NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: USA - TSA Security Directive Pipeline-2021-02F
Focal Document URL: https://www.tsa.gov/sites/default/files/tsa-security-directive-pipeline-2021-02f-and-memo-508c.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-tsa-sd-pipeline-2021-02f.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
I.	Purpose and General Information	TSA is issuing this Security Directive due to the ongoing cybersecurity threat to pipeline systems. The goal is to reduce the risk that cybersecurity threats pose to critical pipeline systems and facilities by implementing layered cybersecurity measures that demonstrate a defense-in-depth approach. Owner/Operators must: (1) establish and implement a TSA-approved Cybersecurity Implementation Plan; (2) develop and maintain an up-to-date Cybersecurity Incident Response Plan; and (3) develop a Cybersecurity Assessment Plan and submit an annual update and annual report. (Summary of requirements detailed in Sections II-III.)	Functional	No Relationship	N/A	N/A	N/A	0		
II.A.1	Applicability, Deadlines for Compliance, and Scope	Covered Pipeline Owner/Operators: This Security Directive applies to Owner/Operators of TSA-designated critical pipeline systems or facilities notified before July 26, 2022, that they are required to comply with the Security Directive Pipeline-2021-02 series.	Functional	No Relationship	N/A	N/A	N/A	0		
II.A.2	N/A	Additional Critical Pipeline Systems or Facilities: If TSA identifies additional Owner/Operators with critical pipeline systems or facilities who were not already subject to the Security Directive Pipeline-2021-02 series, TSA will notify the Owner/Operator and provide specific compliance deadlines for the requirements in this Security Directive.	Functional	No Relationship	N/A	N/A	N/A	0		
II.A.3	N/A	Managed Security Service Providers: If an Owner/Operator has delegated to, or shared responsibility with, a Managed Security Service Provider, wholly or in part, for specific security measures in the Owner/Operator's Cybersecurity Implementation Plan, the Owner/Operator retains sole responsibility under this Security Directive for ensuring compliance with the Owner/Operator's TSA-approved Cybersecurity Implementation Plan and this Security Directive.	Functional	Intersects With	Third-Party Services	TPM-12	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-04
II.A.4	N/A	Authorized Representative: Authorized Representatives are empowered by the Owner/Operator to coordinate and/or conduct activities required by this Security Directive and/or contained within the Owner/Operator's TSA-approved Cybersecurity Implementation Plan. Both Owner/Operators and Authorized Representatives are liable for non-compliance on the part of the Authorized Representative.	Functional	No Relationship	N/A	N/A	N/A	0		
II.A.5	N/A	Scope: The requirements in this Security Directive apply to the covered Owner/Operators' Critical Cyber Systems. Note: If an Owner/Operator determines they have no Critical Cyber Systems, they must notify TSA in writing within 60 days of the effective date. In the event of a change in operations, they must reevaluate whether they have a Critical Cyber System and notify TSA within 60 days of the change.	Functional	Intersects With	Compliance Scope	CPL-03	Mechanisms exist to document and validate the scope of security, compliance and resilience controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	5		CPL-01.2
II.B.1	Cybersecurity Implementation Plan	The Cybersecurity Implementation Plan must provide the information required by Sections III.A. through III.E. of this Security Directive and describe in detail the Owner/Operator's defense-in-depth plan, including physical and logical security controls, for meeting each of the requirements in Sections III.A. through III.E.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	5		GOV-17
II.B.1	Cybersecurity Implementation Plan	The Cybersecurity Implementation Plan must provide the information required by Sections III.A. through III.E. of this Security Directive and describe in detail the Owner/Operator's defense-in-depth plan, including physical and logical security controls, for meeting each of the requirements in Sections III.A. through III.E.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-09	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and (3) Provides a historical record of applied security controls, including changes.	5		IAO-03
II.B.2	N/A	Once approved by TSA, the Owner/Operator must implement and maintain all measures in the TSA-approved Cybersecurity Implementation Plan and meet any schedule stipulated in the plan.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5		CPL-01
III.A	Identification of Critical Cyber Systems	Identify the Owner/Operator's Critical Cyber Systems as defined in Section VII. of this Security Directive. TSA will notify the Owner/Operator if the agency disagrees with the Owner/Operator's determination and may require additional information regarding the methodologies or rationale used to identify Critical Cyber Systems. After consultation, TSA may notify an Owner/Operator that it must include additional Critical Cyber Systems identified by TSA.	Functional	Intersects With	Asset Inventories	AST-04	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (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		AST-02
III.A	Identification of Critical Cyber Systems	Identify the Owner/Operator's Critical Cyber Systems as defined in Section VII. of this Security Directive. TSA will notify the Owner/Operator if the agency disagrees with the Owner/Operator's determination and may require additional information regarding the methodologies or rationale used to identify Critical Cyber Systems. After consultation, TSA may notify an Owner/Operator that it must include additional Critical Cyber Systems identified by TSA.	Functional	Intersects With	Identify Critical Assets	AST-05	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	8		BCD-02
III.A	Identification of Critical Cyber Systems	Identify the Owner/Operator's Critical Cyber Systems as defined in Section VII. of this Security Directive. TSA will notify the Owner/Operator if the agency disagrees with the Owner/Operator's determination and may require additional information regarding the methodologies or rationale used to identify Critical Cyber Systems. After consultation, TSA may notify an Owner/Operator that it must include additional Critical Cyber Systems identified by TSA.	Functional	Intersects With	Technology Assets, Applications, Services and/or Data (TAASD) Ownership Assignment	AST-07.1	Mechanisms exist to ensure Technology Assets, Applications, Services and/or Data (TAASD) ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common understanding of requirements for asset protection.	5		AST-03
