Set Theory Relationship Mapping (STRM)

Reference Document : **Secure Controls Framework (SCF) version 2024.4**
Focal Document: **DHS CISA Trusted Internet Connections 3.0**
Focal Document URL: **https://www.cisa.gov/sites/default/files/2023-12/CISA%20TIC%203.0%20Security%20Capabilities%20Catalog_508c.pdf**
STRM URL: **https://securecontrolsframework.com/content/strm/scf-strm-dhs-cis-tic-3-0.pdf**

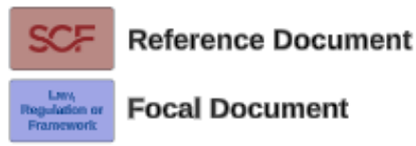
Set Theory Relationship Mapping (STRM) is well-suited for mapping between sets of elements that exist in two distinct concepts that are mostly the same as each other (e.g., cybersecurity & data privacy requirements). STRM also allows the strength of the mapping to be captured.

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.

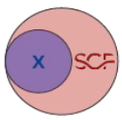
Based on NIST IR 8477, STRM supports five (5) five relationship types to describe the logical similarity between two distinct concepts:

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

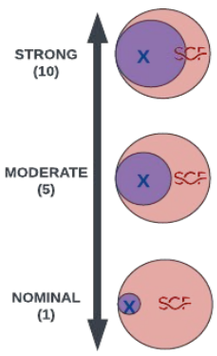


Relationship Type #1: SUBSET OF

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

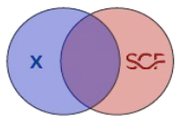


SUBSET OF
Relative Relationship Strength (control versus control)

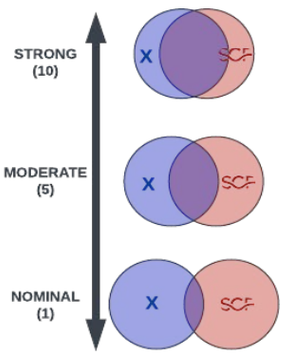


Relationship Type #2: INTERSECTS WITH

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

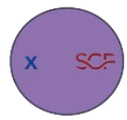


INTERSECTS WITH
Relative Relationship Strength (control versus control)

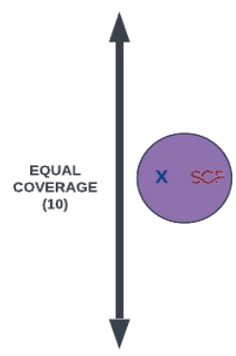


Relationship Type #3: EQUAL

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

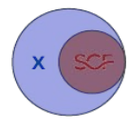


EQUAL
Relative Relationship Strength (control versus control)

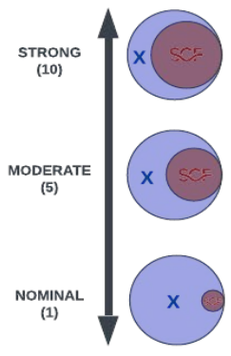


Relationship Type #4: SUPERSET OF

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

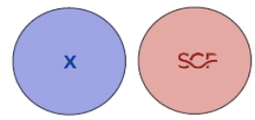


SUPERSET OF
Relative Relationship Strength (control versus control)

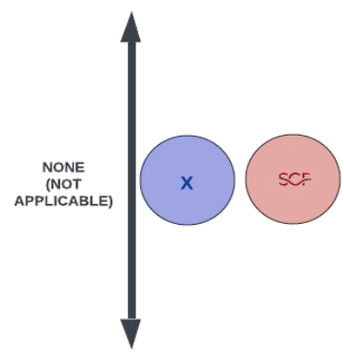


Relationship Type #5: NO RELATIONSHIP

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



NO RELATIONSHIP
Relative Relationship Strength (control versus control)



