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)									
Identification & Authentication	IAC-02	Identification & Authentication for Organizational Users		AC.L1-3.1.1 IA.L1-3.5.1 IA.L1-3.5.2	52.204-21(b)(1)(i) 52.204-21(b)(1)(v) 52.204-21(b)(1)(vi)			Does the organization uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users?	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)	CC6.1 CC6.1-POF3 CC6.1-POF4 CC6.1-POF8		5.5 5.6 6.7 12.5		5.15	IA-2	3.1.1 3.5.1 3.5.2	03.05.01.a 03.05.05.d	PR.AA-01 PR.AA-03 PR.AA-05
Identification & Authentication	IAC-04	Identification & Authentication for Devices		IA.L1-3.5.1 IA.L1-3.5.2	52.204-21(b)(1)(v) 52.204-21(b)(1)(vi)			Does the organization uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically- based and replay resistant?	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)	CC6.1 CC6.1-POF3 CC6.1-POF8		12.5		5.16	IA-3 IA-3(1) IA-3(4)	3.5.1 3.5.2	03.01.18.b 03.05.02	PR.AA-01 PR.AA-03 PR.AA-05
Identification & Authentication	IAC-06	Multi-Factor Authentication (MFA)	IAC-06					Does the organization use automated mechanisms to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com) · Yubico (https://yubico.com)	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com) · Yubico (https://yubico.com)	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com) · Yubico (https://yubico.com)	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com) · Yubico (https://yubico.com)	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com) · Yubico (https://yubico.com)	CC6.6-POF3		6.3 6.4			IA-2(1) IA-2(2)	3.5.3	03.05.03 03.07.05.b	
Identification & Authentication	IAC-07	User Provisioning & De-Provisioning	IAC-07					Does the organization utilize a formal user registration and de-registration process that governs the assignment of access rights?						CC6.2 CC6.2-POF1 CC6.2-POF3 CC6.3-POF1 CC6.3-POF2		6.1 6.2		5.16 5.18	IA-12(4)		03.01.01.g.01 03.01.01.g.02 03.01.01.g.03 03.05.05.a 03.09.02.a.01	
Identification & Authentication	IAC-08	Role-Based Access Control (RBAC)	IAC-08	AC.L1-3.1.1 AC.L1-3.1.2	52.204-21(b)(1)(i) 52.204-21(b)(1)(ii)			Does the organization enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs?	· Role-Based Access Control (RBAC)	· Role-Based Access Control (RBAC)	· Role-Based Access Control (RBAC)	· Role-Based Access Control (RBAC)	· Role-Based Access Control (RBAC)	CC5.2-POF3 CC6.1 CC6.1-POF12 CC6.1-POF13 CC6.3		3.3 6 6.8		5.15 8.3	AC-2(7)	3.1.1 3.1.2 3.1.3	03.01.01.c.01 03.01.01.c.02 03.01.01.c.03 03.01.02 03.01.05.b	PR.AA-05
Identification & Authentication	IAC-10	Authenticator Management	IAC-10					Does the organization: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed?	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)	CC6.1		5.2		5.17 5.18	IA-5 IA-5(1)	3.5.8 3.5.9	03.05.07.a 03.05.07.b 03.05.07.c 03.05.07.d 03.05.07.e	
Identification & Authentication	IAC-10.8	Default Authenticators	IAC-10.8					Does the organization ensure default authenticators are changed as part of account creation or system installation?	· Secure Baseline Configurations (SBC)	· Secure Baseline Configurations (SBC)	· Secure Baseline Configurations (SBC) · Identity & Access Management (IAM) program	· Secure Baseline Configurations (SBC) · Identity & Access Management (IAM) program	· Secure Baseline Configurations (SBC) · Identity & Access Management (IAM) program	CC6.1		4.7		5.17	IA-5 IA-5(5)		03.05.07.e 03.05.12.d	
Identification & Authentication	IAC-15	Account Management	IAC-15	AC.L1-3.1.2	52.204-21(b)(1)(ii)			Does the organization proactively govern account management of individual, group, system, service, application, guest and temporary accounts?	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)	CC6.1				5.15 5.16 5.18	AC-2	3.1.2	03.01.01.a 03.01.01.b 03.01.01.c.01 03.01.01.c.02 03.01.01.d.01	
Identification & Authentication	IAC-15.1	Automated System Account Management (Directory Services)		AC.L1-3.1.1 IA.L1-3.5.1 IA.L1-3.5.2	52.204-21(b)(1)(i) 52.204-21(b)(1)(v) 52.204-21(b)(1)(vi)			Does the organization use automated mechanisms to support the management of system accounts?	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)			5 5.6 6		5.18	AC-2(1)	3.1.1 3.5.1 3.5.2	03.05.05.b 03.05.05.c 03.05.05.d 03.05.07.c 03.05.07.d	