III.B	Network Segmentation	Implement network segmentation policies and controls designed to prevent operational disruption to the Operational Technology system if the Information Technology system is compromised or vice versa.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		GOV-02
III.B	Network Segmentation	Implement network segmentation policies and controls designed to prevent operational disruption to the Operational Technology system if the Information Technology system is compromised or vice versa.	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources.	5		NET-06
III.B.1.a	N/A	A list and description of Information Technology and Operational Technology system interdependencies;	Functional	Intersects With	Asset-Service Dependencies	AST-06	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS) that support more than one critical business function.	5		AST-01.1
III.B.1.a	N/A	A list and description of Information Technology and Operational Technology system interdependencies;	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-17	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive and/or regulated data flows.	5		AST-04
III.B.1.a	N/A	A list and description of Information Technology and Operational Technology system interdependencies;	Functional	Intersects With	Sensitive / Regulated Data Access Mapping	DCH-09	Mechanisms exist to leverage data-specific Access Control Lists (ACL) or Interconnection Security Agreements (ISAs) to generate a logical map of the parties with whom sensitive and/or regulated data is shared.	5		DCH-14.3
III.B.1.b	N/A	A list and description of all external connections to the Operational Technology system; and	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-17	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive and/or regulated data flows.	5		AST-04

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: USA - TSA Security Directive Pipeline-2021-02F
Focal Document URL: https://www.tsa.gov/sites/default/files/tsa-security-directive-pipeline-2021-02f-and-memo-508c.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-tsa-sd-pipeline-2021-02f.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
III.B.1.b	N/A	A list and description of all external connections to the Operational Technology system; and	Functional	Intersects With	Interconnection Security Agreements (ISAs)	NET-05	Mechanisms exist to authorize connections from systems to other systems using Interconnection Security Agreements (ISAs), or similar methods, that document, for each interconnection: (1) Interface characteristics; (2) Security, compliance and resilience requirements; and; (3) The nature of the information communicated.	5		NET-05
III.B.1.c	N/A	A list and description of zone boundaries, including a description of how Information Technology and Operational Technology systems are defined and organized into logical zones based on criticality, consequence, and operational necessity.	Functional	Intersects With	Asset Scope Classification	AST-16	Mechanisms exist to determine security, compliance and resilience control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all Technology Assets, Applications and/or Services (TAAS) and personnel (internal and third-parties).	5		AST-04.1
III.B.1.c	N/A	A list and description of zone boundaries, including a description of how Information Technology and Operational Technology systems are defined and organized into logical zones based on criticality, consequence, and operational necessity.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-17	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive and/or regulated data flows.	5		AST-04
III.B.1.c	N/A	A list and description of zone boundaries, including a description of how Information Technology and Operational Technology systems are defined and organized into logical zones based on criticality, consequence, and operational necessity.	Functional	Intersects With	Control Applicability Boundary Graphical Representation	AST-17.1	Mechanisms exist to ensure control applicability is appropriately-determined for Technology Assets, Applications and/or Services (TAAS) and third parties by graphically representing applicable boundaries.	5		AST-04.2
III.B.1.c	N/A	A list and description of zone boundaries, including a description of how Information Technology and Operational Technology systems are defined and organized into logical zones based on criticality, consequence, and operational necessity.	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		NET-03
III.B.1.c	N/A	A list and description of zone boundaries, including a description of how Information Technology and Operational Technology systems are defined and organized into logical zones based on criticality, consequence, and operational necessity.	Functional	Intersects With	Sensitive / Regulated Data Enclave (Secure Zone)	NET-08.1	Mechanisms exist to implement segmentation controls to restrict inbound and outbound connectivity for sensitive and/or regulated data enclaves (secure zones).	5		NET-06.3
III.B.2	N/A	An identification and description of measures for securing and defending zone boundaries, that includes security controls-	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		NET-03
III.B.2.a	N/A	Security controls to prevent unauthorized communications between zones; and	Functional	Intersects With	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	5		NET-04
III.B.2.a	N/A	Security controls to prevent unauthorized communications between zones; and	Functional	Intersects With	Sensitive / Regulated Data Enclave (Secure Zone)	NET-08.1	Mechanisms exist to implement segmentation controls to restrict inbound and outbound connectivity for sensitive and/or regulated data enclaves (secure zones).	5		NET-06.3
III.B.2.b	N/A	Security controls to prohibit Operational Technology system services from traversing the Information Technology system, unless the content of the Operational Technology system is encrypted while in transit.	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03
III.B.2.b	N/A	Security controls to prohibit Operational Technology system services from traversing the Information Technology system, unless the content of the Operational Technology system is encrypted while in transit.	Functional	Intersects With	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	5		NET-04
