NIST CSF v2.0 - Function	NIST CSF v2.0 - Category	CISA CPG (March 2023)	TSA SDs	TSA's Proposed CRM Rule Requirements
GOVERN (GV)	**Organizational Context (GV.OC):** The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood		Cybersecurity Vulnerability Assessment (Pipeline). 1. Owner/Operators must review Section 7 of TSA's 2018 Pipeline Security Guidelines (with Change 1 (April 2021)), and...a. Assess whether current practices and activities to address cyber risks to Owner/Operators Information and Operational Technology systems align with the Guidelines; b. Identify any gaps; and c. Identify remediation measures that will be taken to fill those gaps and a timeline for implementing these remediation measures. 2. The assessment and identification of gaps must be completed using the form provided by TSA. 3. The completed vulnerability assessment report containing all information required by this section must be submitted to TSA. Owner/Operators who have previously submitted a vulnerability assessment to TSA are not required to update and submit a revised assessment. (SD Pipeline-2021-01) Cybersecurity Vulnerability Assessment (Rail). 1. Owner/Operators must complete a cybersecurity vulnerability assessment and identify cybersecurity gaps using a form provided by TSA. The form utilizes the functions and categories found in the National Institute of Standards and Technology (NIST) Cybersecurity Framework. 2. Owner/Operators must identify remediation measures to address the vulnerabilities and cybersecurity gaps identified during the assessment and implement the plan for applying the identified measures. 3. The completed vulnerability assessment form and remediation plan required by this section must be submitted to TSA. The required information must be submitted via email to TSA at SurfOpsRail-SD@tsa.dhs.gov, using appropriate methods to protect any Sensitive Security Information contained in the completed assessment and the remediation plan. (SD 1580-21-01 and SD 1582-21-01)	**CYBERSECURITY EVALUATION.** (a) General. Each owner/operator required to have a CRM program must complete an initial and recurrent cybersecurity evaluation sufficient to determine the owner/operator's current enterprise-wide cybersecurity profile of logical/virtual and physical security controls when evaluated against the CRM program requirements in this subpart, using a form provided by TSA or other tools approved by TSA. (b) Timing. The initial cybersecurity evaluation must be completed no later than [INSERT DATE 90 DAYS AFTER EFFECTIVE DATE OF FINAL RULE], but no more than one year before the date of submission of the owner/operator's Cybersecurity Operational Implementation Plan .... If commencing or modifying operations subject to these requirements after [INSERT EFFECTIVE DATE OF FINAL RULE], the initial cybersecurity evaluation must be submitted to TSA no later than 45 calendar days after commencing the new or modified operations triggering applicability. (c) Annual updates. The evaluation required by paragraph (a) of this section must be updated annually, no later than one year from the anniversary date of the previously completed evaluation. (d) Notification. The owner/operator must notify TSA within 7 days of completing the evaluation and annual updates required by this section. A copy of the evaluation must be provided to TSA upon request. (e) Sensitive Security Information. This evaluation is a vulnerability assessment as defined in § 1500.3 of this subchapter and must be protected as Sensitive Security Information under § 1520.5(b)(5) of this subchapter. (Proposed 1580.305, 1582.205, and 1586.205.)