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)
3 UNL.SCRMA	Supply Chain Risk Management	Supply chain risk management involves implementing a systematic process for managing risk exposures, threats, and vulnerabilities throughout the supply chain. It also involves developing risk response strategies for the risks presented by the supplier, the supplied products and services, or the cyber supply chain.	Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
3.PE P.EM.EDRPR	Email Domain Reputation Protections	Email domain reputation protections entails monitoring an email domain’s reputation and employing policies to help protect the email domain’s reputation.	Functional	intersects with	Email Domain Reputation Protections	NET-20.1	Mechanisms exist to monitor the organization's email domain’s reputation and protect the email domain’s reputation.	5	
3.PEP.DA.ACONT	Access Control	Access control technologies allow an agency to define policies concerning the allowable activities of users and entities to data and resources.	Functional	subset of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
3.PEP.DA.DAUTE	Data Access and Use Telemetry	This entails identifying agency sensitive data stored, processed, or transmitted, including those located at a service provider and enforcing detailed logging for access or changes to sensitive data.	Functional	intersects with	Data Action Mapping	AST-02.8	Mechanisms exist to create and maintain a map of technology assets where sensitive/regulated data is stored, transmitted or processed.	5	
			Functional	intersects with	Data Access Mapping	DCH-14.3	Mechanisms exist to leverages a data-specific Access Control List (ACL) or Interconnection Security Agreements (ISAs) to generate a logical map of the parties with whom sensitive/regulated data is shared.	5	
3.PEP.DA.DINVE	Data Inventory	Data inventory entails developing, documenting, and maintaining a current inventory of agency data.	Functional	intersects with	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: (1) Accurately reflects the current systems, applications and services in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5	
			Functional	intersects with	Sensitive Data Inventories	DCH-06.2	Mechanisms exist to maintain inventory logs of all sensitive media and conduct sensitive media inventories at least annually.	5	
3.PEP.DA.DLABE	Data Labeling	Data labeling is the process of tagging data by categories to protect and control the use of data and identifying a level of risk associated with the data.	Functional	intersects with	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
			Functional	intersects with	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
			Functional	intersects with	Data Tags	DCH-22.2	Mechanisms exist to utilize data tags to automate tracking of sensitive/regulated data across the information lifecycle.	5	
3.PEP.DA.DLPRE	Data Loss Prevention	DLP technologies detect instances of the exfiltration, either malicious or accidental, of agency data.	Functional	intersects with	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	5	
3.PEP.DA.PDRES	Protections for Data at Rest	Data protection at rest aims to secure data stored on any device or storage medium.	Functional	intersects with	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
			Functional	subset of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
			Functional	intersects with	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is stored.	5	
3.PEP.DA.PDTRA	Protections for Data in Transit	Data protection in transit, or data in motion, aims to secure data that is actively moving from one location to another, such as across the internet or through a private enterprise network.	Functional	intersects with	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
3.PEP.DO.DNMON	Domain Name Monitoring	Domain name monitoring allows agencies to discover the creation of or changes to agency domains.	Functional	intersects with	Domain Registrar Security	NET-10.4	Mechanisms exist to lock the domain name registrar to prevent a denial of service caused by unauthorized deletion, transfer or other unauthorized modification of a domain’s registration details.	5	
3.PEP.DO.DNSIN	Domain Name Sinkholing	Domain name sinkholing protections are a form of denylisting that protect clients from accessing malicious domains by responding to DNS queries for those domains.	Functional	intersects with	DNS & Content Filtering	NET-18	Mechanisms exist to 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.	5	
3.PEP.DO.DNVAC	Domain Name Verification for Agency Clients	Domain name verification protections ensure that domain name lookups from agency clients, whether for internal or external domains, are validated according to Domain Name System Security Extensions (DNSSEC).	Functional	intersects with	Secure Name / Address Resolution Service (Recursive or Caching Resolver)	NET-10.2	Mechanisms exist to perform data origin authentication and data integrity verification on the Domain Name Service (DNS) resolution responses received from authoritative sources when requested by client systems.	5	
			Functional	intersects with	Domain Name Verification	NET-18.5	Mechanisms exist to ensure that domain name lookups, whether for internal or external domains, are validated according to Domain Name System Security Extensions (DNSSEC).	5	
3.PEP.DO.DNVAD	Domain Name Validation for Agency Domains	Domain name validation protections ensure that all agency domain names are secured using DNSSEC, enabling external entities to validate their resolution to the domain names.	Functional	intersects with	Secure Name / Address Resolution Service (Recursive or Caching Resolver)	NET-10.2	Mechanisms exist to perform data origin authentication and data integrity verification on the Domain Name Service (DNS) resolution responses received from authoritative sources when requested by client systems.	5	
3.PEP.DO.PDSER	CISA’s Protective DNS Service	CISA’s Protective DNS Service is a shared service offering that provides domain name sinkholing protections.	Functional	superset of	DNS & Content Filtering	NET-18	Mechanisms exist to 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.	5	
3.PEP.EM.AEPRO	Adaptive Email Protections	Adaptive email protections involve employing risk- based analysis in the application and enforcement of email protections.	Functional	intersects with	Adaptive Email Protections	NET-20.7	Mechanisms exist to utilize adaptive email protections that involve employing risk-based analysis in the application and enforcement of email protections.	5	
3.PEP.EM.APPRO	Anti-phishing Protections	Anti-phishing protections detect instances of phishing and prevent users from accessing them.	Functional	intersects with	Phishing & Spam Protection	END-08	Mechanisms exist to utilize anti-phishing and spam protection technologies to detect and take action on unsolicited messages transported by electronic mail.	5	