III.C	Access Control Measures	Implement access control measures, including for local and remote access, to secure and prevent unauthorized access to Critical Cyber Systems.	Functional	Intersects With	Configuration Management Program	CFG-02	Mechanisms exist to facilitate the implementation of configuration management controls.	5		CFG-01
III.C	Access Control Measures	Implement access control measures, including for local and remote access, to secure and prevent unauthorized access to Critical Cyber Systems.	Functional	Intersects With	Identity & Access Management (IAM)	IAC-02	Mechanisms exist to facilitate the implementation of Identification and Access Management (IAM) controls.	5		IAC-01
III.C	Access Control Measures	Implement access control measures, including for local and remote access, to secure and prevent unauthorized access to Critical Cyber Systems.	Functional	Intersects With	Physical & Environmental Protections	PES-02	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	5		PES-01
III.C.1	N/A	Identification and authentication policies and procedures designed to prevent unauthorized access to Critical Cyber Systems that include-	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		GOV-02
III.C.1	N/A	Identification and authentication policies and procedures designed to prevent unauthorized access to Critical Cyber Systems that include-	Functional	Intersects With	Identification & Authentication Policy	IAC-01	Mechanisms exist to establish a formal, documented identification and authentication policy that: (1) Conveys executive management's intent; (2) Provides organizational direction and expected behaviors; (3) Is reviewed at least annually; and (4) Is updated, as necessary, to adapt to evolving risks, threats and other changes that affect the organization.	8		
III.C.1	N/A	Identification and authentication policies and procedures designed to prevent unauthorized access to Critical Cyber Systems that include-	Functional	Intersects With	Identity & Access Management (IAM)	IAC-02	Mechanisms exist to facilitate the implementation of Identification and Access Management (IAM) controls.	5		IAC-01
III.C.1	N/A	Identification and authentication policies and procedures designed to prevent unauthorized access to Critical Cyber Systems that include-	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-04	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	8		OPS-01.1
III.C.1.a	N/A	A schedule for memorized secret authenticator resets; and	Functional	Intersects With	Password-Based Authentication	IAC-15	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5		IAC-10.1
III.C.1.b	N/A	Documented and defined mitigation measures for components of Critical Cyber Systems that will not have passwords reset in accordance with the schedule required by the preceding subparagraph (III.C.1.a.) and a timeframe to complete these mitigations.	Functional	Intersects With	Compensating Countermeasures	RSK-18	Mechanisms exist to identify and implement one, or more, compensating controls to reduce risk and threat exposure when the primary means of implementing the security function is unavailable or compromised.	5		RSK-06.2
III.C.2	N/A	Multi-factor authentication, or other logical and physical security controls that supplement password authentication to provide risk mitigation commensurate to multi-factor authentication. If an Owner/Operator does not apply multi-factor authentication for access to industrial control workstations in control rooms regulated under 49 CFR parts 192 or 195, the Owner/Operator shall specify what compensating controls are used to manage access.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5		IAC-06
III.C.2	N/A	Multi-factor authentication, or other logical and physical security controls that supplement password authentication to provide risk mitigation commensurate to multi-factor authentication. If an Owner/Operator does not apply multi-factor authentication for access to industrial control workstations in control rooms regulated under 49 CFR parts 192 or 195, the Owner/Operator shall specify what compensating controls are used to manage access.	Functional	Intersects With	Compensating Countermeasures	RSK-18	Mechanisms exist to identify and implement one, or more, compensating controls to reduce risk and threat exposure when the primary means of implementing the security function is unavailable or compromised.	5		RSK-06.2
III.C.3	N/A	Policies and procedures to manage access rights based on the principles of least privilege and separation of duties. Where not technically feasible to apply these principles, the policies and procedures must describe the compensating controls that the Owner/Operator will apply.	Functional	Intersects With	Least Privilege	IAC-30	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		IAC-21
III.C.3	N/A	Policies and procedures to manage access rights based on the principles of least privilege and separation of duties. Where not technically feasible to apply these principles, the policies and procedures must describe the compensating controls that the Owner/Operator will apply.	Functional	Intersects With	Compensating Countermeasures	RSK-18	Mechanisms exist to identify and implement one, or more, compensating controls to reduce risk and threat exposure when the primary means of implementing the security function is unavailable or compromised.	5		RSK-06.2
III.C.4	N/A	Enforcement of standards that limit availability and use of shared accounts to those that are critical for operations, and then only if absolutely necessary.	Functional	Intersects With	Restrictions on Shared Groups / Accounts	IAC-21	Mechanisms exist to authorize the use of shared/group accounts only under certain organization-defined conditions.	5		IAC-15.5

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: USA - TSA Security Directive Pipeline-2021-02F
Focal Document URL: https://www.tsa.gov/sites/default/files/tsa-security-directive-pipeline-2021-02f-and-memo-508c.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-tsa-sd-pipeline-2021-02f.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legecy SCF #
III.C.4	N/A	Enforcement of standards that limit availability and use of shared accounts to those that are critical for operations, and then only if absolutely necessary.	Functional	Intersects With	Credential Sharing	IAC-23	Mechanisms exist to prevent the sharing of generic IDs, passwords or other generic authentication methods.	5		IAC-19
