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

Reference document: Secure Controls Framework (SCF) version 2026.1
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: TSA Security Directive 1580/82-2022-01 - Rail Cybersecurity Mitigation Actions and Testing
Focal Document URL: https://www.tsa.gov/sites/default/files/sd-1580-82-2022-01.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-tsa-security-directive-1580-82-2022-01.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
I	PURPOSE AND GENERAL INFORMATION	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
II	ACTIONS REQUIRED	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
II.A	Applicability, Deadlines for Compliance, and Scope	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
II.A.1	Applicability	The provisions of this Security Directive apply to the following Owner/Operators:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
II.A.1.a	Applicability	Freight Railroad Owner/Operators subject to applicability described in 49 CFR 1580.101.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
II.A.1.b	Other TSA-designated Freight and Passenger Railroad Owner/Operators:	This Security Directive also applies to Owner/Operators of railroads designated by TSA. TSA will notify these Owner/Operator(s) and provide specific compliance deadlines for the requirements in this Security Directive.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
II.A.2	Scope	The requirements in this Security Directive apply to Critical Cyber Systems of TSA-designated freight and passenger railroads. Note: If an Owner/Operator determines they have no Critical Cyber Systems, as defined in Section VII of this Security Directive, they must notify TSA in writing within 60 days of the effective date of this Security Directive. In the event that an Owner/Operator's method of operation changes, they must reevaluate whether they have a Critical Cyber System, and if so, the requirements of this Security Directive are applicable.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
II.B	Cybersecurity Implementation Plan	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
II.B.1	Cybersecurity Implementation Plan	No later than 120 days after the effective date of this Security Directive, Owner/Operators must submit a Cybersecurity Implementation Plan to SurfOpsSD@tsa.dhs.gov for TSA approval.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	GOV-17	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	
II.B.2	Cybersecurity Implementation Plan	The Cybersecurity Implementation Plan must provide all 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	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
II.B.3	Cybersecurity Implementation Plan	Once approved by TSA, the Owner/Operator must implement and maintain all measures in the TSA-approved Cybersecurity Implementation Plan in accordance with the schedule as stipulated in the plan.	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	
III	CYBERSECURITY MEASURES	The Owner/Operator must:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
III.A	CYBERSECURITY MEASURES	Identify the Owner/Operator's Critical Cyber Systems as defined in Section VII of this Security Directive.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
III.A	CYBERSECURITY MEASURES	Identify the Owner/Operator's Critical Cyber Systems as defined in Section VII of this Security Directive.	Functional	Intersects With	Asset Ownership Assignment	AST-03	Mechanisms exist to ensure asset 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	
III.B	CYBERSECURITY MEASURES	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. As applied to Critical Cyber Systems, these policies and controls must include:	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8	
III.B	CYBERSECURITY MEASURES	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. As applied to Critical Cyber Systems, these policies and controls must include:	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for each Technology Asset, Application and/or Service (TAAS) under their control.	8	
III.B	CYBERSECURITY MEASURES	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. As applied to Critical Cyber Systems, these policies and controls must include:	Functional	Intersects With	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	8	
III.B	CYBERSECURITY MEASURES	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. As applied to Critical Cyber Systems, these policies and controls must include:	Functional	Intersects With	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	8	
III.B.1	CYBERSECURITY MEASURES	A list and description of -	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
III.B.1.a	CYBERSECURITY MEASURES	Information Technology and Operational Technology system interdependencies;	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	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/regulated data flows.	8	
III.B.1.a	CYBERSECURITY MEASURES	Information Technology and Operational Technology system interdependencies;	Functional	Intersects With	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS) that support more than one critical business function.	8	
III.B.1.b	CYBERSECURITY MEASURES	All external connections to the Information Technology and Operational Technology system;	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	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/regulated data flows.	8	
III.B.1.b	CYBERSECURITY MEASURES	All external connections to the Information Technology and Operational Technology system;	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	