3.PEP.EM.ARCHA	Authenticated Received Chain	Authenticated received chain allows for an intermediary, like a mailing list or forwarding service, to sign its own authentication of the original email, allowing downstream entities to accept the intermediary’s authentication even if the email was changed.	Functional	intersects with	Authenticated Received Chain (ARC)	NET-20.3	Mechanisms exist to utilize an authenticated received chain that allows for an intermediary to sign its own authentication of the original email, allowing downstream entities to accept the intermediary’s authentication even if the email was changed.	5	
3.PEP.EM.ASPRO	Anti-spam Protections	Anti-spam protections detect and quarantine instances of spam.	Functional	intersects with	Phishing & Spam Protection	END-08	Mechanisms exist to utilize anti-phishing and spam protection technologies to detect and take action on unsolicited messages transported by electronic mail.	5	
3.PEP.EM.CFILT	Content Filtering	Content filtering protections detect the presence of unapproved content and facilitate its removal or denial of access.	Functional	intersects with	DNS & Content Filtering	NET-18	Mechanisms exist to 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.	5	
3.PEP.EM.DLPRE	Data Loss Prevention	DLP technologies detect instances of the exfiltration, either malicious or accidental, of agency data.	Functional	intersects with	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	5	
3.PEP.EM.DSOEM	Domain Signatures for Outgoing Email	Domain signature protections facilitate the authentication of outgoing email by signing the emails and ensuring that external parties may validate the email signatures according to the DMARC email authentication protocol that is defined in RFC 7489.	Functional	intersects with	User Digital Signatures for Outgoing Email	NET-20.5	Mechanisms exist to enable users to digitally sign their emails, allowing external parties to authenticate the email’s sender and its contents according to the Domain-based Message Authentication Reporting and Conformance (DMARC) email authentication protocol.	5	
3.PEP.EM.DSVIE	Domain Signature Verification for Incoming Email	Domain signature verification protections authenticate incoming email according to the Domain-based Message Authentication Reporting and Conformance (DMARC) email authentication protocol defined in Request for Comments (RFC) 74895F6.	Functional	intersects with	Domain-Based Message Authentication Reporting and Conformance (DMARC)	NET-20.4	Mechanisms exist to implement domain signature verification protections that authenticate incoming email according to the Domain-based Message Authentication Reporting and Conformance (DMARC).	5	
3.PEP.EM.E3AEP	EINSTEIN 3 Accelerated Email Protections	EINSTEIN 3 Accelerated (E3A) is an intrusion prevention capability offered by NCPS, provided by CISA, that includes an email filtering security service.	Functional	superset of	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-08	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	5	
			Functional	intersects with	Detonation Chambers (Sandboxes)	IRO-15	Mechanisms exist to utilize a detonation chamber capability to detect and/or block potentially-malicious files and email attachments.	5	
3.PEP.EM.EETRA	Encryption for Email Transmission	Email services are configured to use encrypted connections, when possible, for communications between clients and other email servers.	Functional	intersects with	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
3.PEP.EM.ELABE	Email Labeling	Email labeling is the process of automatically tagging incoming or outgoing email to manage risk.	Functional	intersects with	Email Labeling	NET-20.8	Automated mechanisms exist to implement email labeling that apply organization-defined tags to incoming or outgoing email.	5	
3.PEP.EM.EOEMA	Encryption for Outgoing Email	Email encryption protections allow for the encryption of outgoing emails, which limits the visibility of their contents to the intended recipients.	Functional	intersects with	Encryption for Outgoing Email	NET-20.6	Mechanisms exist to enable the encryption of outgoing emails using organization-approved cryptographic means.	5	
3.PEP.EM.LCTPR	Link Click- through Protections	Link click-through protections ensure that when a link from an email is clicked, the requester is directed to a protection that verifies the security of the link destination before permitting access.	Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
			Functional	intersects with	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	5	
			Functional	intersects with	DNS & Content Filtering	NET-18	Mechanisms exist to 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.	5	
3.PEP.EM.MCQUE	Mail Content Query	Mail content query enables search and discovery for email across agency mailboxes.	Functional	intersects with	Electronic Discovery (eDiscovery)	BCD-12.3	Mechanisms exist to utilize electronic discovery (eDiscovery) that covers current and archived communication transactions.	5	
3.PEP.EM.MFPRO	Malicious File Protections	Malicious file protections detect malicious attachments files in emails and prevent users from accessing them.	Functional	intersects with	Detonation Chambers (Sandboxes)	IRO-15	Mechanisms exist to utilize a detonation chamber capability to detect and/or block potentially-malicious files and email attachments.	5	
			Functional	intersects with	Email Content Protections	NET-20	Mechanisms exist to implement an email filtering security service to detect malicious attachments in emails and prevent users from accessing them.	5	
3.PEP.EM.MLPRO	Malicious Link Protections	Malicious link protections detect malicious links in emails and prevent users from accessing them.	Functional	intersects with	DNS & Content Filtering	NET-18	Mechanisms exist to 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.	5	
3.PEP.EM.PDPRO	Post-Delivery Protections	Post-delivery protections apply updated email protections to already delivered emails, enabling quarantining and mitigation for emails in mailboxes.	Functional	intersects with	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
			Functional	intersects with	Detonation Chambers (Sandboxes)	IRO-15	Mechanisms exist to utilize a detonation chamber capability to detect and/or block potentially-malicious files and email attachments.	5	
3.PEP.EM.SDENY	Sender Denylisting	Sender denylisting protections prevent the reception of email from denylisted senders, domains, or email servers.	Functional	intersects with	Sender Denylisting	NET-20.2	Mechanisms exist to implement sender denylisting protections that prevent the reception of email from denylisted senders, domains and/or email servers.	5	