III.C.4.a	N/A	When the Owner/Operator uses shared accounts for operational purposes, the policies and procedures must ensure access to shared accounts is limited through account management that uses principles of least privilege and separation of duties; and	Functional	Intersects With	Restrictions on Shared Groups / Accounts	IAC-21	Mechanisms exist to authorize the use of shared/group accounts only under certain organization-defined conditions.	5		IAC-15.5
III.C.4.a	N/A	When the Owner/Operator uses shared accounts for operational purposes, the policies and procedures must ensure access to shared accounts is limited through account management that uses principles of least privilege and separation of duties; and	Functional	Intersects With	Least Privilege	IAC-30	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	5		IAC-21
III.C.4.b	N/A	Individuals who no longer need access do not have knowledge of the password necessary to access the shared account.	Functional	Intersects With	Restrictions on Shared Groups / Accounts	IAC-21	Mechanisms exist to authorize the use of shared/group accounts only under certain organization-defined conditions.	5		IAC-15.5
III.C.4.b	N/A	Individuals who no longer need access do not have knowledge of the password necessary to access the shared account.	Functional	Intersects With	Credential Sharing	IAC-23	Mechanisms exist to prevent the sharing of generic IDs, passwords or other generic authentication methods.	5		IAC-19
III.C.5	N/A	Schedule for review of existing domain trust relationships to ensure their necessity and policies to manage domain trusts.	Functional	Intersects With	Identity & Access Management (IAM)	IAC-02	Mechanisms exist to facilitate the implementation of Identification and Access Management (IAM) controls.	5		IAC-01
III.C.5	N/A	Schedule for review of existing domain trust relationships to ensure their necessity and policies to manage domain trusts.	Functional	Intersects With	Cross Domain Solution (CDS)	NET-41	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	5		NET-02.3
III.D	Continuous Monitoring and Detection	Implement continuous monitoring and detection policies and procedures that are designed to prevent, detect, and respond to cybersecurity threats and anomalies affecting Critical Cyber Systems.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		GOV-02
III.D	Continuous Monitoring and Detection	Implement continuous monitoring and detection policies and procedures that are designed to prevent, detect, and respond to cybersecurity threats and anomalies affecting Critical Cyber Systems.	Functional	Intersects With	Continuous Monitoring Policy	MON-01	Mechanisms exist to establish a formal, documented continuous monitoring policy that: (1) Conveys executive management's intent;	5		
III.D	Continuous Monitoring and Detection	Implement continuous monitoring and detection policies and procedures that are designed to prevent, detect, and respond to cybersecurity threats and anomalies affecting Critical Cyber Systems.	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5		MON-01
III.D.1.a	N/A	Capabilities to prevent malicious email, such as spam and phishing emails, from adversely impacting operations;	Functional	Intersects With	Endpoint Protection Mechanisms	END-03	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	8		END-02
III.D.1.a	N/A	Capabilities to prevent malicious email, such as spam and phishing emails, from adversely impacting operations;	Functional	Intersects With	Phishing & Spam Protection	NET-40.2	Mechanisms exist to utilize anti-phishing and spam protection technologies to detect and take action on unsolicited messages transported by electronic mail.	5		END-08
III.D.1.b	N/A	Capabilities to prohibit ingress and egress communications with known or suspected malicious Internet Protocol addresses;	Functional	Intersects With	DNS & Content Filtering	NET-17	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		NET-18
III.D.1.b	N/A	Capabilities to prohibit ingress and egress communications with known or suspected malicious Internet Protocol addresses;	Functional	Intersects With	Route Internal Traffic to Proxy Servers	NET-18.1	Mechanisms exist to route internal communications traffic to external networks through organization-approved proxy servers at managed interfaces.	5		NET-18.1
III.D.1.c	N/A	Capabilities to control impact of known or suspected malicious web domains or web applications, such as by preventing users and devices from accessing malicious websites;	Functional	Intersects With	DNS & Content Filtering	NET-17	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		NET-18
III.D.1.d	N/A	Capabilities to block and prevent unauthorized code, including macro scripts, from executing; and	Functional	Intersects With	Role-Based Permissions To Implement Changes	CHG-04.2	Mechanisms exist to limit the ability to implement Technology Asset, Application and/or Service (TAAS) changes to designated privileged roles.	5		END-03
III.D.1.d	N/A	Capabilities to block and prevent unauthorized code, including macro scripts, from executing; and	Functional	Intersects With	Mobile Code	END-13	Mechanisms exist to address mobile code / operating system-independent applications.	5		END-10
III.D.1.e	N/A	Capabilities to monitor and/or block connections from known or suspected malicious command and control servers (such as Tor exit nodes, and other anonymization services).	Functional	Intersects With	DNS & Content Filtering	NET-17	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		NET-18
III.D.2.a	N/A	Procedures to audit unauthorized access to internet domains and addresses;	Functional	Intersects With	Inbound & Outbound Communications Traffic	MON-22	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	5		MON-01.3
III.D.2.a	N/A	Procedures to audit unauthorized access to internet domains and addresses;	Functional	Intersects With	DNS & Content Filtering	NET-17	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		NET-18
III.D.2.b	N/A	Procedures to document and audit any communications between the Operational Technology system and an external system that deviates from the Owner/Operator's identified baseline of communications;	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5		MON-16
III.D.2.b	N/A	Procedures to document and audit any communications between the Operational Technology system and an external system that deviates from the Owner/Operator's identified baseline of communications;	Functional	Intersects With	Inbound & Outbound Communications Traffic	MON-22	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	5		MON-01.3