III.B.1.c	CYBERSECURITY MEASURES	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; and	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	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/regulated data flows.	5	
III.B.1.c	CYBERSECURITY MEASURES	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; and	Functional	Intersects With	Asset Scope Classification	AST-04.1	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	
III.B.1.c	CYBERSECURITY MEASURES	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; and	Functional	Intersects With	Control Applicability Boundary Graphical Representation	AST-04.2	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	
III.B.1.c	CYBERSECURITY MEASURES	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; and	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	
III.B.1.c	CYBERSECURITY MEASURES	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; and	Functional	Intersects With	Sensitive / Regulated Data Enclave (Secure Zone)	NET-06.3	Mechanisms exist to implement segmentation controls to restrict inbound and outbound connectivity for sensitive/regulated data enclaves (secure zones).	5	
III.B.1.d	CYBERSECURITY MEASURES	Policies to ensure Information Technology and Operational Technology system services transit the other only when necessary for validated business or operational purposes.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8	
III.B.1.d	CYBERSECURITY MEASURES	Policies to ensure Information Technology and Operational Technology system services transit the other only when necessary for validated business or operational purposes.	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.	8	
III.B.2	CYBERSECURITY MEASURES	An identification and description of measures for securing and defending zone boundaries, that includes security controls -	Functional	Subset Of	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	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	10	
III.B.2.a	CYBERSECURITY MEASURES	To prevent unauthorized communications between zones; and	Functional	Subset Of	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	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	10	
III.B.2.b	CYBERSECURITY MEASURES	To prohibit Operational Technology system services from traversing the Information Technology system, and vice-versa, unless the content is encrypted or, if not technologically feasible, otherwise secured and protected to ensure integrity and prevent corruption or compromise while the content is in transit.	Functional	Subset Of	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	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	10	
III.C	CYBERSECURITY MEASURES	Implement access control measures, including those for local and remote access, to secure and prevent unauthorized access to Critical Cyber Systems. These measures must incorporate the following policies, procedures, and controls:	Functional	Intersects With	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	8	
III.C	CYBERSECURITY MEASURES	Implement access control measures, including those for local and remote access, to secure and prevent unauthorized access to Critical Cyber Systems. These measures must incorporate the following policies, procedures, and controls:	Functional	Intersects With	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	8	
III.C	CYBERSECURITY MEASURES	Implement access control measures, including those for local and remote access, to secure and prevent unauthorized access to Critical Cyber Systems. These measures must incorporate the following policies, procedures, and controls:	Functional	Intersects With	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	8	
III.C.1	CYBERSECURITY MEASURES	Identification and authentication policies and procedures designed to prevent unauthorized access to Critical Cyber Systems that include -	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
III.C.1	CYBERSECURITY MEASURES	Identification and authentication policies and procedures designed to prevent unauthorized access to Critical Cyber Systems that include -	Functional	Intersects With	Exception Management	GOV-02.1	Mechanisms exist to prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and recorded.	8	
III.C.1	CYBERSECURITY MEASURES	Identification and authentication policies and procedures designed to prevent unauthorized access to Critical Cyber Systems that include -	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for each Technology Asset, Application and/or Service (TAAS) under their control.	8	

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
III.C.1	CYBERSECURITY MEASURES	Identification and authentication policies and procedures designed to prevent unauthorized access to Critical Cyber Systems that include -	Functional	Intersects With	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	8	
III.C.1	CYBERSECURITY MEASURES	Identification and authentication policies and procedures designed to prevent unauthorized access to Critical Cyber Systems that include -	Functional	Intersects With	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	8	
III.C.1.a	CYBERSECURITY MEASURES	A policy for memorized secret authenticators resets that includes criteria for when resets must occur10; and	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
III.C.1.b	CYBERSECURITY MEASURES	Documented and defined mitigation measures for components of Critical Cyber Systems that will not fall under the policy required by the preceding subparagraph (IIIШ.C.1.a), and a timeframe to complete these mitigations.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