	Risk Management Strategy (GV.RM): The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions		*See* ***CYBERSECURITY EVALUATION*** *(above).*	
	Roles, Responsibilities, and Authorities (GV.RR): Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated	**1.B. Organizational Cybersecurity Leadership**. A single leader is responsible and accountable for cybersecurity within an organization. **1.C. OT Cybersecurity Leadership.** A single leader is responsible and accountable for OT-specific cybersecurity within an organization with OT assets.		**GOVERNANCE.** (a) *Accountable Executive.* (1) No later than [INSERT DATE 30 DAYS FROM EFFECTIVE DATE OF FINAL RULE], the owner/operator must provide to TSA the names, titles, business telephone numbers, and business email addresses of the owner/operator's accountable executive, who is the primary individual to be contacted with regard to the owner/operator's CRM program. If any of the information required by this paragraph changes, the owner/operator must provide the updated information to TSA within 7 days of the change. (2) The accountable executive must be an individual who has the authority and knowledge necessary for the development, implementation, and managerial oversight of the TSA-approved CRM program, including cybersecurity administration, risk assessments, inspections and control procedures, and coordinating communications with the owner/operator's leadership and staff on implementation and sustainment of the CRM program. To the extent possible, the accountable executive should not be the Cybersecurity Coordinator or an individual responsible for management of Information or Operational Technology system or systems' administration. (Proposed §§ 1580.309, 1582.209, and 1586.209.)
		1.D. Improving IT and OT Cybersecurity Relationships. Improve OT cybersecurity and more rapidly and effectively respond to OT cyber incidents.	Owner/Operators must designate and use a primary and at least one alternate Cybersecurity Coordinator at the corporate level. 1. Owner/Operators must provide in writing to TSA, at TSA-Surface-Cyber@tsa.dhs.gov, the names, titles, phone number(s), and email address(es) of the Cybersecurity Coordinator and alternate Cybersecurity Coordinator(s) within seven days of the commencement of new operations or change in any of the information required by this section. 2. The Cybersecurity Coordinator and alternate must—a. Be a U.S. citizen who is eligible for a security clearance; b. Serve as the primary contact for cyber-related intelligence information and cybersecurity-related activities and communications with TSA and CISA; c. Be accessible to TSA and CISA 24 hours a day, seven days a week; d. Coordinate cyber and related security practices and procedures internally; and e. Work with appropriate law enforcement and emergency response agencies. (SD 1580-21-01, SD 1582-21-01, and SD Pipeline-2021-01)	**CYBERSECURITY COORDINATOR.** (a)(1) Except as provided in paragraph (a)(2) of this section, each owner/operator...must designate employees at the corporate level to serve as the primary and at least one alternate Cybersecurity Coordinator with responsibility for sharing critical cybersecurity information. (2) Each owner/operator [of private rail cars or of a bus-only public transportation system] must designate and use a primary and at least one alternate Cybersecurity Coordinator, only if notified by TSA in writing that a threat exists concerning that type of operation. (b) The Cybersecurity Coordinator and alternate(s) must (1) Serve as the primary contact for cyber-related intelligence information and cybersecurity-related activities and communications with TSA and the Cybersecurity and Infrastructure Security Agency (CISA); (2) Have the following knowledge and skills, through current certifications or equivalent job experience: (i) General cybersecurity guidance and best practices; (ii) Relevant law and regulations pertaining to cybersecurity; (iii) Handling of Sensitive Security Information and security-related communications; and (iv) Current cybersecurity threats applicable to the owner/operator's operations and systems. (3) Be accessible to TSA and CISA 24 hours per day, 7 days per week; (4) Have a Homeland Security Information Network (HSIN) account or other TSA-designated communication platform for information sharing relevant to the requirements in this subpart; and (5) Work with appropriate law enforcement and emergency response agencies in addressing cybersecurity threats or responding to cybersecurity incidents. (c) The Cybersecurity Coordinator and alternate(s) must be a U.S. citizen eligible for a security clearance, unless otherwise waived by TSA. (d) Owner/operators must provide in writing to TSA the names, titles, business phone number(s), and business email address(es) of the Cybersecurity Coordinator and alternate Cybersecurity Coordinator(s) required by paragraph (a) of this section no later than [INSERT DATE 7 DAYS AFTER EFFECTIVE DATE OF FINAL RULE], or within 7 days of the commencement of new operations, or change in any of the information required by this section that occur after [INSERT DATE 7 DAYS AFTER EFFECTIVE DATE OF FINAL RULE]. (Proposed 1580.311, 1582.211, and 1586.211.)