III.D.2.c	N/A	Procedures to identify and respond to execution of unauthorized code, including macro scripts; and	Functional	Intersects With	Unauthorized Software Installation Alerts	CHG-12	Automated mechanisms exist to generate an alert upon the detection of an unauthorized software installation.	5		CFG-05.1
III.D.2.c	N/A	Procedures to identify and respond to execution of unauthorized code, including macro scripts; and	Functional	Intersects With	Malicious Code Protection (Antimalware)	END-04	Mechanisms exist to utilize antimalware, or similar technologies, to detect and eradicate malicious code.	5		END-04
III.D.2.d	N/A	Procedures to implement capabilities (such as Security, Orchestration, Automation, and Response) to define, prioritize, and drive standardized incident response activities.	Functional	Intersects With	Incident Response Operations	IRO-02	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	5		IRO-01
III.D.2.d	N/A	Procedures to implement capabilities (such as Security, Orchestration, Automation, and Response) to define, prioritize, and drive standardized incident response activities.	Functional	Intersects With	Incident Handling	IRO-06	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		IRO-02
III.D.2.d	N/A	Procedures to implement capabilities (such as Security, Orchestration, Automation, and Response) to define, prioritize, and drive standardized incident response activities.	Functional	Intersects With	Security Orchestration, Automation, and Response (SOAR)	OPS-08	Mechanisms exist to utilize Security Orchestration, Automation and Response (SOAR) tools to define, prioritize and automate the response to security incidents.	5		OPS-06
III.D.3.a	N/A	Logging policies that require continuous collection and analyzing of data for potential intrusions and anomalous behavior; and	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5		MON-01
III.D.3.a	N/A	Logging policies that require continuous collection and analyzing of data for potential intrusions and anomalous behavior; and	Functional	Intersects With	Content of Event Logs	MON-09	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (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		MON-03

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: USA - TSA Security Directive Pipeline-2021-02F
Focal Document URL: https://www.tsa.gov/sites/default/files/tsa-security-directive-pipeline-2021-02f-and-memo-508c.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-tsa-sd-pipeline-2021-02f.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
III.D.3.b	N/A	Logging policies that ensure data is maintained for sufficient periods to allow for effective investigation of cybersecurity incidents.	Functional	Intersects With	Event Log & Security-Relevant Telemetry Retention	MON-13	Mechanisms exist to retain event logs and security-relevant telemetry for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	5		MON-10
III.D.4	N/A	Mitigation measures or manual controls to ensure industrial control systems can be isolated when a cybersecurity incident in the Information Technology system creates risk to the safety and reliability of the Operational Technology system.	Functional	Intersects With	Isolation of System Components	NET-42.1	Mechanisms exist to employ boundary protections to isolate Technology Assets, Applications and/or Services (TAAS) that support critical missions and/or business functions.	5		NET-03.7
III.D.4	N/A	Mitigation measures or manual controls to ensure industrial control systems can be isolated when a cybersecurity incident in the Information Technology system creates risk to the safety and reliability of the Operational Technology system.	Functional	Intersects With	Compensating Countermeasures	RSK-18	Mechanisms exist to identify and implement one, or more, compensating controls to reduce risk and threat exposure when the primary means of implementing the security function is unavailable or compromised.	5		RSK-06.2
III.E	Patch Management	Reduce the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers, and firmware on Critical Cyber Systems consistent with the Owner/Operator's risk-based methodology.	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-02	Mechanisms exist to facilitate the implementation and monitoring of risk-based vulnerability management capabilities.	5		VPM-01
III.E.1	N/A	A patch management strategy that ensures all critical security patches and updates on Critical Cyber Systems are current.	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-02	Mechanisms exist to facilitate the implementation and monitoring of risk-based vulnerability management capabilities.	5		VPM-01
III.E.1	N/A	A patch management strategy that ensures all critical security patches and updates on Critical Cyber Systems are current.	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		VPM-05
III.E.2.a	N/A	The strategy must include the risk methodology for categorizing and determining criticality of patches and updates, and an implementation timeline based on categorization and criticality; and	Functional	Intersects With	Vulnerability Remediation Process	VPM-06	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5		VPM-02
III.E.2.a	N/A	The strategy must include the risk methodology for categorizing and determining criticality of patches and updates, and an implementation timeline based on categorization and criticality; and	Functional	Intersects With	Time To Remediate / Benchmarks For Corrective Action	VPM-07	Mechanisms exist to track the effectiveness of remediation operations through metrics reporting.	5		VPM-05.3
III.E.2.b	N/A	Prioritization of all security patches and updates on CISA's Known Exploited Vulnerabilities Catalog.	Functional	Intersects With	Vulnerability Ranking	VPM-05	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	5		VPM-03
III.E.3	N/A	If the Owner/Operator cannot apply patches and updates on specific Operational Technology systems without causing a severe degradation of operational capability to meet business critical functions, the patch management strategy must include a description and timeline of additional mitigations that address the risk created by not installing the patch or update.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-12	Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum: (1) Deficiency tracking number; (2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection; (6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner); (8) Resources required to conduct remediation actions; (9) Planned remedial actions to the deficiency(ies); (10) Proposed remediation timeline; and (11) Disposition statement (e.g., closeout summary).	5		IAO-05