Identification & Authentication	IAC-16	Privileged Account Management (PAM)	IAC-16					Does the organization restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS)?			· ManageEngine Enterprise Password Management (https://manageengine.com) · Securden (https://securden.com) · CyberArk (https://cyberark.com)	· ManageEngine Enterprise Password Management (https://manageengine.com) · Securden (https://securden.com) · CyberArk (https://cyberark.com)	· ManageEngine Enterprise Password Management (https://manageengine.com) · Securden (https://securden.com) · CyberArk (https://cyberark.com)	CC6.1		2.7 5.1 5.4		5.15 5.18 8.2		3.1.5	03.01.06.a 03.01.07.a 03.01.07.b	
Identification & Authentication	IAC-17	Periodic Review of Account Privileges	IAC-17					Does the organization periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary?						CC6.2 CC6.2-POF2 CC6.2-POF3 CC6.3-POF4				5.15 5.18 8.2	AC-6(7)		03.01.01.g.03 03.01.05.c 03.01.05.d 03.10.01.c 03.10.01.d	
Identification & Authentication	IAC-20	Access Enforcement		AC.L1-3.1.1	52.204-21(b)(1)(i)			Does the organization enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege?"	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)	· Microsoft Active Directory (https://microsoft.com) · Microsoft Entra (https://microsoft.com) · AWS IAM (https://aws.amazon.com)	CC6.1				5.18	AC-3 AC-6	3.1.1	03.01.01.c.03 03.01.01.d.01 03.01.01.d.02 03.01.02 03.01.03	
Identification & Authentication	IAC-21	Least Privilege	IAC-21					Does the organization utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions?	· Role Based Access Control (RBAC)	· Role Based Access Control (RBAC)	· Role Based Access Control (RBAC)	· Role Based Access Control (RBAC)	· Role Based Access Control (RBAC)	CC5.2-POF3 CC6.1 CC6.1-POF12 CC6.1-POF13 CC6.1-POF7		5.4		5.15 5.18 8.3 8.12	AC-6 SA-8(14)	3.1.5	03.01.01.c.03 03.01.01.d.01 03.01.01.d.02 03.01.04.b 03.01.05.a	PR.AA-05 PR.DS-10
Incident Response	IRO-01	Incident Response Operations						Does the organization implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents?	· Incident Response Plan (IRP)	· Incident Response Plan (IRP)	· Integrated Incident Response Program (IIRP)	· Integrated Incident Response Program (IIRP)	· Integrated Incident Response Program (IIRP)	A1.2-POF5 CC2.2-POF10 CC2.2-POF3 CC7.3 CC7.3-POF1		17 17.5		5.24	IR-1	NFO-IR-1	03.06.01	DE.AE GV.SC-08 RS RS.MI

Policy Domain	Standard #	Standard Name	SCF CORE Fundamentals	US CMMC 2.0 Level 1	US FAR 52.204-21	US FAR 52.204-27	US FAR Section 889	Control Question	Possible Solutions & Considerations Micro-Small Business (<10 staff) BLS Firm Size Classes 1-2	Possible Solutions & Considerations Small Business (10-49 staff) BLS Firm Size Classes 3-4	Possible Solutions & Considerations Medium Business (50-249 staff) BLS Firm Size Classes 5-6	Possible Solutions & Considerations Large Business (250-999 staff) BLS Firm Size Classes 7-8	Possible Solutions & Considerations Enterprise (> 1,000 staff) BLS Firm Size Class 9	AICPA TSC 2017:2022 (used for SOC 2)	BSI Standard 200-1	CIS CSC v8.1	ISO 27001 v2022	ISO 27002 v2022	NIST 800-53 rev5	NIST 800-171 rev2	NIST 800-171 rev3	NIST CSF v2.0
Incident Response	IRO-02	Incident Handling	IRO-02					Does the organization cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis;	· Incident Response Plan (IRP)	· Incident Response Plan (IRP)	· Integrated Incident Response Program (IIRP) · ITIL 4 (https://axelos.com) · Incident and problem management	· Integrated Incident Response Program (IIRP) · ITIL 4 (https://axelos.com) · Incident and problem management	· Integrated Incident Response Program (IIRP) · ITIL 4 (https://axelos.com) · Incident and problem management	A1.2-POF5 CC2.2-POF10 CC2.2-POF3 CC2.2-POF6 CC2.3-POF8 CC7.3		2.3 17 17.1 17.3 17.4 17.5		5.24 5.25 5.26 6.8	IR-4	3.6.1 3.6.2	03.03.04.b 03.06.01 03.06.02.a 03.06.02.b 03.06.02.c 03.06.02.d	DE.AE DE.AE-02 DE.AE-03 DE.AE-04 DE.AE-06 DE.AE-08
Incident Response	IRO-04	Incident Response Plan (IRP)	IRO-04					Does the organization maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders?	· Incident Response Plan (IRP)	· Incident Response Plan (IRP)	· Integrated Incident Response Program (IIRP)	· Integrated Incident Response Program (IIRP)	· Integrated Incident Response Program (IIRP)	CC2.2-POF10 CC2.3-POF8 CC7.3 CC7.3-POF1 CC7.4 CC7.4-POF1		17.1 17.4 17.5 17.6 17.9		5.24 5.26	IR-8	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	DE.AE-08 ID.IM-04 RS RS.MA RS.MA-01 RS.MA-02
Maintenance	MNT-01	Maintenance Operations						Does the organization develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise?	· IT maintenance program	· IT maintenance program	· IT maintenance program	· IT maintenance program	· IT maintenance program					7.13	MA-1	NFO-MA-1	03.04.03.c 03.07.04.a 03.07.06.a	PR.PS PR.PS-02 PR.PS-03