III.C.1.b	CYBERSECURITY MEASURES	Documented and defined mitigation measures for components of Critical Cyber Systems that will not fall under the policy required by the preceding subparagraph (IIIШ.C.1.a), and a timeframe to complete these mitigations.	Functional	Intersects With	Exception Management	GOV-02.1	Mechanisms exist to prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and recorded.	5	
III.C.1.b	CYBERSECURITY MEASURES	Documented and defined mitigation measures for components of Critical Cyber Systems that will not fall under the policy required by the preceding subparagraph (IIIШ.C.1.a), and a timeframe to complete these mitigations.	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
III.C.2	CYBERSECURITY MEASURES	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 Operational Technology components or assets, the Owner/Operator must specify what compensating controls are used to manage access.	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 Technology Assets, Applications and/or Services (TAAS); and/ or(3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data.	8	
III.C.2	CYBERSECURITY MEASURES	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 Operational Technology components or assets, the Owner/Operator must specify what compensating controls are used to manage access.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-05	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) Prioritize	8	
III.C.2	CYBERSECURITY MEASURES	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 Operational Technology components or assets, the Owner/Operator must specify what compensating controls are used to manage access.	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	8	
III.C.3	CYBERSECURITY MEASURES	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	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
III.C.3	CYBERSECURITY MEASURES	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	Exception Management	GOV-02.1	Mechanisms exist to prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and recorded.	5	
III.C.3	CYBERSECURITY MEASURES	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	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for each Technology Asset, Application and/or Service (TAAS) under their control.	8	
III.C.3	CYBERSECURITY MEASURES	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	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	8	
III.C.3	CYBERSECURITY MEASURES	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	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	8	
III.C.3	CYBERSECURITY MEASURES	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-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
III.C.4	CYBERSECURITY MEASURES	Enforcement of standards that limit the availability and use of shared accounts to those that are critical for operations, and then only if absolutely necessary. When the Owner/Operator uses shared accounts for operational purposes, the policies and procedures must ensure -	Functional	Intersects With	Restrictions on Shared Groups / Accounts	IAC-15.5	Mechanisms exist to authorize the use of shared/group accounts only under certain organization-defined conditions.	8	
III.C.4	CYBERSECURITY MEASURES	Enforcement of standards that limit the availability and use of shared accounts to those that are critical for operations, and then only if absolutely necessary. When the Owner/Operator uses shared accounts for operational purposes, the policies and procedures must ensure -	Functional	Intersects With	Credential Sharing	IAC-19	Mechanisms exist to prevent the sharing of generic IDs, passwords or other generic authentication methods.	8	
III.C.4.a	CYBERSECURITY MEASURES	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-15.5	Mechanisms exist to authorize the use of shared/group accounts only under certain organization-defined conditions.	8	
III.C.4.a	CYBERSECURITY MEASURES	Access to shared accounts is limited through account management that uses principles of least privilege and separation of duties; and	Functional	Intersects With	Credential Sharing	IAC-19	Mechanisms exist to prevent the sharing of generic IDs, passwords or other generic authentication methods.	8	
III.C.4.b	CYBERSECURITY MEASURES	Individuals who no longer need access do not have knowledge of the password necessary to access the shared accounts.	Functional	Intersects With	Restrictions on Shared Groups / Accounts	IAC-15.5	Mechanisms exist to authorize the use of shared/group accounts only under certain organization-defined conditions.	8	
III.C.4.b	CYBERSECURITY MEASURES	Individuals who no longer need access do not have knowledge of the password necessary to access the shared accounts.	Functional	Intersects With	Credential Sharing	IAC-19	Mechanisms exist to prevent the sharing of generic IDs, passwords or other generic authentication methods.	8	
III.C.5	CYBERSECURITY MEASURES	Regularly updated schedule for review of existing domain trust relationships to ensure their necessity and establish policies to manage these relationships.	Functional	Intersects With	Embedded Technology Reviews	EMB-10	Mechanisms exist to perform evaluations of deployed embedded technologies as needed, or at least on an annual basis, to ensure that necessary updates to mitigate the risks associated with legacy embedded technologies are identified and implemented.	5	
III.C.5	CYBERSECURITY MEASURES	Regularly updated schedule for review of existing domain trust relationships to ensure their necessity and establish policies to manage these relationships.	Functional	Intersects With	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	5	