III.E.3	N/A	If the Owner/Operator cannot apply patches and updates on specific Operational Technology systems without causing a severe degradation of operational capability to meet business critical functions, the patch management strategy must include a description and timeline of additional mitigations that address the risk created by not installing the patch or update.	Functional	Intersects With	Compensating Countermeasures	RSK-18	Mechanisms exist to identify and implement one, or more, compensating controls to reduce risk and threat exposure when the primary means of implementing the security function is unavailable or compromised.	5		RSK-06.2
III.F.1	Cybersecurity Incident Response Plan	Owner/Operators must have an up-to-date Cybersecurity Incident Response Plan for the Critical Cyber Systems that include measures to reduce the risk of operational disruption, or the risk of other significant impacts on business critical functions should the covered pipeline or facility experience a cybersecurity incident.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-08	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	8		IRO-04
III.F.1.a	N/A	Prompt containment of the infected server or device.	Functional	Intersects With	Incident Handling	IRO-06	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		IRO-02
III.F.1.b	N/A	Segregation of the infected network (or devices) to ensure malicious code does not spread by, as necessary: (i) segregating (removing from the network) the infected device(s); (ii) segregating any other devices that shared a network with the infected device(s); (iii) preserving volatile memory by collecting a forensic memory image of affected device(s) before powering off or moving; and (iv) isolating and securing all infected and potentially infected devices, making sure to clearly label any equipment that has been affected by malicious code.	Functional	Intersects With	Incident Handling	IRO-06	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		IRO-02
III.F.1.b	N/A	Segregation of the infected network (or devices) to ensure malicious code does not spread by, as necessary: (i) segregating (removing from the network) the infected device(s); (ii) segregating any other devices that shared a network with the infected device(s); (iii) preserving volatile memory by collecting a forensic memory image of affected device(s) before powering off or moving; and (iv) isolating and securing all infected and potentially infected devices, making sure to clearly label any equipment that has been affected by malicious code.	Functional	Intersects With	Chain of Custody & Forensics	IRO-13	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	5		IRO-08
III.F.1.c	N/A	Security and integrity of backed-up data, including measures to secure backups, store backup data separate from the system, and procedures to ensure that the backup data is free of known malicious code when the backup is made and when tested for restoral.	Functional	Intersects With	Resilient Data Backup Architecture	BCD-23	Mechanisms exist to maintain a secure, immutable backup architecture.	5		
III.F.1.c	N/A	Security and integrity of backed-up data, including measures to secure backups, store backup data separate from the system, and procedures to ensure that the backup data is free of known malicious code when the backup is made and when tested for restoral.	Functional	Intersects With	Data Backups	BCD-24	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 satisfy Recovery Time	5		BCD-11
III.F.1.c	N/A	Security and integrity of backed-up data, including measures to secure backups, store backup data separate from the system, and procedures to ensure that the backup data is free of known malicious code when the backup is made and when tested for restoral.	Functional	Intersects With	Data Backup & Restoration Hardware Protection	BCD-31	Mechanisms exist to protect data backup and restoration hardware and software.	5		BCD-13
III.F.1.d	N/A	Established capability and governance for isolating the Information and Operational Technology systems in the event of a cybersecurity incident that results or could result in operational disruption.	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources.	5		NET-06
III.F.1.d	N/A	Established capability and governance for isolating the Information and Operational Technology systems in the event of a cybersecurity incident that results or could result in operational disruption.	Functional	Intersects With	Isolation of System Components	NET-42.1	Mechanisms exist to employ boundary protections to isolate Technology Assets, Applications and/or Services (TAAS) that support critical missions and/or business functions.	5		NET-03.7
III.F.1.e	N/A	Exercises to test the effectiveness of procedures, and personnel responsible for implementing measures, in this Cybersecurity Incident Response Plan, no less than annually. These exercises must: (i) test at least two objectives of the Owner/Operator's Cybersecurity Incident Response Plan required by subparagraphs F.1.a. through F.1.d., no less than annually; and (ii) include the employees identified (by position) in paragraph F.2 as active participants in the exercises.	Functional	Intersects With	Incident Response Capabilities Testing	IRO-09	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5		IRO-06

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: USA - TSA Security Directive Pipeline-2021-02F
Focal Document URL: https://www.tsa.gov/sites/default/files/tsa-security-directive-pipeline-2021-02f-and-memo-508c.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-tsa-sd-pipeline-2021-02f.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
III.F.2	N/A	The Cybersecurity Incident Response Plan must identify who (by position) is responsible for implementing the specific measures in the Incident Response Plan and any necessary resources needed to implement the measures.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-08	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5		IRO-04
III.F.2	N/A	The Cybersecurity Incident Response Plan must identify who (by position) is responsible for implementing the specific measures in the Incident Response Plan and any necessary resources needed to implement the measures.	Functional	Intersects With	Integrated Security Incident Response Team (ISIRT)	IRO-11	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations.	5		IRO-07