Network Security	NET-01	Network Security Controls (NSC)		SC.L1-3.13.1	52.204-21(b)(1)(x)			Does the organization develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC)?						CC6.1 CC6.1-POF5 CC6.6 CC6.6-POF1 CC6.6-POF2 CC6.6-POF3		12 12.1 12.2 12.3 12.6		5.14 8.12 8.20 8.21	SC-1	3.13.1 NFO-SC-1	03.01.12.a 03.01.16.a 03.01.16.b 03.01.18.a 03.13.01.a	PR.IR-01
Network Security	NET-02	Layered Network Defenses	NET-02					Does the organization implement security functions as a layered structure that minimizes interactions between layers of the design and avoids any dependence by lower layers on the functionality or correctness of higher layers?						CC6.6 CC6.6-POF4		12.2		8.20			03.13.01.b	PR.IR-01
Network Security	NET-02.2	Guest Networks	NET-02.2	SC.L1-3.13.1	52.204-21(b)(1)(x)			Does the organization implement and manage a secure guest network?												3.13.1	03.01.16.a 03.01.16.b	
Network Security	NET-03	Boundary Protection	NET-03	SC.L1-3.13.1	52.204-21(b)(1)(x)			Does the organization monitor and control communications at the external network boundary and at key internal boundaries within the network?						CC6.1 CC6.1-POF5 CC6.6 CC6.6-POF1 CC6.6-POF3 CC6.6-POF4		13.5 9.6		8.20 8.21	SC-7 SC-7(9) SC-7(11)	3.13.1	03.01.12.a 03.13.01.a 03.13.01.b 03.13.01.c	
Network Security	NET-04	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04					Does the organization implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized?	· Access Control Lists (ACLs)	· Access Control Lists (ACLs)	· Access Control Lists (ACLs)	· Access Control Lists (ACLs)	· Access Control Lists (ACLs)	CC6.1 CC6.1-POF6 CC6.6 CC6.6-POF1		3.3 4.6 12.6 13.4		5.14 8.3 8.20	AC-4	3.1.3	03.01.03 03.13.01.a 03.13.01.c	
Network Security	NET-06	Network Segmentation (macrosegementation)		SC.L1-3.13.5	52.204-21(b)(1)(xi)			Does the organization ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources?	· Subnetting · Virtual Local Area Network (VLAN)	· Subnetting · Virtual Local Area Network (VLAN)	· Subnetting · Virtual Local Area Network (VLAN)	· Subnetting · Virtual Local Area Network (VLAN)	· Subnetting · Virtual Local Area Network (VLAN)	CC6.1				8.20 8.22	AC-4(21)	3.13.5	03.13.01.b	
Network Security	NET-14	Remote Access	NET-14					Does the organization define, control and review organization-approved, secure remote access methods?						CC6.6 CC6.6-POF3		12.7		6.7	AC-17 AC-17(6)	3.1.12	03.01.12.a 03.01.12.b 03.01.12.c 03.01.12.d	
Network Security	NET-14.5	Work From Anywhere (WFA) - Telecommuting Security	NET-14.5					Does the organization define secure telecommuting practices and govern remote access to Technology Assets, Applications, Services and/or Data (TAASD) for remote workers?										6.7 7.9		3.1.12 3.10.6	03.01.12.a 03.01.12.c 03.10.06.a 03.10.06.b	
Network Security	NET-15	Wireless Networking	NET-15					Does the organization control authorized wireless usage and monitor for unauthorized wireless access?	· Secure Baseline Configurations (SBC)	· Secure Baseline Configurations (SBC)	· Secure Baseline Configurations (SBC)	· Secure Baseline Configurations (SBC)	· Secure Baseline Configurations (SBC)					8.21	AC-18	3.1.16	03.01.16.a 03.01.16.b	
Network Security	NET-18	DNS & Content Filtering	NET-18					Does the organization force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites?	· Secure Baseline Configurations (SBC)	· Secure Baseline Configurations (SBC)	· Secure Baseline Configurations (SBC)	· Secure Baseline Configurations (SBC)	· Secure Baseline Configurations (SBC)			9 9.2 9.3 13.10		5.14 8.23	SC-7(8) SC-18(3)	3.1.3	03.14.06.c	DE.CM-03
Physical & Environmental Security	PES-01	Physical & Environmental Protections						Does the organization facilitate the operation of physical and environmental protection controls?						A1.2 A1.2-POF1 A1.2-POF2 A1.2-POF3 A1.2-POF4 A1.2-POF5				5.14 5.15 5.18 7.1 7.5	PE-1 PE-23	3.10.2 NFO-PE-1	03.08.01 03.08.02 03.10.01.a 03.10.07.a	DE.CM-02 ID.AM PR.AA PR.AA-06 PR.IR-02
Physical & Environmental Security	PES-02	Physical Access Authorizations	PES-02	PE.L1-3.10.1	52.204-21(b)(1)(viii)			Does the organization maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible)?						CC6.4 CC6.4-POF1 CC6.4-POF2				5.15 5.18 7.1	PE-2	3.10.1	03.08.01 03.08.02 03.10.01.a 03.10.01.b 03.10.01.c 03.10.01.d	PR.AA PR.AA-06
Physical & Environmental Security	PES-02.1	Role-Based Physical Access		PE.L1-3.10.1	52.204-21(b)(1)(viii)			Does the organization authorize physical access to facilities based on the position or role of the individual?						CC6.4 CC6.4-POF1 CC6.4-POF2				5.15 5.18	PE-2(1)	3.10.1	03.08.01 03.08.02 03.10.01.b 03.10.01.d	PR.AA-06