NIST CSF v2.0 - Function	NIST CSF v2.0 - Category	CISA CPG (March 2023)	TSA SDs	TSA's Proposed CRM Rule Requirements
				GOVERNANCE. The COIP must also include: (1) Identification of positions designated by the owner/operator to manage implementation of policies, procedures, and capabilities described in the COIP and coordinate improvements to the CRM program. (2) Corporate-level identification of any authorized representatives, as defined in the TSA Cybersecurity Lexicon, who are responsible for any or all of the CRM program or cybersecurity measures identified in the CRM program, and written documentation (such as contractual agreements) clearly identifying the roles and responsibilities of the authorized representative under the CRM program. (3) The information required by paragraph (a) of this section. (Proposed 1580.309(b), 1582.209(b), and 1586.209(b).)
	Policies, Processes, and Procedures (GV.PO): Organizational cybersecurity policy is established, communicated, and enforced.	**1.B. Organizational Cybersecurity Leadership**. A single leader is responsible and accountable for cybersecurity within an organization.		***See GOVERNANCE/Accountable Executive (above).***
		1.C. OT Cybersecurity Leadership. A single leader is responsible and accountable for OT-specific cybersecurity within an organization with OT assets.		
	Oversight (GV.OV): Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy		*See **CYBERSECURITY ASSESSMENT PLAN (below)** and **CYBERSECURITY EVALUATION (above).** See also proposed §§ 1580.307(f), 1582.207(f), and 1586.207(f), would require status reports and updates of COIP based on results of required evaluations assessments and other identified vulnerabilities.*	
	Cybersecurity Supply Chain Risk Management (GV.SC): Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders.	**1.G. Supply Chain Incident Reporting.** Organizations more rapidly learn about and respond to known incidents or breaches across vendors and service providers.		**SUPPLY CHAIN RISK MANAGEMENT (Awareness).** The owner/operator must incorporate into its COIP policies, procedures, and capabilities to address supply chain cybersecurity vulnerabilities that include requiring ...(a) All procurement documents and contracts, including service-level agreements, executed or updated after [INSERT EFFECTIVE DATE OF FINAL RULE] include a requirement for the vendor or service provider to notify the owner/operator of the following: (1) cybersecurity incidents affecting the vendor or service provider within a specified timeframe sufficient for the owner/operator to identify and address any potential risks to their Critical Cyber Systems based on the scope and type of cybersecurity incident. (2) Confirmed security vulnerabilities affecting the goods, services, or capabilities provided by the vendor or service provider within a specified timeframe sufficient for the owner/operator to identify and address any potential risks to their Critical Cyber Systems based on the scope and type of security vulnerability. (Proposed 1580.315(a), 1582.215(a), and 1586.215(a).)
		1.H. Supply Chain Vulnerability Disclosure. Organizations more rapidly learn about and respond to vulnerabilities in assets provided by vendors and service providers.		SUPPLY CHAIN RISK MANAGEMENT **(Notifications by vendor of cybersecurity incidents).** The owner/operator must incorporate into its COIP policies, procedures, and capabilities to address supply chain cybersecurity vulnerabilities that include requiring....(d) Upon notification of a cybersecurity incident or vulnerability under paragraphs (a) or (b) of this section, immediate consideration of mitigation measures sufficient to address the resulting risk to Critical Cyber Systems and, as applicable, revision to the COIP in accordance with § 1570.107 of this subchapter. (Proposed 1580.315(d), 1582.215(d), and 1586.215(d).)
		1.I.. Vendor/Supplier Cybersecurity Requirements. Reduce risk by buying more secure products and services from more secure suppliers.		SUPPLY CHAIN RISK MANAGEMENT **(Evaluation of vendor cybersecurity).** The owner/operator must incorporate into its COIP policies, procedures, and capabilities to address supply chain cybersecurity vulnerabilities that include requiring...(b) Procurement documents and contracts, including service-level agreements, incorporate an evaluation by the owner/operator or qualified third-party of the cybersecurity measures implemented by vendors or service providers of goods, services, or capabilities that will be connected to, installed on, or used by the owner/operator's Critical Cyber Systems. (Proposed 1580.315(b), 1582.215(b), and 1586.215(b).)