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)
3.PEP.EM.UDSOE	User Digital Signatures for Outgoing Email	User digital signature protections enable users to digitally sign their emails, allowing external parties to authenticate the email's sender and its contents.	Functional	intersects with	User Digital Signatures for Outgoing Email	NET-20.5	Mechanisms exist to enable users to digitally sign their emails, allowing external parties to authenticate the email's sender and its contents according to the Domain-based Message Authentication Reporting and Conformance (DMARC) email authentication protocol.	5	
3.PEP.EM.UTIPP	User Tipping	User tipping capabilities enable users to report emails, attachments, or URLs they suspect to be phishing attempts, spam, or otherwise malicious.	Functional	intersects with	User Threat Reporting	NET-20.9	Mechanisms exist to incorporate submissions from users of phishing attempts, spam or otherwise malicious actions to better protect the organization.	5	
3.PEP.EN.ACONT	Application Container	An application container is a virtualization approach in which applications are isolated to a known set of dependencies, access methods, and interfaces.	Functional	intersects with	Application Container	SEA-21	Mechanisms exist to utilize an application container (virtualization approach) to isolate to a known set of dependencies, access methods and interfaces.	5	
3.PEP.EN.CMONI	Costs Monitoring	Costs monitoring entails the monitoring of costs incurred by enterprise resources.	Functional	subset of	Cybersecurity & Data Privacy Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy-related resource planning controls that define a viable plan for achieving cybersecurity & data privacy objectives.	10	
			Functional	intersects with	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data privacy requirements within business process planning for projects / initiatives.	5	
3.PEP.EN.RDACC	Remote Desktop Access	Remote desktop access solutions provide a mechanism for connecting to and controlling a remote physical or virtual computer.	Functional	intersects with	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	
3.PEP.EN.SITDE	Shadow Information Technology Detection	Shadow information technology (IT) detection systems detect the presence of unauthorized software and systems in use by an agency.	Functional	intersects with	Shadow Information Technology Detection	OPS-07	Mechanisms exist to detect the presence of unauthorized software, systems and services in use by the organization.	5	
3.PEP.EN.SOARE	Security Orchestration, Automation, and Response	Security Orchestration, Automation, and Response (SOAR) tools define, prioritize, and automate the response to security incidents.	Functional	intersects with	Security Orchestration, Automation, and Response (SOAR)	OPS-06	Mechanisms exist to utilize Security Orchestration, Automation and Response (SOAR) tools to define, prioritize and automate the response to security incidents.	5	
3.PEP.EN.VPNET	Virtual Private Network	Virtual private network (VPN) solutions provide a secure communications mechanism between networks that may traverse across unprotected or public networks.	Functional	intersects with	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	
			Functional	intersects with	Managed Access Control Points	NET-14.3	Mechanisms exist to route all remote accesses through managed network access control points (e.g., VPN concentrator).	5	
			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.	5	
			Functional	intersects with	Third-Party Remote Access Governance	NET-14.6	Mechanisms exist to proactively control and monitor third-party accounts used to access, support, or maintain system components via remote access.	5	
3.PEP.FI.AMALW	Anti-malware	Anti-malware protections detect the presence of malicious code and facilitate its quarantine or removal.	Functional	intersects with	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
3.PEP.FI.CDREC	Content Disarm and Reconstruction	Content disarm and reconstruction technology detects the presence of unapproved active content and facilitates its removal.	Functional	intersects with	Content Disarm and Reconstruction (CDR)	NET-19	Automated Content Disarm and Reconstruction (CDR) mechanisms exist to detect the presence of unapproved active content and facilitate its removal, resulting in content with only known safe elements.	5	
3.PEP.FI.DCHAM	Detonation Chamber	Detonation chambers facilitate the detection of malicious code using protected and isolated execution environments to analyze the files.	Functional	intersects with	Detonation Chambers (Sandboxes)	IRO-15	Mechanisms exist to utilize a detonation chamber capability to detect and/or block potentially-malicious files and email attachments.	5	
3.PEP.FI.DLPRE	Data Loss Prevention	Data loss prevention (DLP) technologies detect instances of the exfiltration, either malicious or accidental, of agency data.	Functional	intersects with	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	5	
3.PEP.ID.AAUTH	Adaptive Authentication	Adaptive authentication aligns the strength of the PR.AC user or entity authentication mechanisms to the level of risk associated with the requested authorization.	Functional	intersects with	Adaptive Identification & Authentication	IAC-13	Mechanisms exist to allow individuals to utilize alternative methods of authentication under specific circumstances or situations.	5	
3.PEP.ID.BBASE	Behavioral Baselining	Behavioral baselining is capturing information about user and entity behavior to enable dynamic threat discovery and facilitate vulnerability management.	Functional	intersects with	Anomalous Behavior	MON-16	Mechanisms exist to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5	
			Functional	intersects with	Suspicious Communications & Anomalous System Behavior	SAT-03.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.	5	
			Functional	intersects with	Behavioral Baselining	THR-11	Automated mechanisms exist to establish behavioral baselines that capture information about user and entity behavior to enable dynamic threat discovery.	5	
3.PEP.ID.CAUTH	Continuous Authentication	Continuous authentication entails validating and re-authenticating identity through the lifecycle of entity interactions.	Functional	intersects with	Continuous Authentication	IAC-13.3	Automated mechanisms exist to enable continuous re-authentication through the lifecycle of entity interactions.	5	
3.PEP.ID.EIAMA	Enterprise Identity and Access Management	Enterprise ICAM entails maintaining visibility into agency identities across agency environments and managing changes to those identities through a formal (preferably automated) process.	Functional	subset of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
3.PEP.ID.EINVE	Entitlement Inventory	Entitlement inventory entails developing, documenting, and maintaining a current inventory of user and entity permissions and authorizations to agency resources.	Functional	intersects with	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	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	intersects with	Privileged Account Inventories	IAC-16.1	Mechanisms exist to inventory all privileged accounts and validate that each person with elevated privileges is authorized by the appropriate level of organizational management.	5	
3.PEP.ID.MAUTH	Multi-factor Authentication	MFA entails using two or more factors to verify user or entity identity.	Functional	intersects with	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	5	
3.PEP.ID.SIDEN	Service Identity	Service identity ensures that users and entities can authenticate the identities of agency services.	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	
			Functional	intersects with	Identification & Authentication for Third Party Systems & Services	IAC-05	Mechanisms exist to identify and authenticate third-party systems and services.	5	
3.PEP.ID.SMANA	Secrets Management	Secrets management entails developing and using a formal process to securely track and manage digital authentication credentials, including certificates, passwords, and API keys.	Functional	intersects with	Authenticator Management	IAC-10	Mechanisms exist to securely manage authenticators for users and devices.	5	
			Functional	intersects with	Password Managers	IAC-10.11	Mechanisms exist to protect and store passwords via a password manager tool.	5	
			Functional	intersects with	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5	
3.PEP.IN.AACON	Adaptive Access Control	Adaptive access control technologies factor in additional context, like security risk, operational needs, and other heuristics, when evaluating access control decisions.	Functional	intersects with	Adaptive Identification & Authentication	IAC-13	Mechanisms exist to allow individuals to utilize alternative methods of authentication under specific circumstances or situations.	5	
3.PEP.IN.CTLMO	Certificate Transparency Log Monitoring	Certificate transparency log monitoring allows agencies to discover when new certificates are issued for agency domains.	Functional	intersects with	Certificate Monitoring	CRY-12	Automated mechanisms exist to discover when new certificates are issued for organization-controlled domains.	5	
3.PEP.IN.DPLAT	Deception Platforms	Deception platform technologies provide decoy environments, from individual machines to entire networks, that can be used to deflect attacks away from the operational systems supporting agency missions/business functions.	Functional	intersects with	Honeypots	SEA-11	Mechanisms exist to utilize honeypots that are specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting and analyzing such attacks.	5	
3.PEP.IN.EDRES	Endpoint Detection and Response	Endpoint detection and response (EDR) tools combine endpoint and network event data to aid in the detection of malicious activity.	Functional	intersects with	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
3.PEP.IN.IDPSY	Intrusion Detection and Prevention Systems	Intrusion detection systems detect and report malicious activity. Intrusion prevention systems attempt to stop the activity.	Functional	intersects with	Host Intrusion Detection and Prevention Systems (HIDS / HIPS)	END-07	Mechanisms exist to utilize Host-based Intrusion Detection / Prevention Systems (HIDS / HIPS), or similar technologies, to monitor for and protect against anomalous host activity, including lateral movement across the network	5	
3.PEP.IN.NDRES	Network Detection and Response	Network detection and response involves the collection and analysis of network event data to aid in the detection and remediation of malicious activity.	Functional	intersects with	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-08	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	5	
3.PEP.NE.ACONT	Access Control	Access control protections prevent the ingress, egress, or transmission of unauthorized network traffic.	Functional	subset of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
			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	
3.PEP.NE.HCONT	Host Containment	Host containment protections enable a network to revoke or quarantine a host's access to the network.	Functional	intersects with	Host Containment	NET-08.3	Automated mechanisms exist to enforce host containment protections that revoke or quarantine a host's access to the network.	5	
3.PEP.NE.IADEN	Internet Address Denylisting	Internet address denylisting protections prevent the ingest or transiting of traffic received from or destined to a denylisted internet address.	Functional	intersects with	Internet Address Denylisting	NET-18.6	Mechanisms exist to implement Internet address denylisting protections that blocks traffic received from or destined to a denylisted Internet address.	5	
3.PEP.NE.MICRO	Microsegmentation	Microsegmentation divides the network, either physically or virtually, according to the communication needs of application and data workflows, facilitating security controls to protect the data.	Functional	intersects with	Microsegmentation	NET-06.6	Automated mechanisms exist to enable microsegmentation, either physically or virtually, to divide the network according to application and data workflows communications needs.	5	
3.PEP.NE.NSEGM	Network Segmentation (macrosegementation)	Network segmentation separates a given network into subnetworks, facilitating security controls between the subnetworks, and decreasing the attack surface of the network.	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	
3.PEP.NE.RCONT	Resource Containment	Resource containment protections enable removal or quarantine of a resource's access to other resources.	Functional	intersects with	Resource Containment	NET-08.4	Automated mechanisms exist to enforce resource containment protections that remove or quarantine a resource's access to other resources.	5	