III.G.1	Cybersecurity Assessment Plan	The Owner/Operator must develop a Cybersecurity Assessment Plan for proactively assessing Critical Cyber Systems to ascertain the effectiveness of cybersecurity measures and to identify and resolve device, network, and/or system vulnerabilities.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-02	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10		IAO-01
III.G.2.a	N/A	The Cybersecurity Assessment Plan must assess the effectiveness of the Owner/Operator's TSA-approved Cybersecurity Implementation Plan;	Functional	Intersects With	Control Validation Testing (CVT)	IAO-04	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5		IAO-02
III.G.2.b	N/A	Include a cybersecurity architecture design review at least once every two years that includes verification and validation of network traffic and system log review and analysis to identify cybersecurity vulnerabilities related to network design, configuration, and inter-connectivity to internal and external systems;	Functional	Intersects With	Control Validation Testing (CVT)	IAO-04	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5		IAO-02
III.G.2.c	N/A	Incorporate other assessment capabilities, such as penetration testing of Information Technology systems and the use of "red" and "purple" team (adversarial perspective) testing;	Functional	Intersects With	Penetration Testing	VPM-18	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5		VPM-07
III.G.2.c	N/A	Incorporate other assessment capabilities, such as penetration testing of Information Technology systems and the use of "red" and "purple" team (adversarial perspective) testing;	Functional	Intersects With	Red Team Exercises	VPM-21	Mechanisms exist to utilize "red team" exercises to simulate attempts by adversaries to compromise Technology Assets, Applications and/or Services (TAAS) in accordance with organization-defined rules of engagement.	5		VPM-10
III.G.2.d	N/A	Include a schedule for assessing and auditing specific cybersecurity measures and/or actions required by subparagraphs G.2.a. through G.2.c. The schedule must ensure at least one-third (1/3) of the policies, procedures, measures, and capabilities in the TSA-approved Cybersecurity Implementation Plan are assessed each year, with 100 percent assessed over any three-year period; and	Functional	Intersects With	Control Validation Testing (CVT)	IAO-04	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5		IAO-02
III.G.2.e	N/A	Ensure a Cybersecurity Assessment Plan annual report of the results of assessments conducted in accordance with the Plan is submitted to TSA as described in paragraph G.4. The required report must indicate: (i) for the previous 12 months, which assessment method(s) were used to determine whether the policies, procedures, and capabilities described by the Owner/Operator in its Cybersecurity Implementation Plan are effective; and (ii) results of the individual assessments conducted in the previous 12 months.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	5		GOV-17
III.G.2.e	N/A	Ensure a Cybersecurity Assessment Plan annual report of the results of assessments conducted in accordance with the Plan is submitted to TSA as described in paragraph G.4. The required report must indicate: (i) for the previous 12 months, which assessment method(s) were used to determine whether the policies, procedures, and capabilities described by the Owner/Operator in its Cybersecurity Implementation Plan are effective; and (ii) results of the individual assessments conducted in the previous 12 months.	Functional	Intersects With	Assessment Boundaries	IAO-03	Mechanisms exist to establish the scope of assessments by defining the assessment boundary, according to people, processes and technology that directly or indirectly impact the confidentiality, integrity, availability and safety of the Technology Assets, Applications, Services and/or Data (TAASD) under review.	5		IAO-01.1
III.G.3	N/A	The Owner/Operator must submit its Cybersecurity Assessment Plan on an annual basis to TSA for approval. The Cybersecurity Assessment Plan must be submitted to TSA no later than 12 months from the date of TSA's approval of the Owner/Operator's previous Cybersecurity Assessment Plan.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	5		GOV-17
III.G.4	N/A	The Owner/Operator must submit the Cybersecurity Assessment Plan report required by section G.2.e. to TSA no later than 12 months from the date of TSA's approval of the most recent Cybersecurity Assessment Plan.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	5		GOV-17
IV.A	Records	Use of previous plans, assessments, tests, and evaluations. As applicable, Owner/Operators may use previously developed plans, assessments, tests, and evaluations to meet the requirements of this Security Directive. If the Owner/Operator relies on these materials, they must include an index of the records and their location organized in the same sequence as the requirements in this Security Directive. In addition, these materials must be explicitly incorporated by reference into the Cybersecurity Implementation Plan and made available to TSA upon request.	Functional	Intersects With	Ability To Demonstrate Conformity	CPL-04	Mechanisms exist to ensure the organization is able to demonstrate security, compliance and/or resilience capability conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	3		CPL-01.3
IV.B	N/A	Protection of sensitive security information. The Owner/Operator must, at a minimum, store and transmit the following information required by this Security Directive consistent with the requirements in 49 CFR part 1520: (1) plans and reports; and (2) audit, testing, or assessment results.	Functional	Intersects With	Data Protection	DCH-02	Mechanisms exist to facilitate the implementation of data protection controls.	5		DCH-01
IV.C.1	N/A	The Owner/Operator must make records necessary to establish compliance with the requirements of this Security Directive available to TSA upon request for inspection and/or copying.	Functional	Intersects With	Ability To Demonstrate Conformity	CPL-04	Mechanisms exist to ensure the organization is able to demonstrate security, compliance and/or resilience capability conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	5		CPL-01.3