III.C.5	CYBERSECURITY MEASURES	Regularly updated schedule for review of existing domain trust relationships to ensure their necessity and establish policies to manage these relationships.	Functional	Intersects With	Cross Domain Solution (CDS)	NET-02.3	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	5	
III.D	CYBERSECURITY MEASURES	Implement continuous monitoring and detection policies and procedures that are designed to prevent, detect, and respond to cybersecurity threats and correct anomalies affecting Critical Cyber Systems. These measures must include:	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
III.D	CYBERSECURITY MEASURES	Implement continuous monitoring and detection policies and procedures that are designed to prevent, detect, and respond to cybersecurity threats and correct anomalies affecting Critical Cyber Systems. These measures must include:	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for each Technology Asset, Application and/or Service (TAAS) under their control.	8	
III.D	CYBERSECURITY MEASURES	Implement continuous monitoring and detection policies and procedures that are designed to prevent, detect, and respond to cybersecurity threats and correct anomalies affecting Critical Cyber Systems. These measures must include:	Functional	Intersects With	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	8	
III.D	CYBERSECURITY MEASURES	Implement continuous monitoring and detection policies and procedures that are designed to prevent, detect, and respond to cybersecurity threats and correct anomalies affecting Critical Cyber Systems. These measures must include:	Functional	Intersects With	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	8	
III.D	CYBERSECURITY MEASURES	Implement continuous monitoring and detection policies and procedures that are designed to prevent, detect, and respond to cybersecurity threats and correct anomalies affecting Critical Cyber Systems. These measures must include:	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
III.D.1	CYBERSECURITY MEASURES	Capabilities to -	Functional	Subset Of	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for each Technology Asset, Application and/or Service (TAAS) under their control.	10	
III.D.1.a	CYBERSECURITY MEASURES	Defend against malicious email, such as spam and phishing emails, to preclude or mitigate against adverse impacts to operations;	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	
III.D.1.b	CYBERSECURITY MEASURES	Block ingress and egress communications with known or suspected malicious Internet Protocol addresses;	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	
III.D.1.b	CYBERSECURITY MEASURES	Block 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	
III.D.1.c	CYBERSECURITY MEASURES	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-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	
III.D.1.d	CYBERSECURITY MEASURES	Block and prevent unauthorized code, including macro scripts, from executing; and	Functional	Intersects With	Prohibit Installation Without Privileged Status	END-03	Automated mechanisms exist to prohibit software installations without explicitly assigned privileged status.	5	
III.D.1.d	CYBERSECURITY MEASURES	Block and prevent unauthorized code, including macro scripts, from executing; and	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
III.D.1.e	CYBERSECURITY MEASURES	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-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	
III.D.2	CYBERSECURITY MEASURES	Procedures to -	Functional	Subset Of	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	10	
III.D.2.a	CYBERSECURITY MEASURES	Audit unauthorized access to internet domains and addresses;	Functional	Intersects With	Inbound & Outbound Communications Traffic	MON-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	5	
III.D.2.a	CYBERSECURITY MEASURES	Audit unauthorized access to internet domains and addresses;	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	
III.D.2.b	CYBERSECURITY MEASURES	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-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	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	Notes
III.D.2.b	CYBERSECURITY MEASURES	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	
III.D.2.c	CYBERSECURITY MEASURES	Identify and respond to execution of unauthorized code, including macro scripts; and	Functional	Intersects With	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	3	
III.D.2.c	CYBERSECURITY MEASURES	Identify and respond to execution of unauthorized code, including macro scripts; and	Functional	Intersects With	Unauthorized Installation Alerts	CFG-05.1	Mechanisms exist to configure systems to generate an alert when the unauthorized installation of software is detected.	5	
III.D.2.d	CYBERSECURITY MEASURES	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-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	5	
III.D.2.d	CYBERSECURITY MEASURES	Implement capabilities (such as Security, Orchestration, Automation, and Response) to define, prioritize, and drive standardized incident response activities.	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	
III.D.2.d	CYBERSECURITY MEASURES	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-06	Mechanisms exist to utilize Security Orchestration, Automation and Response (SOAR) tools to define, prioritize and automate the response to security incidents.	8	
III.D.3	CYBERSECURITY MEASURES	Logging policies that -	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
III.D.3.a	CYBERSECURITY MEASURES	Require continuous collection and analyzing of data for potential intrusions and anomalous behavior on Critical Cyber Systems and other Operational and Information Technology systems that directly connects with Critical Cyber Systems; and	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