Physical & Environmental Security	PES-03	Physical Access Control	PES-03	PE.L1-3.10.3 PE.L1-3.10.5	52.204-21(b)(1)(viii) 52.204-21(b)(1)(ix)			Does the organization enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible)?			· Staffed lobby (receptionist) · Physical security guards · Verify individual access authorizations before granting access to the facility. · Control entry to the facility containing the	· Staffed lobby (receptionist) · Physical security guards · Verify individual access authorizations before granting access to the facility. · Control entry to the facility containing the	· Staffed lobby (receptionist) · Physical security guards · Verify individual access authorizations before granting access to the facility. · Control entry to the facility containing the	CC6.4 CC6.4-POF1 CC6.4-POF2				5.15 5.18 7.1 7.4	PE-3 PE-3(2) PE-3(3)	3.10.3 3.10.5	03.10.02.a 03.10.07.a 03.10.07.a.01 03.10.07.a.02 03.10.07.d	DE.CM-02 PR.AA PR.AA-06
Physical & Environmental Security	PES-03.3	Physical Access Logs		PE.L1-3.10.4	52.204-21(b)(1)(viii)			Does the organization generate a log entry for each access attempt through controlled ingress and egress points?	· Visitor logbook · iLobby (https://golobby.com) · The Receptionist (https://thereceptionist.com) · LobbyGuard (http://lobbyguard.com)	· Visitor logbook · iLobby (https://golobby.com) · The Receptionist (https://thereceptionist.com) · LobbyGuard (http://lobbyguard.com)	· Visitor logbook · iLobby (https://golobby.com) · The Receptionist (https://thereceptionist.com) · LobbyGuard (http://lobbyguard.com)	· Staffed lobby (receptionist) · Visitor logbook	· Staffed lobby (receptionist) · Visitor logbook	CC6.4-POF4				7.2	PE-8	3.10.4 NFO-PE-8	03.10.02.a 03.10.07.b	DE.CM-02
Physical & Environmental Security	PES-03.4	Access To Critical Systems		PE.L1-3.10.1	52.204-21(b)(1)(viii)			Does the organization enforce physical access to critical systems or sensitive/regulated data, in addition to the physical access controls for the facility?											PE-3(1)	3.10.1	03.10.07.a.01 03.10.07.a.02	
Physical & Environmental Security	PES-06	Visitor Control	PES-06	PE.L1-3.10.3	52.204-21(b)(1)(ix)			Does the organization identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible)?	· Visitor logbook · iLobby (https://golobby.com) · The Receptionist (https://thereceptionist.com) · LobbyGuard (http://lobbyguard.com)	· Visitor logbook · iLobby (https://golobby.com) · The Receptionist (https://thereceptionist.com) · LobbyGuard (http://lobbyguard.com)	· Visitor logbook · iLobby (https://golobby.com) · The Receptionist (https://thereceptionist.com) · LobbyGuard (http://lobbyguard.com)	· Staffed lobby (receptionist) · Visitor logbook	· Staffed lobby (receptionist) · Visitor logbook					7.2		3.10.3	03.10.02.b 03.10.07.c	
Physical & Environmental Security	PES-06.1	Distinguish Visitors from On-Site Personnel		PE.L1-3.10.3	52.204-21(b)(1)(ix)			Does the organization easily distinguish between onsite personnel and visitors, especially in areas where sensitive/regulated data is accessible?	· Visible badges for visitors that are different from organizational personnel	· Visible badges for visitors that are different from organizational personnel	· Visible badges for visitors that are different from organizational personnel	· Visible badges for visitors that are different from organizational personnel	· Visible badges for visitors that are different from organizational personnel							3.10.3	03.10.02.b 03.10.07.c	
Physical & Environmental Security	PES-06.3	Restrict Unescorted Access		PE.L1-3.10.3	52.204-21(b)(1)(ix)			Does the organization restrict unescorted access to facilities to personnel with required security clearances, formal access authorizations and validate the need for access?											PE-2(3)	3.10.3	03.10.07.c	
Physical & Environmental Security	PES-12	Equipment Siting & Protection		PE.L1-3.10.1	52.204-21(b)(1)(viii)			Does the organization locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access?						A1.2				7.3 7.5 7.8 7.12	PE-18 PE-23 SC-7(14)	3.10.1	03.10.07.e 03.10.08	

Policy Domain	Standard #	Standard Name	SCF CORE Fundamentals	US CMMC 2.0 Level 1	US FAR 52.204-21	US FAR 52.204-27	US FAR Section 889	Control Question
Physical & Environmental Security	PES-12.1	Transmission Medium Security		PE.L1-3.10.1	52.204-21(b)(1)(viii)			Does the organization protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage?
Physical & Environmental Security	PES-12.2	Access Control for Output Devices		PE.L1-3.10.1	52.204-21(b)(1)(viii)			Does the organization restrict access to printers and other system output devices to prevent unauthorized individuals from obtaining the output?
