Set Theory Relationship Mapping (STRM)

Reference Document : **Secure Controls Framework (SCF) version 2024.4**
Focal Document: **CMMC Self-Assessment Guide Level 1**
Focal Document URL: **https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level1_V2.0_FinalDraft_20211210_508.pdf**
STRM URL: **https://securecontrolsframework.com/content/strm/scf-strm-cmmc-2-level-1.pdf**

Set Theory Relationship Mapping (STRM) is well-suited for mapping between sets of elements that exist in two distinct concepts that are mostly the same as each other (e.g., cybersecurity & data privacy requirements). STRM also allows the strength of the mapping to be captured.

STRM relies on a justification for the relationship claim. There are three (3) options for the rationale, which is a high-level context within which the two concepts are related:

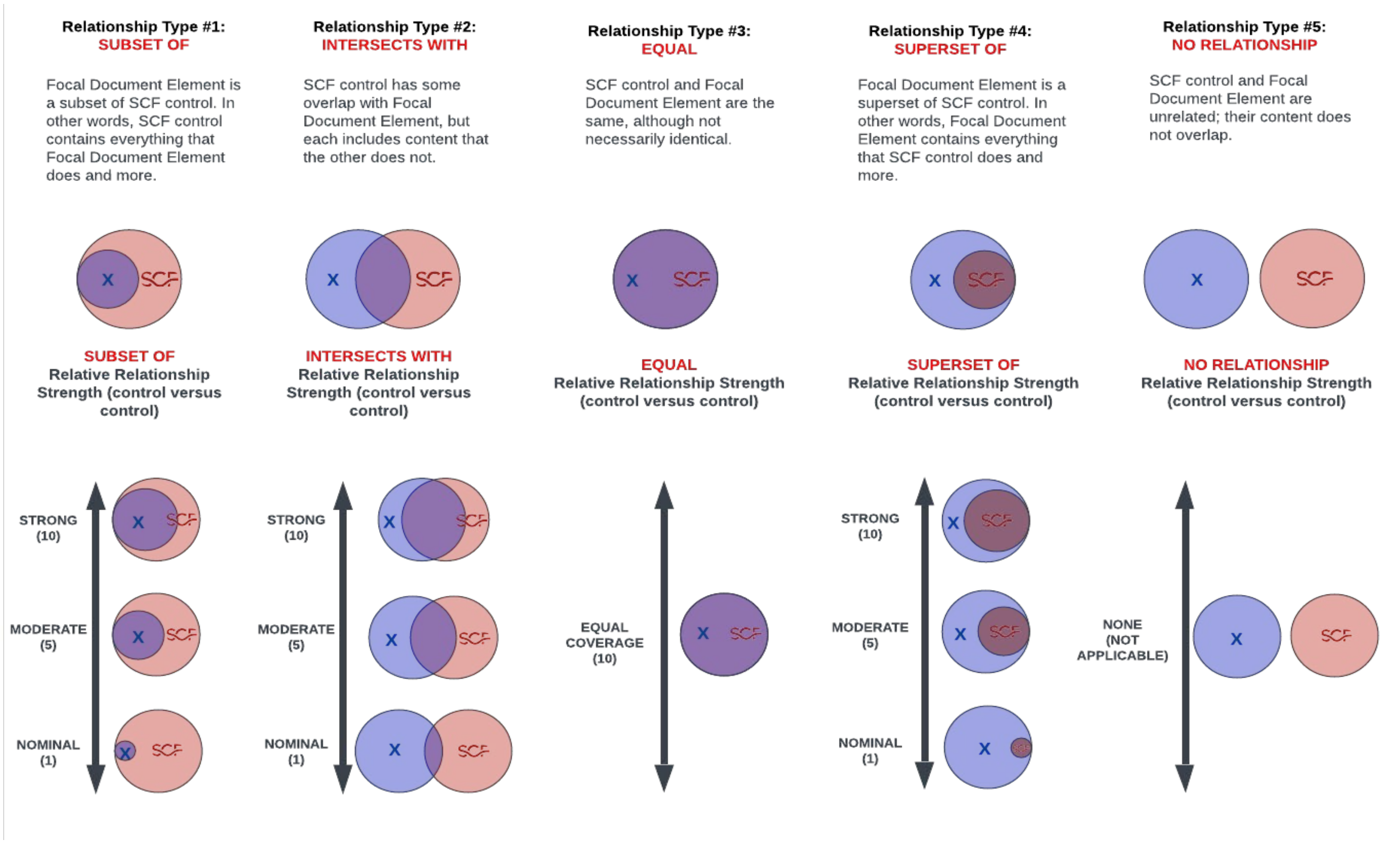
1. **Syntactic**: How similar is the wording that expresses the two concepts? This is a word-for-word analysis of the relationship, not an interpretation of the language.
2. **Semantic**: How similar are the meanings of the two concepts? This involves some interpretation of each concept's language.
3. **Functional**: How similar are the results of executing the two concepts? This involves understanding what will happen if the two concepts are implemented, performed, or otherwise executed.