III.D.3.a	CYBERSECURITY MEASURES	Require continuous collection and analyzing of data for potential intrusions and anomalous behavior on Critical Cyber Systems and other Operational and Information Technology systems that directly connects with Critical Cyber Systems; and	Functional	Intersects With	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	5	
III.D.3.a	CYBERSECURITY MEASURES	Require continuous collection and analyzing of data for potential intrusions and anomalous behavior on Critical Cyber Systems and other Operational and Information Technology systems that directly connects with Critical Cyber Systems; and	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	
III.D.3.a	CYBERSECURITY MEASURES	Require continuous collection and analyzing of data for potential intrusions and anomalous behavior on Critical Cyber Systems and other Operational and Information Technology systems that directly connects with Critical Cyber Systems; and	Functional	Intersects With	Analyze and Prioritize Monitoring Requirements	MON-01.16	Mechanisms exist to assess the organization's needs for monitoring and prioritize the monitoring of Technology Assets, Applications and/or Services (TAAS), based on TAAS criticality and the sensitivity of the data it stores, transmits and processes.	5	
III.D.3.a	CYBERSECURITY MEASURES	Require continuous collection and analyzing of data for potential intrusions and anomalous behavior on Critical Cyber Systems and other Operational and Information Technology systems that directly connects with Critical Cyber Systems; and	Functional	Intersects With	Content of Event Logs	MON-03	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	
III.D.3.b	CYBERSECURITY MEASURES	Ensure data is maintained for sufficient periods, to provide effective investigation of cybersecurity incidents.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
III.D.3.b	CYBERSECURITY MEASURES	Ensure data is maintained for sufficient periods, to provide effective investigation of cybersecurity incidents.	Functional	Intersects With	Analyze and Prioritize Monitoring Requirements	MON-01.16	Mechanisms exist to assess the organization's needs for monitoring and prioritize the monitoring of Technology Assets, Applications and/or Services (TAAS), based on TAAS criticality and the sensitivity of the data it stores, transmits and processes.	5	
III.D.3.b	CYBERSECURITY MEASURES	Ensure data is maintained for sufficient periods, to provide effective investigation of cybersecurity incidents.	Functional	Intersects With	Audit Trails	MON-03.2	Mechanisms exist to link system access to individual users or service accounts.	5	
III.D.3.b	CYBERSECURITY MEASURES	Ensure data is maintained for sufficient periods, to provide effective investigation of cybersecurity incidents.	Functional	Intersects With	Event Log Retention	MON-10	Mechanisms exist to retain event logs 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	
III.D.4	CYBERSECURITY MEASURES	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.11	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	8	
III.D.4	CYBERSECURITY MEASURES	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.11	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
III.E	CYBERSECURITY MEASURES	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. These measures must include:	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
III.E.1	CYBERSECURITY MEASURES	A patch management strategy that ensures all critical security patches and updates on Critical Cyber Systems are current.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
III.E.1	CYBERSECURITY MEASURES	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-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	
III.E.2	CYBERSECURITY MEASURES	The strategy required by section III.E.1. must include:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
III.E.2.a	CYBERSECURITY MEASURES	The risk methodology for categorizing and determining criticality of patches and updates, and an implementation timeline based on categorization and criticality; and	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
III.E.2.a	CYBERSECURITY MEASURES	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-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
III.E.2.a	CYBERSECURITY MEASURES	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-05.3	Mechanisms exist to track the effectiveness of remediation operations through metrics reporting.	5	
III.E.2.b	CYBERSECURITY MEASURES	Prioritization of all security patches and updates on the Cybersecurity and Infrastructure Security Agency's Known Exploited Vulnerabilities Catalog.12	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
III.E.2.b	CYBERSECURITY MEASURES	Prioritization of all security patches and updates on the Cybersecurity and Infrastructure Security Agency's Known Exploited Vulnerabilities Catalog.12	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
III.E.2.b	CYBERSECURITY MEASURES	Prioritization of all security patches and updates on the Cybersecurity and Infrastructure Security Agency's Known Exploited Vulnerabilities Catalog.12	Functional	Intersects With	Vulnerability Ranking	VPM-03	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	5	
III.E.3	CYBERSECURITY MEASURES	If the Owner/Operator cannot apply patches and updates on specific Operational Technology systems without causing a severe degradation of operational capability to meet necessary capacity, 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-05	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	5	