Data Privacy	PRI-01	Data Privacy Program						Does the organization facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently?
Project & Resource Management	PRM-01	Cybersecurity & Data Protection Portfolio Management						Does the organization facilitate the implementation of cybersecurity and data protection-related resource planning controls that define a viable plan for achieving cybersecurity and data protection objectives?
Risk Management	RSK-01	Risk Management Program						Does the organization facilitate the implementation of strategic, operational and tactical risk management controls?
Risk Management	RSK-03	Risk Identification	RSK-03					Does the organization identify and document risks, both internal and external?
Risk Management	RSK-04	Risk Assessment	RSK-04					Does the organization conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of its Technology Assets, Applications, Services and/or Data (TAASD)?
Risk Management	RSK-04.1	Risk Register	RSK-04.1					Does the organization maintain a risk register that facilitates monitoring and reporting of risks?
Risk Management	RSK-06	Risk Remediation	RSK-06					Does the organization remediate risks to an acceptable level?
Security Awareness & Training	SAT-01	Cybersecurity & Data Protection-Minded Workforce						Does the organization facilitate the implementation of security workforce development and awareness controls?
Security Awareness & Training	SAT-02	Cybersecurity & Data Protection Awareness Training	SAT-02					Does the organization provide all employees and contractors appropriate awareness education and training that is relevant for their job function?
Third-Party Management	TPM-01	Third-Party Management		AC.L1-3.1.1	52.204-21(b)(1)(i)	52.204-27(b)		Does the organization facilitate the implementation of third-party management controls?
Third-Party Management	TPM-01.1	Third-Party Inventories	TPM-01.1					Does the organization maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of its Technology Assets, Applications, Services and/or Data (TAASD)?
Third-Party Management	TPM-03	Supply Chain Risk Management (SCRM)	TPM-03					Does the organization: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the
Third-Party Management	TPM-05	Third-Party Contract Requirements	TPM-05	AC.L1-3.1.1	52.204-21(b)(1)(i)	52.204-27(b)		Does the organization require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting its needs to protect its Technology Assets, Applications, Services and/or Data (TAASD)?
Third-Party Management	TPM-05.2	Contract Flow-Down Requirements		AC.L1-3.1.1	52.204-21(b)(1)(i)	52.204-27(b)		Does the organization ensure cybersecurity and data protection requirements are included in contracts that flow-down to applicable sub-contractors and suppliers?
Third-Party Management	TPM-05.4	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4					Does the organization document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and data protection controls between internal stakeholders and
Third-Party Management	TPM-08	Review of Third-Party Services	TPM-08					Does the organization monitor, regularly review and audit External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity and data protection controls?
Vulnerability & Patch Management	VPM-01	Vulnerability & Patch Management Program (VPMP)		SI.L1-3.14.1	52.204-21(b)(1)(xii)			Does the organization facilitate the implementation and monitoring of vulnerability management controls?
Vulnerability & Patch Management	VPM-02	Vulnerability Remediation Process	VPM-02	SI.L1-3.14.1	52.204-21(b)(1)(xii)			Does the organization ensure that vulnerabilities are properly identified, tracked and remediated?
Vulnerability & Patch Management	VPM-05	Software & Firmware Patching	VPM-05	SI.L1-3.14.1	52.204-21(b)(1)(xii)			Does the organization conduct software patching for all deployed systems, applications and firmware?
Vulnerability & Patch Management	VPM-06	Vulnerability Scanning	VPM-06					Does the organization detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications?
Web Security	WEB-01	Web Security		AC.L1-3.1.22	52.204-21(b)(1)(iv)			Does the organization facilitate the implementation of an enterprise-wide web management policy, as well as associated standards, controls and procedures?