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)
3.PEP.RE.DDSPR	Distributed Denial of Service Protections	Distributed Denial of Service (DDoS) protections mitigate the effects of distributed denial of service attacks.	Functional	intersects with	Denial of Service (DoS) Protection	NET-02.1	Automated mechanisms exist to protect against or limit the effects of denial of service attacks.	5	
3.PEP.RE.EEXPS	Elastic Expansion	Elastic expansion enables agencies to dynamically expand the resources available for services as conditions require.	Functional	intersects with	Elastic Expansion	CAP-05	Mechanisms exist to dynamically expand the resources available for services, as demand conditions change.	5	
3.PEP.RE.RDELI	Regional Delivery	Regional delivery technologies enable the deployment of agency services across geographically diverse locations.	Functional	intersects with	Regional Delivery	CAP-06	Mechanisms exist to support operations that are geographically dispersed via regional delivery of technological services.	5	
3.PEP.SE.ACMIT	Active Content Mitigation	Active content mitigation protections detect the presence of unapproved active content and facilitate its removal.	Functional	intersects with	Host Intrusion Detection and Prevention Systems (HIDS / HIPS)	END-07	Mechanisms exist to utilize Host-based Intrusion Detection / Prevention Systems (HIDS / HIPS), or similar technologies, to monitor for and protect against anomalous host activity, including lateral movement across the network	5	
			Functional	intersects with	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
3.PEP.SE.ACONT	Access Control	Access control technologies allow an agency to define policies limiting what actions may be performed by connected users and entities.	Functional	intersects with	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	5	
3.PEP.SE.DLPRE	Data Loss Prevention	DLP technologies detect instances of the exfiltration, either malicious or accidental, of agency data.	Functional	intersects with	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	5	
3.PEP.SE.MCFIL	Malicious Content Filtering	Malicious content filtering protections detect the presence of malicious content and facilitate its removal.	Functional	intersects with	DNS & Content Filtering	NET-18	Mechanisms exist to 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.	5	
3.PEP.SE.PCENF	Protocol Compliance Enforcement	Protocol compliance enforcement technologies ensure that traffic complies with protocol definitions, documented by the Internet Engineering Task Force (IETF).	Functional	intersects with	Protocol Compliance Enforcement	NET-18.4	Automated mechanisms exist to ensure network traffic complies with Internet Engineering Task Force (IETF) protocol specifications.	5	
3.PEP.UN.APPRO	Anti-phishing Protections	Anti-phishing protections detect instances of phishing and prevent users from accessing them.	Functional	intersects with	Phishing & Spam Protection	END-08	Mechanisms exist to utilize anti-phishing and spam protection technologies to detect and take action on unsolicited messages transported by electronic mail.	5	
3.PEP.UN.CTERM	Connection Termination	Connection termination mechanisms ensure the meeting host can positively control participation through inactivity timeouts, on-demand prompts, unique access codes for each meeting, host participant eviction, and even meeting duration limits.	Functional	intersects with	Participant Connection Management	END-14.4	Mechanisms exist to ensure the meeting host can positively control an individual's participation in virtual meetings.	5	
3.PEP.UN.DLPRE	Data Loss Prevention	Mechanisms should be implemented to control the sharing of information between UCC participants, intentional or incidental. This may be integrated into additional agency DLP technologies and can include keyword matching, attachment file type or existence prohibitions, attachment size limitations, or even audio/visual filters.	Functional	intersects with	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	5	
3.PEP.UN.ECOMM	Encrypted Communication	Communication between virtual meeting participants and any data exchanged is encrypted at rest and in transit. Some UCC offerings support end-to-end encryption, where encryption is performed on the clients and can only be decrypted by the other authenticated participants and cannot be decrypted by the UCC vendor.	Functional	intersects with	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
3.PEP.UN.IVERI	Identity Verification	Identity verification ensures that access to the virtual meeting is limited to appropriate individuals. Waiting room features, where the meeting host authorizes vetted individuals to join the meeting, can also be utilized.	Functional	intersects with	Participant Identity Verification	END-14.3	Mechanisms exist to verify individual identities to ensure that access to virtual meetings is limited to appropriate individuals.	5	
3.PEP.UN.LCTPR	Link Click- through Protections	Link click-through protections ensure that when a link in communications is clicked, the requester is directed to a protection that verifies the security of the link destination before permitting access.	Functional	intersects with	Malicious Link & File Protections	END-14.5	Automated mechanisms exist to detect malicious links and/or files in communications and prevent users from accessing those malicious links and/or files.	5	
3.PEP.UN.MFPRO	Malicious File Protections	Malicious file protections detect malicious files in communications and prevent users from accessing them.	Functional	intersects with	Malicious Link & File Protections	END-14.5	Automated mechanisms exist to detect malicious links and/or files in communications and prevent users from accessing those malicious links and/or files.	5	
3.PEP.UN.MLPRO	Malicious Link Protections	Malicious link protections detect malicious links in communications and prevent users from accessing them.	Functional	intersects with	Malicious Link & File Protections	END-14.5	Automated mechanisms exist to detect malicious links and/or files in communications and prevent users from accessing those malicious links and/or files.	5	
3.PEP.WE.ACMIT	Active Content Mitigation	Active content mitigation protections detect the presence of unapproved active content and facilitate its removal.	Functional	intersects with	Host Intrusion Detection and Prevention Systems (HIDS / HIPS)	END-07	Mechanisms exist to utilize Host-based Intrusion Detection / Prevention Systems (HIDS / HIPS), or similar technologies, to monitor for and protect against anomalous host activity, including lateral movement across the network	5	