III.E.3	CYBERSECURITY MEASURES	If the Owner/Operator cannot apply patches and updates on specific Operational Technology systems without causing a severe degradation of operational capability to meet necessary capacity, 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-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
III.F	CYBERSECURITY MEASURES	Develop a Cybersecurity Assessment Program for proactively assessing and auditing cybersecurity measures.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
III.F.1	CYBERSECURITY MEASURES	The Owner/Operator must develop a Cybersecurity Assessment Program 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-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
III.F.2	CYBERSECURITY MEASURES	The Cybersecurity Assessment Program required by Section III.F.1. must -	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
III.F.2.a	CYBERSECURITY MEASURES	Assess the effectiveness of the Owner/Operator's TSA-approved Cybersecurity Implementation Plan;	Functional	Intersects With	Assessments	IAO-02	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	
III.F.2.b	CYBERSECURITY MEASURES	Include an architectural design review to be conducted within the first 12 months after the Cybersecurity Implementation Plan approval and at least once every two years thereafter. An architectural design review contains verification and validation of network traffic, a system log review, and analysis to identify cybersecurity vulnerabilities related to network design, configuration, and interconnectivity to internal and external systems; and	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
III.F.2.b	CYBERSECURITY MEASURES	Include an architectural design review to be conducted within the first 12 months after the Cybersecurity Implementation Plan approval and at least once every two years thereafter. An architectural design review contains verification and validation of network traffic, a system log review, and analysis to identify cybersecurity vulnerabilities related to network design, configuration, and interconnectivity to internal and external systems; and	Functional	Intersects With	Assessment Boundaries	IAO-01.1	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	
III.F.2.b	CYBERSECURITY MEASURES	Include an architectural design review to be conducted within the first 12 months after the Cybersecurity Implementation Plan approval and at least once every two years thereafter. An architectural design review contains verification and validation of network traffic, a system log review, and analysis to identify cybersecurity vulnerabilities related to network design, configuration, and interconnectivity to internal and external systems; and	Functional	Intersects With	Assessments	IAO-02	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	
III.F.2.c	CYBERSECURITY MEASURES	Incorporate other assessment capabilities designed to identify vulnerabilities based on evolving threat information and adversarial capabilities, such as penetration testing of Information Technology systems, including the use of "red" and "purple"team (adversarial perspective) testing.	Functional	Intersects With	Assessments	IAO-02	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	
III.F.3	CYBERSECURITY MEASURES	No later than 60 days after TSA's approval of the Owner/Operator's Cybersecurity Implementation Plan, the Owner/Operator must submit the annual plan for their Cybersecurity Assessment Program to SurfOps-SD@tsa.dhs.gov. This plan must describe the Cybersecurity Assessment Program required by Section III.F.1, including the schedule for specific actions. The Owner/Operator must update this plan on an annual basis and submit it no later than one year from the date of the previous plan's submission.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	GOV-17	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	

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
IV	RECORDS	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
IV.A	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
IV.B	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 1520:13	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
IV.B.1	Protection of sensitive security information	Plans and reports; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
IV.B.2	Protection of sensitive security information	Audit, testing, or assessment results.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
IV.C	Documentation to Establish Compliance	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
IV.C.1	Documentation to Establish Compliance	The Owner/Operator must make records necessary to establish compliance with this Security Directive available to TSA upon request for inspection and/or copying.	Functional	Intersects With	Ability To Demonstrate Conformity	CPL-01.3	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	
IV.C.2	Documentation to Establish Compliance	TSA may request to inspect or copy the following documents to establish compliance with this Security Directive:	Functional	Intersects With	Assessor Access	CPL-03.3	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	
IV.C.2.a	Documentation to Establish Compliance	Hardware/software asset inventory, including supervisory control, and data acquisition systems;	Functional	Intersects With	Assessor Access	CPL-03.3	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	
IV.C.2.b	Documentation to Establish Compliance	Firewall rules;	Functional	Intersects With	Assessor Access	CPL-03.3	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	
IV.C.2.c	Documentation to Establish Compliance	Network diagrams, switch and router configurations, architecture diagrams, publicly routable internet protocol addresses, and Virtual Local Area Networks.	Functional	Intersects With	Assessor Access	CPL-03.3	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	