Standard #	Possible Solutions & Considerations Micro-Small Business (<10 staff) BLS Firm Size Classes 1-2	Possible Solutions & Considerations Small Business (10-49 staff) BLS Firm Size Classes 3-4	Possible Solutions & Considerations Medium Business (50-249 staff) BLS Firm Size Classes 5-6	Possible Solutions & Considerations Large Business (250-999 staff) BLS Firm Size Classes 7-8	Possible Solutions & Considerations Enterprise (> 1,000 staff) BLS Firm Size Class 9
PES-12.1					
PES-12.2			· Printer management (print only when at the printer with proximity card or code)	· Printer management (print only when at the printer with proximity card or code)	· Printer management (print only when at the printer with proximity card or code)
PRI-01	· Data privacy program	· Data privacy program	· Data privacy program	· Data privacy program	· Data privacy program
PRM-01					
RSK-01	· Risk Management Program (RMP)	· Risk Management Program (RMP)	· Risk Management Program (RMP)	· Risk Management Program (RMP)	· Risk Management Program (RMP)
RSK-03	· Risk Management Program (RMP)	· Risk Management Program (RMP)	· Risk Management Program (RMP)	· Risk Management Program (RMP)	· Risk Management Program (RMP)
RSK-04	· Risk Management Program (RMP) · Risk assessment · Business Impact Analysis (BIA) · Data Protection Impact Assessment (DPIA)	· Risk Management Program (RMP) · Risk assessment · Business Impact Analysis (BIA) · Data Protection Impact Assessment (DPIA)	· Risk Management Program (RMP) · Risk assessment · Business Impact Analysis (BIA) · Data Protection Impact Assessment (DPIA)	· Risk Management Program (RMP) · Risk assessment · Business Impact Analysis (BIA) · Data Protection Impact Assessment (DPIA)	· Risk Management Program (RMP) · Risk assessment · Business Impact Analysis (BIA) · Data Protection Impact Assessment (DPIA)
RSK-04.1	· Risk Management Program (RMP) · Risk register · Plan of Action & Milestones (POA&M)	· Risk Management Program (RMP) · Risk register · Plan of Action & Milestones (POA&M)	· Risk Management Program (RMP) · Risk register · Plan of Action & Milestones (POA&M)	· Risk Management Program (RMP) · Risk register · Plan of Action & Milestones (POA&M)	· Risk Management Program (RMP) · Risk register · Plan of Action & Milestones (POA&M)
RSK-06	· Risk Management Program (RMP) · Risk register · Plan of Action & Milestones (POA&M)	· Risk Management Program (RMP) · Risk register · Plan of Action & Milestones (POA&M)	· Risk Management Program (RMP) · Risk register · Plan of Action & Milestones (POA&M)	· Risk Management Program (RMP) · Risk register · Plan of Action & Milestones (POA&M)	· Risk Management Program (RMP) · Risk register · Plan of Action & Milestones (POA&M)
SAT-01	· Third-party advisors (e.g., virtual CISO, Managed Security Services Provider (MSSP), etc.)	· Third-party advisors (e.g., virtual CISO, Managed Security Services Provider (MSSP), etc.)	· Chief Information Security Officer (CISO)	· Chief Information Security Officer (CISO)	· Chief Information Security Officer (CISO)
SAT-02	· Initial & annual cybersecurity and data privacy awareness training · KnowB4 (https://knowbe4.com)	· Initial & annual cybersecurity and data privacy awareness training · KnowB4 (https://knowbe4.com)	· Initial & annual cybersecurity and data privacy awareness training · KnowB4 (https://knowbe4.com)	· Initial & annual cybersecurity and data privacy awareness training · KnowB4 (https://knowbe4.com)	· Initial & annual cybersecurity and data privacy awareness training · KnowB4 (https://knowbe4.com)
TPM-01	· Cybersecurity Supply Chain Risk Management (C-SCRM) program · Product / project management	· Cybersecurity Supply Chain Risk Management (C-SCRM) program · Product / project management	· Cybersecurity Supply Chain Risk Management (C-SCRM) program · Product / project management	· Cybersecurity Supply Chain Risk Management (C-SCRM) program · Product / project management	· Cybersecurity Supply Chain Risk Management (C-SCRM) program · Product / project management
TPM-01.1	· Cybersecurity Supply Chain Risk Management (C-SCRM) program	· Cybersecurity Supply Chain Risk Management (C-SCRM) program	· Cybersecurity Supply Chain Risk Management (C-SCRM) program	· Cybersecurity Supply Chain Risk Management (C-SCRM) program	· Cybersecurity Supply Chain Risk Management (C-SCRM) program