IV.C.1	N/A	The Owner/Operator must make records necessary to establish compliance with the requirements of this Security Directive available to TSA upon request for inspection and/or copying.	Functional	Intersects With	Assessor Access	CPL-10	Mechanisms exist to grant assessors minimum necessary access to conduct conformity assessments, including: (1) Logical access to design, development, production, inspection and testing artifacts; and (2) Physical access to facilities.	5		CPL-03.3
IV.C.2	N/A	TSA may request to inspect or copy the following documents to establish compliance with this Security Directive: (a) hardware/software asset inventory, including supervisory control, and data acquisition systems; (b) firewall rules; (c) network diagrams, switch and router configurations, architecture diagrams, publicly routable internet protocol addresses, and Virtual Local Area Networks; (d) policy, procedural, and other documents that informed the development, and documented implementation of, the Owner/Operator's Cybersecurity Implementation Plan, Cybersecurity Incident Response Plan, Cybersecurity Assessment Plan, and assessment or audit results; (e) data providing a "snapshot" of activity on and between Information and Operational Technology systems, such as log files, packet captures, "East-West Traffic" and "North-South Traffic"; and (f) any other records or documents necessary to	Functional	Intersects With	Assessor Access	CPL-10	Mechanisms exist to grant assessors minimum necessary access to conduct conformity assessments, including: (1) Logical access to design, development, production, inspection and testing artifacts; and (2) Physical access to facilities.	5		CPL-03.3
V.A.1	Procedures for Security Directives	Confirm Receipt. Immediately provide written confirmation of receipt of this Security Directive via e-mail to TSA at SurfOps-SD@tsa.dhs.gov;	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	5		GOV-17

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **USA - TSA Security Directive Pipeline-2021-02F**
Focal Document URL: https://www.tsa.gov/sites/default/files/tsa-security-directive-pipeline-2021-02f-and-memo-508c.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-tsa-sd-pipeline-2021-02f.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legecy SCF #
V.A.2	N/A	Dissemination. Immediately disseminate the information and measures in this Security Directive to corporate senior management and security management representatives. The Owner/Operator must provide the applicable security measures in this Security Directive to the Owner/Operator's direct employees and authorized representatives responsible for implementing applicable security measures as necessary to ensure compliance.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	5		GOV-17
V.A.2	N/A	Dissemination. Immediately disseminate the information and measures in this Security Directive to corporate senior management and security management representatives. The Owner/Operator must provide the applicable security measures in this Security Directive to the Owner/Operator's direct employees and authorized representatives responsible for implementing applicable security measures as necessary to ensure compliance.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		GOV-02
V.B	N/A	Comments. Owner/Operators may comment on this Security Directive by submitting data, views, or arguments in writing to TSA via e-mail. Any comments referring to specific measures must be protected in accordance with the requirements in 49 CFR part 1520. Submission of a comment does not delay the effective date of the Security Directive.	Functional	No Relationship	N/A	N/A	N/A	0		
V.C	N/A	Submission of Documentation to TSA. Owner/Operators are required to submit documents in a manner prescribed by TSA. TSA will provide Owner/Operators specific instructions for submission of required documents.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	5		GOV-17
VI.A	Amendments to Cybersecurity Implementation Plan	Changes to ownership or control of operations. An Owner/Operator required to submit a Cybersecurity Implementation Plan under Section II.B. must submit a request to amend its Cybersecurity Implementation Plan if, after approval, there are any changes to the ownership or control of the operation.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	5		GOV-17
VI.B	N/A	Changes to conditions affecting security. An Owner/Operator must submit a request to amend its Cybersecurity Implementation Plan if, after approval, the Owner/Operator makes, or intends to make, permanent changes to the policies, procedures, or measures approved by TSA, including changes to address: (1) determinations that a specific policy, procedure, or measure in the Cybersecurity Implementation Plan is ineffective based on results of the audits and assessments required under Section III.G.; or (2) the Owner/Operator has identified or obtained new or additional capabilities for meeting the requirements in the Security Directive that have not been previously approved by TSA.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	5		GOV-17
VI.C	N/A	Permanent change. For purposes of this section, a "permanent change" is one intended to be in effect for 45 or more calendar days.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	5		GOV-17
VI.D	N/A	Schedule for requesting amendment. The Owner/Operator must file the request for an amendment to its Cybersecurity Implementation Plan with TSA no later than 50 calendar days after the permanent change takes effect, unless TSA allows a longer time period.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	5		GOV-17
VI.E	N/A	TSA approval. TSA may approve a requested amendment to a Cybersecurity Implementation Plan if TSA determines that it is in the interest of the public and transportation security and the proposed amendment provides the level of security required under this Security Directive. TSA may request additional information from the Owner/Operator before rendering a decision.	Functional	No Relationship	N/A	N/A	N/A	0		
VI.F	N/A	Petition for reconsideration. No later than 30 calendar days after receiving a denial of an amendment to a Cybersecurity Implementation Plan, the Owner/Operator may file a petition for reconsideration following the procedures in 49 CFR 1570.119.	Functional	No Relationship	N/A	N/A	N/A	0		
VII.	Definitions	(see definitions section)	Functional	Intersects With	Standardized Terminology	GOV-03.2	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	5		SEA-02.1