			Functional	intersects with	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
3.PEP.WE.ACONT	Access Control	Access control technologies allow an agency to define policies limiting what actions may be performed by connected users and entities.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
			Functional	intersects with	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	5	
3.PEP.WE.APROX	Authenticated Proxy	Authenticated proxies require entities to authenticate with the proxy before making use of it, enabling user, group, and location-aware security controls.	Functional	intersects with	Authenticated Proxy	NET-18.8	Mechanisms exist to force systems and processes to authenticate Internet-bound traffic with a proxy to enable user, group and/or location-aware security controls.	5	
3.PEP.WE.BCONT	Bandwidth Control	Bandwidth control technologies allow for limiting the amount of bandwidth used by different classes of domains.	Functional	intersects with	Bandwidth Control	NET-18.7	Mechanisms exist to implement bandwidth control technologies to limit the amount of bandwidth used by categories of domains that are bandwidth-intensive.	5	
3.PEP.WE.BINSP	Break and Inspect	Break and Inspect systems, or encryption proxies, terminate encrypted traffic, logging or performing policy enforcement against the plaintext, and re- encrypting the traffic, if applicable, before transmitting to the final destination.	Functional	intersects with	Visibility of Encrypted Communications	NET-18.2	Mechanisms exist to configure the proxy to make encrypted communications traffic visible to monitoring tools and mechanisms.	5	
3.PEP.WE.CDENY	Certificate Denylisting	Certificate denylisting protections prevent communication with entities that use a set of known bad certificates.	Functional	intersects with	Certificate Denylisting	NET-18.9	Mechanisms exist to prevent communication with systems and/or services that use a set of known bad certificates.	5	
3.PEP.WE.CFILT	Content Filtering	Content filtering protections detect the presence of unapproved content and facilitate its removal or denial of access.	Functional	intersects with	DNS & Content Filtering	NET-18	Mechanisms exist to 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.	5	
3.PEP.WE.DCFIL	Domain Category Filtering	Domain category filtering technologies allow for classes of domains (e.g., banking, medical) to receive a different set of security protections.	Functional	intersects with	DNS & Content Filtering	NET-18	Mechanisms exist to 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.	5	
3.PEP.WE.DLPRE	Data Loss Prevention	DLP technologies detect instances of the exfiltration, either malicious or accidental, of agency data.	Functional	intersects with	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	5	
3.PEP.WE.DREPF	Domain Reputation Filtering	Domain reputation filtering protections are a form of domain denylisting based on a domain's reputation, as defined by either the agency or an external entity.	Functional	intersects with	DNS & Content Filtering	NET-18	Mechanisms exist to 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.	5	
3.PEP.WE.DRESF	Domain Resolution Filtering	Domain resolution filtering prevents entities from using unauthorized DNS resolution services over the DNS-over-Hypertext Transfer Protocol Secure (HTTPS) domain resolution protocol.	Functional	intersects with	DNS & Content Filtering	NET-18	Mechanisms exist to 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.	5	
3.PEP.WE.MCFIL	Malicious Content Filtering	Malicious content filtering protections detect the presence of malicious content and facilitate its removal.	Functional	intersects with	DNS & Content Filtering	NET-18	Mechanisms exist to 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.	5	
3.PEP.WE.PCENF	Protocol Compliance Enforcement	Protocol compliance enforcement technologies ensure that traffic complies with protocol definitions, documented by the Internet Engineering Task Force (IETF).	Functional	intersects with	Protocol Compliance Enforcement	NET-18.4	Automated mechanisms exist to ensure network traffic complies with Internet Engineering Task Force (IETF) protocol specifications.	5	
3.UNI.AACCO	Auditing and Accounting	Auditing and accounting includes capturing business records (e.g., logs and other telemetry), making them available for auditing and accounting as required, and designing an auditing system that considers insider threat (e.g., separation of duties violation tracking) such that insider abuse or misuse can be detected.	Functional	subset of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
			Functional	intersects with	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data privacy and supply chain activities to achieve integrated situational awareness.	5	
			Functional	intersects with	System-Wide / Time-Correlated Audit Trail	MON-02.7	Automated mechanisms exist to compile audit records into an organization-wide audit trail that is time-correlated.	5	
			Functional	intersects with	Content of Event Logs	MON-03	Mechanisms exist to configure systems 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; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5	
			Functional	intersects with	Audit Trails	MON-03.2	Mechanisms exist to link system access to individual users or service accounts.	5	
3.UNI.BRECO	Backup and Recovery	Backup and recovery entails keeping copies of configuration and data, as needed, to allow for the quick restoration of service in the event of malicious incidents, system failures, or corruption.	Functional	intersects with	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
			Functional	intersects with	Retention Of Previous Configurations	CFG-02.3	Mechanisms exist to retain previous versions of baseline configuration to support roll back.	5	
3.UNI.CLMAN	Central Log Management with Analysis	Central log management with analysis is the collection, storage, and analysis of telemetry, where the collection and storage are designed to facilitate data fusion and where the security analysis aids in discovery and response to malicious activity.	Functional	subset of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
			Functional	intersects with	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.	5	
			Functional	intersects with	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM) or similar automated tool, to support the centralized collection of security-related event logs.	5	