TPM-03	· Cybersecurity Supply Chain Risk Management (C-SCRM) program · Data Protection Impact Assessment (DPIA)	· Cybersecurity Supply Chain Risk Management (C-SCRM) program · Data Protection Impact Assessment (DPIA)	· Cybersecurity Supply Chain Risk Management (C-SCRM) program · Data Protection Impact Assessment (DPIA)	· Cybersecurity Supply Chain Risk Management (C-SCRM) program · Data Protection Impact Assessment (DPIA)	· Cybersecurity Supply Chain Risk Management (C-SCRM) program · Data Protection Impact Assessment (DPIA)
TPM-05	· Cybersecurity Supply Chain Risk Management (C-SCRM) program · Data Protection Impact Assessment (DPIA) · Third-party contract requirements for	· Cybersecurity Supply Chain Risk Management (C-SCRM) program · Data Protection Impact Assessment (DPIA) · Third-party contract requirements for	· Cybersecurity Supply Chain Risk Management (C-SCRM) program · Data Protection Impact Assessment (DPIA) · Third-party contract requirements for	· Cybersecurity Supply Chain Risk Management (C-SCRM) program · Data Protection Impact Assessment (DPIA) · Third-party contract requirements for	· Cybersecurity Supply Chain Risk Management (C-SCRM) program · Data Protection Impact Assessment (DPIA) · Third-party contract requirements for
TPM-05.2	· Cybersecurity Supply Chain Risk Management (C-SCRM) program · Data Protection Impact Assessment (DPIA) · Third-party contract requirements for	· Cybersecurity Supply Chain Risk Management (C-SCRM) program · Data Protection Impact Assessment (DPIA) · Third-party contract requirements for	· Cybersecurity Supply Chain Risk Management (C-SCRM) program · Data Protection Impact Assessment (DPIA) · Third-party contract requirements for	· Cybersecurity Supply Chain Risk Management (C-SCRM) program · Data Protection Impact Assessment (DPIA) · Third-party contract requirements for	· Cybersecurity Supply Chain Risk Management (C-SCRM) program · Data Protection Impact Assessment (DPIA) · Third-party contract requirements for
TPM-05.4	· Cybersecurity Supply Chain Risk Management (C-SCRM) program · Third-party contract requirements for cybersecurity controls · Customer Responsibility Matrix (CRM)	· Cybersecurity Supply Chain Risk Management (C-SCRM) program · Third-party contract requirements for cybersecurity controls · Customer Responsibility Matrix (CRM)	· Cybersecurity Supply Chain Risk Management (C-SCRM) program · Third-party contract requirements for cybersecurity controls · Customer Responsibility Matrix (CRM)	· Cybersecurity Supply Chain Risk Management (C-SCRM) program · Third-party contract requirements for cybersecurity controls · Customer Responsibility Matrix (CRM)	· Cybersecurity Supply Chain Risk Management (C-SCRM) program · Third-party contract requirements for cybersecurity controls · Customer Responsibility Matrix (CRM)
TPM-08	· Cybersecurity Supply Chain Risk Management (C-SCRM) program	· Cybersecurity Supply Chain Risk Management (C-SCRM) program	· Cybersecurity Supply Chain Risk Management (C-SCRM) program	· Cybersecurity Supply Chain Risk Management (C-SCRM) program	· Cybersecurity Supply Chain Risk Management (C-SCRM) program
VPM-01	· Third-party advisors (e.g., virtual CISO, Managed Security Services Provider (MSSP), etc.)	· Third-party advisors (e.g., virtual CISO, Managed Security Services Provider (MSSP), etc.)	· Vulnerability & Patch Management Program	· Vulnerability & Patch Management Program	· Vulnerability & Patch Management Program
VPM-02					
VPM-05	· ManageEngine Endpoint Central (https://manageengine.com)	· ManageEngine Endpoint Central (https://manageengine.com)	· ManageEngine Endpoint Central (https://manageengine.com)	· ManageEngine Endpoint Central (https://manageengine.com)	· ManageEngine Endpoint Central (https://manageengine.com)
VPM-06	· External vulnerability scans (unauthenticated) · Internal vulnerability scans (authenticated) · Nessus (https://tenable.com)	· External vulnerability scans (unauthenticated) · Internal vulnerability scans (authenticated) · Nessus (https://tenable.com)	· External vulnerability scans (unauthenticated) · Internal vulnerability scans (authenticated) · Nessus (https://tenable.com)	· External vulnerability scans (unauthenticated) · Internal vulnerability scans (authenticated) · Nessus (https://tenable.com)	· External vulnerability scans (unauthenticated) · Internal vulnerability scans (authenticated) · Nessus (https://tenable.com)
WEB-01					

Standard #	AICPA TSC 2017:2022 (used for SOC 2)	BSI Standard 200-1	CIS CSC v8.1	ISO 27001 v2022	ISO 27002 v2022	NIST 800-53 rev5	NIST 800-171 rev2	NIST 800-171 rev3	NIST CSF v2.0