Based on NIST IR 8477, STRM supports five (5) five relationship types to describe the logical similarity between two distinct concepts:

1. **Subset Of**
2. **Intersects With**
3. **Equal**
4. **Superset Of**
5. **No Relationship**

SCF Reference Document

Law, Regulation or Framework Focal Document



Relationship Type #1: SUBSET OF

Focal Document Element is a subset of SCF control. In other words, SCF control contains everything that Focal Document Element does and more.

Relationship Type #2: INTERSECTS WITH

SCF control has some overlap with Focal Document Element, but each includes content that the other does not.

Relationship Type #3: EQUAL

SCF control and Focal Document Element are the same, although not necessarily identical.

Relationship Type #4: SUPERSET OF

Focal Document Element is a superset of SCF control. In other words, Focal Document Element contains everything that SCF control does and more.

Relationship Type #5: NO RELATIONSHIP

SCF control and Focal Document Element are unrelated; their content does not overlap.

X
SCF
SUBSET OF Relative Relationship Strength (control versus control)
INTERSECTS WITH Relative Relationship Strength (control versus control)
EQUAL Relative Relationship Strength (control versus control)
SUPERSET OF Relative Relationship Strength (control versus control)
NO RELATIONSHIP Relative Relationship Strength (control versus control)
STRONG (10)
MODERATE (5)
NOMINAL (1)
EQUAL COVERAGE (10)
NONE (NOT APPLICABLE)

CMMC FDE#	FAR 52.204-21 FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
Not In CMMC Level 1	52.204-21(a)	N/A	Read FAR 52.204-21(a) for full text (https://www.acquisition.gov/far/52.204-21)	Functional	intersects with	Standardized Terminology	SEA-02.1	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	5	
Not In CMMC Level 1	52.204-21(b)	N/A	This is merely a section title without content.	Functional	no relationship	N/A	N/A	N/A	N/A	N/A
Not In CMMC Level 1	52.204-21(b)(1)	N/A	The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:	Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
				Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	8	
				Functional	intersects with	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	8	
				Functional	intersects with	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing data and technology-related risks.	8	
				Functional	subset of	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	10	
AC.L1-3.1.1	52.204-21(b)(1)(i)	Authorized Access Control	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Functional	intersects with	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	5	
				Functional	intersects with	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
				Functional	intersects with	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	5	
				Functional	intersects with	Identifier Management (User Names)	IAC-09	Mechanisms exist to govern naming standards for usernames and systems.	5	
				Functional	intersects with	Authenticator Management	IAC-10	Mechanisms exist to securely manage authenticators for users and devices.	5	
				Functional	intersects with	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	
				Functional	intersects with	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	5	
				Functional	intersects with	Automated System Account Management (Directory Services)	IAC-15.1	Automated mechanisms exist to support the management of system accounts (e.g., directory services).	5	
				Functional	equal	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	10	
				Functional	intersects with	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	8	
				Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
				Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
				Functional	intersects with	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity & data privacy requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
AC.L1-3.1.2	52.204-21(b)(1)(ii)	Transaction & Function Control	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	Functional	intersects with	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	5	
				Functional	intersects with	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	5	
				Functional	intersects with	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5	
				Functional	intersects with	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	3	
				Functional	intersects with	Work From Anywhere (WFA) - Telecommuting Security	NET-14.5	Mechanisms exist to define secure telecommuting practices and govern remote access to systems and data for remote workers.	3	
AC.L1-3.1.20	52.204-21(b)(1)(iii)	External Connections	Verify and control/limit connections to and use of external information systems.	Functional	equal	Use of External Information Systems	DCH-13	Mechanisms exist to govern how external parties, systems and services are used to securely store, process and transmit data.	10	
				Functional	intersects with	Portable Storage Devices	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.	3	
				Functional	intersects with	Protecting Sensitive Data on External Systems	DCH-13.3	Mechanisms exist to ensure that the requirements for the protection of sensitive information processed, stored or transmitted on external systems, are implemented in accordance with applicable statutory, regulatory and contractual obligations.	5	
				Functional	intersects with	Ad-Hoc Transfers	DCH-17	Mechanisms exist to secure ad-hoc exchanges of large digital files with internal or external parties.	3	
				Functional	intersects with	Limits of Authorized Use	DCH-13.1	Mechanisms exist to prohibit external parties, systems and services from storing, processing and transmitting data unless authorized individuals first: (1) Verifying the implementation of required security controls; or (2) Retaining a processing agreement with the entity hosting the external systems or service.	5	
AC.L1-3.1.22	52.204-21(b)(1)(iv)	Control Public Information	Control information posted or processed on publicly accessible information systems.	Functional	intersects with	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	5	
				Functional	intersects with	Cloud Security Architecture	CLD-02	Mechanisms exist to ensure the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud employments.	5	
				Functional	intersects with	Multi-Tenant Environments	CLD-06	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	5	
				Functional	intersects with	Sensitive Data In Public Cloud Providers	CLD-10	Mechanisms exist to limit and manage the storage of sensitive/regulated data in public cloud providers.	5	
				Functional	intersects with	Publicly Accessible Content	DCH-15	Mechanisms exist to control publicly-accessible content.	5	
				Functional	intersects with	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	8	
				Functional	intersects with	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity & data privacy principles in their daily work.	8	
				Functional	intersects with	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	8	
				Functional	intersects with	Social Media & Social Networking Restrictions	HRS-05.2	Mechanisms exist to define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information.	8	