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)
3.UNI.CMANA	Configuration Management	Configuration management is the implementation of a formal plan for documenting and managing changes to the environment, and monitoring for deviations, preferably automated.	Functional	subset of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
			Functional	intersects with	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of systems through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	5	
			Functional	subset of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
			Functional	intersects with	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
			Functional	intersects with	Automated Access Enforcement / Auditing	CHG-04.1	Mechanisms exist to perform after-the-fact reviews of configuration change logs to discover any unauthorized changes.	5	
3.UNI.DTDIS	Dynamic Threat Discovery	Dynamic threat discovery is the practice of using dynamic approaches (e.g., heuristics, baselining, etc.) to discover new malicious activity.	Functional	intersects with	Indicators of Compromise (IOC)	IRO-03	Mechanisms exist to define specific Indicators of Compromise (IOC) to identify the signs of potential cybersecurity events.	5	
			Functional	intersects with	Monitoring for Indicators of Compromise (IOC)	MON-11.3	Automated mechanisms exist to identify and alert on Indicators of Compromise (IoC).	5	
			Functional	intersects with	Anomalous Behavior	MON-16	Mechanisms exist to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5	
			Functional	intersects with	Suspicious Communications & Anomalous System Behavior	SAT-03.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.	5	
			Functional	intersects with	Indicators of Exposure (IOE)	THR-02	Mechanisms exist to develop Indicators of Exposure (IOE) to understand the potential attack vectors that attackers could use to attack the organization.	5	
			Functional	intersects with	Behavioral Baselining	THR-11	Automated mechanisms exist to establish behavioral baselines that capture information about user and entity behavior to enable dynamic threat discovery.	5	
3.UNI.ETINT	Enterprise Threat Intelligence Feeds	Enterprise threat intelligence is the usage of threat intelligence from private or government sources to implement mitigations for the identified risks.	Functional	subset of	Threat Intelligence Feeds Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	10	
			Functional	intersects with	Threat Intelligence Feeds Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
3.UNI.EUSSE	Effective Use of Shared Services	Effective use of shared services means that shared services are employed, where applicable, and individually tailored and measured to independently validate service conformance, and offer effective protections for tenants against malicious actors, both external and internal to the service provider.	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	Information In Shared Resources	SEA-05	Mechanisms exist to prevent unauthorized and unintended information transfer via shared system resources.	5	
3.UNI.IDMRP	Integrated Desktop, Mobile, and Remote Policies	This entails the definition and enforcement of policies that apply to a given agency entity independent of its location.	Functional	subset of	Endpoint Security	END-01	Mechanisms exist to facilitate the implementation of endpoint security 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.	5	
3.UNI.INVENT	Inventory	Inventory entails developing, documenting, and maintaining a current inventory of all systems, networks, and components so that only authorized devices are given access, and unauthorized and unmanaged devices are found and restricted from gaining access.	Functional	intersects with	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: (1) Accurately reflects the current systems, applications and services in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5	
			Functional	intersects with	Network Access Control (NAC)	AST-02.5	Automated mechanisms exist to employ Network Access Control (NAC), or a similar technology, which is capable of detecting unauthorized devices and disable network access to those unauthorized devices.	5	
3.UNI.IRPIH	Incident Response Planning and Incident Handling	Incident response planning and incident handling is the documentation and implementation of a set of instructions, procedures, or technical capabilities to sense and detect, respond to, limit consequences of malicious cyberattacks, and restore the integrity of the network and associated systems.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
			Functional	subset of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	10	
			Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
			Functional	intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
3.UNI.LPRIV	Least Privilege	Least privilege is a design principle whereby each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.	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.	5	
3.UNI.PEPAR	Policy Enforcement Parity	Policy enforcement parity entails consistently applying security protections and other policies, independent of the communication mechanism, forwarding path, or endpoints used.	Functional	intersects with	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	5	
			Functional	intersects with	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership.	5	
			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	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
			Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
3.UNI.PMANA	Patch Management	Patch management is the identification, acquisition, installation, and verification of patches for products and systems.	Functional	intersects with	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	5	
3.UNI.RESIL	Resilience	Resilience entails ensuring that systems, services, and protections maintain acceptable performance under adverse conditions.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
			Functional	subset of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	10	
			Functional	intersects with	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for cybersecurity & data privacy principles that addresses risk to organizational operations, assets, individuals, other organizations.	5	
			Functional	intersects with	Defense-In-Depth (DiD) Architecture	SEA-03	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	5	
			Functional	intersects with	Achieving Resilience Requirements	SEA-01.2	Mechanisms exist to achieve resilience requirements in normal and adverse situations.	5	
3.UNI.SADMI	Secure Administration	Secure administration entails performing administrative tasks in a secure manner, using secure protocols.	Functional	subset of	Maintenance Operations	MNT-01	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.	10	
			Functional	intersects with	Remote Maintenance Cryptographic Protection	MNT-05.3	Cryptographic mechanisms exist to protect the integrity and confidentiality of remote, non-local maintenance and diagnostic communications.	5	
			Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	
3.UNI.SAUTH	Strong Authentication	Strong authentication verifies the identity of users, devices, or other entities through rigorous means (e.g., multi-factor authentication) before granting access.	Functional	intersects with	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5	
			Functional	intersects with	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	5	