PES-12.1					7.12	PE-4 SC-7(14)	3.10.1	03.10.08	
PES-12.2	PI1.4					PE-5	3.10.1	03.10.07.e	
PRI-01	CC1.3-POF6 CC2.3-POF7 CC8.1-POF17 CC8.1-POF18 P1.0				5.1 5.34	PM-18 PT-1			GV.OC-03
PRM-01	CC2.2 CC3.1 CC3.1-POF4 CC3.4 CC5.2	8.2		5.1(e)	5.4 5.8	PL-1	NFO-PL-1	03.16.01	GV.RM GV.RR-03
RSK-01	A1.2-POF1 CC3.1 CC3.2-POF1 CC3.2-POF3 CC3.2-POF5	10.2.1	16.6	6.1 6.1.1 6.1.1(a) 6.1.1(b) 6.1.1(c)	7.5	PM-9 PM-29 RA-1	NFO-RA-1	03.11.01.a 03.17.01.a	GV GV.OV-02 GV.OV-03 GV.RM GV.RM-01
RSK-03	A1.2 A1.2-POF1 CC3.2 CC3.2-POF1 CC3.2-POF2			6.1.2(c) 6.1.2(c)(1) 6.1.2(c)(2)	5.8			03.11.01.a	ID
RSK-04	A1.2 CC3.1-POF16 CC3.2-POF1 CC3.2-POF2 CC3.2-POF3			6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e)	5.8 7.5	RA-3	3.11.1	03.11.01.a	GV.RM-06 ID ID.RA-01 ID.RA-05
RSK-04.1	CC4.2-POF3							03.12.02.a.01 03.12.02.a.02	GV.RM-06 ID ID.RA-01
RSK-06	CC1.1-POF4 CC4.2 CC5.3-POF4 CC7.4 CC7.4-POF8		18.3	6.1.3 6.1.3(a) 6.1.3(b) 6.1.3(c) 6.1.3(d)	5.8		3.11.3	03.11.02.b 03.12.02.a.02	GV.RM-04 ID.RA-05 ID.RA-06
SAT-01	CC1.4 CC1.4-POF3 CC2.2-POF12 CC2.2-POF8	6	14 14.1	7.4 7.4(a) 7.4(b) 7.4(c) 7.4(d)	6.3	AT-1 PM-13	NFO-AT-1	03.02.01.a	PR.AT
SAT-02	CC1.4-POF7 CC2.2-POF12 CC2.2-POF8		14.3 14.7 14.8	7.4 7.4(a) 7.4(b) 7.4(c) 7.4(d)	6.3	AT-2	3.2.1	03.01.22.a 03.02.01.a.01 03.02.01.a.02 03.02.01.a.03 03.02.01.b	PR.AT PR.AT-01
TPM-01	CC1.1-POF5 CC1.4-POF2 CC1.4-POF3 CC2.3-POF10 CC2.3-POF12		15 15.2		5.19 5.20 8.30	SA-4 SR-1	3.1.1 NFO-SA-4	03.01.20.a 03.01.20.b 03.01.20.c.01 03.07.06.a 03.16.01	GV.SC-04 GV.SC-06 GV.SC-07 GV.SC-08 GV.SC-10
TPM-01.1	CC2.1-POF6		15.1		5.19			03.07.06.a	GV.SC-04 GV.SC-07 GV.SC-08 ID.AM ID.AM-01
TPM-03	CC1.1-POF5 CC3.2-POF7 CC9.1 CC9.2-POF1 CC9.2-POF10				5.19 5.21 5.22 8.30	SA-9(3) SR-2 SR-2(1)		03.11.01.a 03.17.01.a 03.17.03.a 03.17.03.b	GV.SC GV.SC-06 GV.SC-07
TPM-05	CC1.1-POF5 CC2.3-POF10 CC2.3-POF11 CC2.3-POF12 CC2.3-POF2		15.4		5.19 5.20 5.21 5.31 6.6	SR-3(3)	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	GV.OC-02 GV.OC-03 GV.SC-02 GV.SC-05 GV.SC-06
TPM-05.2	CC2.3-POF12 CC9.2-POF1 CC9.2-POF10 CC9.2-POF9 P6.4-POF3					SR-3(3)	3.1.1	03.16.03.a 03.16.03.b 03.16.03.c 03.17.02 03.17.03.b	GV.OC-03 GV.SC-02 GV.SC-05 GV.SC-06 GV.SC-10
TPM-05.4	CC1.1-POF5 CC1.3-POF3 CC1.3-POF4 CC1.3-POF5 CC2.2-POF5		15	4.3(c)	5.2 5.23	SA-9(3)		03.07.06.a 03.16.03.b	GV.OC GV.OC-02 GV.RM-05 GV.RR GV.RR-02
TPM-08	CC1.4-POF2 CC1.4-POF3 CC3.4 CC3.4-POF5 CC9.1		15 15.6		5.19 5.20 5.22 8.21	SR-6 SR-6(1)		03.16.03.c 03.17.02	GV.SC-07 ID.IM-01 ID.IM-02
VPM-01	CC3.2-POF7 CC3.2-POF9 CC3.4-POF6 CC8.1-POF14 CC8.1-POF16		7 7.1 18		8.8	SI-2 SI-3	3.14.1	03.11.02.a 03.14.01.a	ID.RA-01 ID.RA-08 PR.PS-02
VPM-02	CC4.2 CC5.3-POF4 CC7.4-POF8		7.2 7.7		8.8	PM-4 SC-18(1)	3.14.1	03.11.02.b 03.12.02.a.02 03.14.01.a	ID.RA-08 PR.PS-02
VPM-05	CC8.1-POF14 CC8.1-POF16		7.3 7.4 12.1 18.3		8.8	SI-2 SI-2(4) SI-3	3.11.3 3.14.1	03.11.02.b 03.12.02.a.02 03.14.01.a 03.14.01.b	PR.PS-02
VPM-06	CC3.2-POF7 CC3.4-POF6 CC7.1 CC7.1-POF5 CC9.2-POF13		7.5 7.6		8.8	RA-5	3.11.2	03.11.02.a	ID.RA-01
WEB-01							3.1.22	03.01.22.a	

Policy Domain	Standard #	Standard Name	SCF CORE Fundamentals	US CMMC 2.0 Level 1	US FAR 52.204-21	US FAR 52.204-27	US FAR Section 889	Control Question	Possible Solutions & Considerations Micro-Small Business (<10 staff) BLS Firm Size Classes 1-2	Possible Solutions & Considerations Small Business (10-49 staff) BLS Firm Size Classes 3-4	Possible Solutions & Considerations Medium Business (50-249 staff) BLS Firm Size Classes 5-6	Possible Solutions & Considerations Large Business (250-999 staff) BLS Firm Size Classes 7-8	Possible Solutions & Considerations Enterprise (> 1,000 staff) BLS Firm Size Class 9	AICPA TSC 2017-2022 (used for SOC 2)	BSI Standard 200-1	CIS CSC v8.1	ISO 27001 v2022	ISO 27002 v2022	NIST 800-53 rev5	NIST 800-171 rev2	NIST 800-171 rev3	NIST CSF v2.0
Web Security	WEB-02	Use of Demilitarized Zones (DMZ)		AC.L1-3.1.22	52.204-21(b)(1)(iv)			Does the organization utilize a Demilitarized Zone (DMZ) to restrict inbound traffic to authorized Technology Assets, Applications and/or Services (TAAS) on certain services, protocols and ports?										8.22		3.1.22		
Web Security	WEB-04	Client-Facing Web Services		AC.L1-3.1.22	52.204-21(b)(1)(iv)			Does the organization deploy reasonably-expected security controls to protect the confidentiality and availability of client data that is stored, transmitted or processed by the Internet-based service?												3.1.22		