CMMC FDE#	FAR 52.204-21 FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
				Functional	intersects with	Web Security	WEB-01	Mechanisms exist to facilitate the implementation of an enterprise-wide web management policy, as well as associated standards, controls and procedures.	3	
				Functional	intersects with	Use of Demilitarized Zones (DMZ)	WEB-02	Mechanisms exist to utilize a Demilitarized Zone (DMZ) to restrict inbound traffic to authorized devices on certain services, protocols and ports.	3	
				Functional	intersects with	Client-Facing Web Services	WEB-04	Mechanisms exist to 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	
IA.L1-3.5.1	52.204-21(b)(1)(v)	Identification	Identify information system users, processes acting on behalf of users, or devices.	Functional	intersects with	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	8	
				Functional	intersects with	Identification & Authentication for Devices	IAC-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically- based and replay resistant.	8	
IA.L1-3.5.2	52.204-21(b)(1)(vi)	Authentication	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	Functional	intersects with	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
				Functional	intersects with	Identification & Authentication for Devices	IAC-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically- based and replay resistant.	5	
MP.L1-3.8.3	52.204-21(b)(1)(vii)	Media Disposal	Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.	Functional	subset of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
				Functional	intersects with	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.	8	
				Functional	subset of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
				Functional	equal	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	10	
				Functional	intersects with	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	8	
PE.L1-3.10.1	52.204-21(b)(1)(viii)	Limit Physical Access	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	Functional	subset of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
				Functional	subset of	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	10	
				Functional	intersects with	Physical Security of Offices, Rooms & Facilities	PES-04	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	5	
				Functional	intersects with	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	5	
				Functional	intersects with	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5	
				Functional	intersects with	Access Control for Output Devices	PES-12.2	Physical security mechanisms exist to restrict access to printers and other system output devices to prevent unauthorized individuals from obtaining the output.	5	
PE.L1-3.10.3	52.204-21(b)(1)(ix)	Escort Visitors	Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.	Functional	intersects with	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	3	
				Functional	intersects with	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5	
				Functional	intersects with	Distinguish Visitors from On-Site Personnel	PES-06.1	Physical access control mechanisms exist to easily distinguish between onsite personnel and visitors, especially in areas where sensitive/regulated data is accessible.	3	
				Functional	intersects with	Restrict Unescorted Access	PES-06.3	Physical access control mechanisms exist to restrict unescorted access to facilities to personnel with required security clearances, formal access authorizations and validate the need for access.	5	
PE.L1-3.10.4	Not In FAR 52.204-21	Physical Access Logs	Maintain audit logs of physical access.	Functional	equal	Physical Access Logs	PES-03.3	Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points.	10	
PE.L1-3.10.5	Not In FAR 52.204-21	Manage Physical Access	Control and manage physical access devices.	Functional	subset of	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	10	
SC.L1-3.13.1	52.204-21(b)(1)(x)	Boundary Protection	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	Functional	subset of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
				Functional	intersects with	Layered Network Defenses	NET-02	Mechanisms exist to implement security functions as a layered structure that minimizes interactions between layers of the design and avoids any dependence by lower layers on the functionality or correctness of higher layers.	3	
				Functional	intersects with	Guest Networks	NET-02.2	Mechanisms exist to implement and manage a secure guest network.	3	
				Functional	equal	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	10	
SC.L1-3.13.5	52.204-21(b)(1)(xi)	Public-Access System Separation	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	Functional	intersects with	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
				Functional	intersects with	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	5	
SI.L1-3.14.1	52.204-21(b)(1)(xii)	Flaw Remediation	Identify, report, and correct information and information system flaws in a timely manner.	Functional	subset of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
				Functional	subset of	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	10	
				Functional	subset of	Continuous Vulnerability Remediation Activities	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	10	
				Functional	intersects with	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	8	
SI.L1-3.14.2	52.204-21(b)(1)(xiii)	Malicious Code Protection	Provide protection from malicious code at appropriate locations within organizational information systems.	Functional	subset of	Endpoint Security	END-01	Mechanisms exist to facilitate the implementation of endpoint security controls.	10	
				Functional	equal	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	10	
SI.L1-3.14.4	52.204-21(b)(1)(xiv)	Update Malicious Code Protection	Update malicious code protection mechanisms when new releases are available.	Functional	intersects with	Automatic Antimalware Signature Updates	END-04.1	Mechanisms exist to automatically update antimalware technologies, including signature definitions.	8	
SI.L1-3.14.5	52.204-21(b)(1)(xv)	System & File Scanning	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	Functional	intersects with	Always On Protection	END-04.7	Mechanisms exist to ensure that anti-malware technologies are continuously running in real-time and cannot be disabled or altered by non-privileged users, unless specifically authorized by management on a case-by-case basis for a limited time period.	8	