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	Strong Customer Authentication (SCA)	WEB-06	Mechanisms exist to implement Strong Customer Authentication (SCA) for consumers to reasonably prove their identity.	5	
3.UNI.SAWAR	Situational Awareness	Situational awareness is maintaining effective awareness, both current and historical, across all components.	Functional	subset of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
			Functional	intersects with	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	5	
3.UNI.TSYNC	Time Synchronization	Time synchronization is the coordination of system (e.g., servers, workstations, network devices) clocks to minimize the difference between system clock times and enable accurate comparison of timestamps between systems.	Functional	intersects with	Synchronization With Authoritative Time Source	MON-07.1	Mechanisms exist to synchronize internal system clocks with an authoritative time source.	5	
			Functional	intersects with	Clock Synchronization	SEA-20	Mechanisms exist to utilize time-synchronization technology to synchronize all critical system clocks.	5	
3.UNI.UATRA	User Awareness and Training	User awareness and training entails that all users are informed of their roles and responsibilities and appropriate cybersecurity education is provisioned to enable users to perform their duties in a secure manner.	Functional	subset of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
			Functional	intersects with	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	5	
			Functional	intersects with	Users With Elevated Privileges	HRS-02.1	Mechanisms exist to ensure that every user accessing a system that processes, stores, or transmits sensitive information is cleared and regularly trained to handle the information in question.	5	
			Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
			Functional	intersects with	User Awareness	HRS-03.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.	5	
			Functional	subset of	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
			Functional	intersects with	Cybersecurity & Data Privacy Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	
			Functional	intersects with	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
3.UNI.VMANG	Vulnerability Management	Vulnerability management is the practice of proactively working to discover vulnerabilities by including the use of both active and passive means of discovery and by taking action to mitigate discovered vulnerabilities.	Functional	intersects with	Threat Intelligence Feeds Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
			Functional	subset of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
			Functional	intersects with	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.	5	
			Functional	intersects with	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
3.UNL.CMREP	Continuous Monitoring Reporting	Continuous monitoring reporting entails the maintenance of ongoing awareness of informational security, vulnerabilities, and threats to support organizational risk management decisions.	Functional	subset of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
			Functional	intersects with	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	5	
			Functional	intersects with	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.	5	
			Functional	intersects with	Monitoring Reporting	MON-06	Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.	5	
3.UNL.GPAUD	Governance and Policy Auditing	Governance and policy auditing entails validating the proper definition, application, and enforcement of agency rules and policies.	Functional	subset of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual 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.	5	
3.UNL.RLMAN	Resource Lifecycle Management	Resource lifecycle management is the end-to-end process of managing resources from development to operation to retirement, such that resources are provisioned and decommissioned in conjunction with the applications they support.	Functional	intersects with	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to systems within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
			Functional	intersects with	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of technology assets.	5	
3.UNL.STEXE	Security Test and Exercise	Security tests (e.g., penetration testing or red teaming) verify the extent to which a system resists active attempts to compromise its security. Security exercises are simulations of emergencies that validate and identify gaps in plans and procedures.	Functional	intersects with	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization’s readiness to execute the plan.	5	
			Functional	intersects with	Simulated Incidents	IRO-05.1	Mechanisms exist to incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations.	5	
			Functional	intersects with	Incident Response Testing	IRO-06	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5	
			Functional	intersects with	Application Penetration Testing	TDA-09.5	Mechanisms exist to perform application-level penetration testing of custom-made applications and services.	5	
			Functional	intersects with	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on systems and web applications.	5	
			Functional	intersects with	Red Team Exercises	VPM-10	Mechanisms exist to utilize "red team" exercises to simulate attempts by adversaries to compromise systems and applications in accordance with organization-defined rules of engagement.	5	