IV.C.2.d	Documentation to Establish Compliance	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 Program, and assessment or audit results.	Functional	Intersects With	Assessor Access	CPL-03.3	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	
IV.C.2.e	Documentation to Establish Compliance	Data providing a "snapshot" of activity on and between Information and Operational Technology systems such as -	Functional	Intersects With	Assessor Access	CPL-03.3	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	
IV.C.2.e.i	Documentation to Establish Compliance	Log files;	Functional	Intersects With	Assessor Access	CPL-03.3	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	
IV.C.2.e.ii	Documentation to Establish Compliance	A capture of network traffic (e.g., packet capture (PCAP)), not to exceed a period of twenty-four hours, as identified and directed by TSA;	Functional	Intersects With	Assessor Access	CPL-03.3	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	
IV.C.2.e.iii	Documentation to Establish Compliance	"East-West Traffic" of Operational Technology systems/sites/environments within the scope of this Security Directive's requirements; and	Functional	Intersects With	Assessor Access	CPL-03.3	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	
IV.C.2.e.iv	Documentation to Establish Compliance	"North-South Traffic" between Information and Operational Technology systems, and the perimeter boundaries between them.	Functional	Intersects With	Assessor Access	CPL-03.3	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	
IV.C.2.f	Documentation to Establish Compliance	Any other records or documents necessary to establish compliance with this Security Directive.	Functional	Intersects With	Assessor Access	CPL-03.3	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	
V	PROCEDURES FOR SECURITY DIRECTIVES	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
V.A	General Procedures	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
V.A.1	Confirm Receipt	Immediately provide written confirmation of receipt of this Security Directive via e-mail to SurfOps-SD@tsa.dhs.gov;	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	GOV-17	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	
V.A.2	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	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
V.B	Comments	Owner/Operators may comment on this Security Directive by submitting data, views, or arguments in writing to TSA via e-mail at TSA-Surface@tsa.dhs.gov. Any comments referring to specific measures in this Security Directive must be protected in accordance with the requirements in 49 CFR part 1520. TSA may amend the Security Directive based on comments received. Submission of a comment does not delay the effective date of the Security Directive or requirement to comply with the provisions of the Security Directive.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
VI	AMENDMENTS TO CYBERSECURITY IMPLEMENTATION PLAN	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
VI.A	Changes to ownership or control of operations	An Owner/Operator required to submit a Cybersecurity Implementation Plan under Section II.B. of this Security Directive 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	GOV-17	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	
VI.B	Changes to conditions affecting security	An Owner/Operator required to submit a Cybersecurity Implementation Plan under Section II.B. of this Security Directive 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, but not limited to changes to address:	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	GOV-17	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	
VI.B.1	Changes to conditions affecting security	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.F. of this Security Directive; or	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	GOV-17	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	
VI.B.2	Changes to conditions affecting security	The Owner/Operator has identified or acquired new or additional Critical Cyber Systems or 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	GOV-17	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	
VI.C	Permanent change	For purposes of this section, a "permanent change" is one intended to be in effect for 45 or more days.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	GOV-17	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	
VI.D	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 days after the permanent change takes effect, unless TSA allows a longer time period.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	GOV-17	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	
VI.E	TSA approval	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
VI.E.1	TSA approval	TSA may approve a requested amendment to a Cybersecurity Implementation Plan if TSA determines that it is in the interest of public and transportation security and the proposed amendment provides the level of security required under this Security Directive.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
VI.E.2	TSA approval	TSA may request additional information from the Owner/Operator before rendering a decision.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
VI.F	Petition for reconsideration	No later than 30 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 set in 49 CFR 1570.119.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
VII	DEFINITIONS	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control