				SUPPLY CHAIN RISK MANAGEMENT (Prioritizing cybersecurity in procurement decisions). The owner/operator must incorporate into its COIP policies, procedures, and capabilities to address supply chain cybersecurity vulnerabilities that include requiring...(c) When provided two offerings of roughly similar cost and function, giving preference to the offering that provides the greater level of cybersecurity necessary to protect against, or effectively respond to, cybersecurity incidents affecting the owner/operator's Critical Cyber Systems. (Proposed 1580.315(c), 1582.215(c), and 1586.215(c).)

NIST CSF v2.0 - Function	NIST CSF v2.0 - Category	CISA CPG (March 2023)	TSA SDs	TSA's Proposed CRM Rule Requirements
	Asset Management (ID.AM): Assets (e.g., data, hardware software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy	**1.A. Asset Inventory.** Better identify known, unknown (shadow), and unmanaged assets, and more rapidly detect and respond to new vulnerabilities.	Owner/Operator's must 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 the Owner/Operator to provide additional information regarding the methodologies or rationale used to identify Critical Cyber Systems. After consultation with Owner/Operators, TSA may notify an Owner/Operator that it must include additional Critical Cyber Systems identified by TSA not previously identified by the Owner/Operator in their Cybersecurity Implementation Plan. (SD 1580/82-2022-01 and SD Pipeline-2021-02) (NOTE: The SD requires rail operators to identify Positive Train Control (PTC) systems as a Critical Cyber System.)	**IDENTIFICATION OF CRITICAL CYBER SYSTEMS.** (a) Identifying information. The owner/operator must incorporate into its COIP a list of Critical Cyber Systems, as defined in the TSA Cybersecurity Lexicon, that provides, at a minimum, the following identifying information for each Critical Cyber System: (1) Identifier (system name or commercial name), and (2) System manufacturer/designer name. (b) Identification methodology. The owner/operator must include a description of the methodology and information used to identify Critical Cyber Systems that, at a minimum, includes the following information as used to identify critical systems: (1) Standards and factors, including system interdependencies with critical functions, used to identify Information Technology and Operational Technology systems that could be vulnerable to a cybersecurity incident; (2) Sources and data, such as known threat information relevant to the system, that informed decisions regarding the likelihood of the system being subject to a cybersecurity incident; (3) Potential operational impacts of a cybersecurity incident, including scenarios that identify potential supply chain impacts and how long critical operations and capabilities could be sustained with identified alternatives if a system is offline; and (4) Sustainability and operational impacts if an Information or Operational Technology system not identified as a Critical Cyber System becomes unavailable due to a cybersecurity incident. (c) Positive Train Control (PTC) Systems [applicable to rail only]. Owner/operators who are either required to install and operate PTC under 49 CFR part 236, subpart I, and/or voluntarily install and operate PTC under CFR part 236, subpart H or I, must include PTC systems as a Critical Cyber System. (d) System information and network architecture. For all Critical Cyber Systems, the owner/operator must provide the following information: (1) Information and Operational Technology system interdependencies for Critical Cyber Systems; (2) All external connections to Critical Cyber Systems; (3) Zone boundaries for Critical Cyber Systems, including a description of how Information and Operational Technology systems are defined and organized into logical/virtual zones based on criticality, consequence, and operational necessity; (4) Baseline of acceptable communications between Critical Cyber Systems and external connections or between Information and Operational Technology systems; and (5) Operational needs that prevent or delay implementation of the requirements in this subpart, such as application of security patches and updates, encryption of communications traversing Information and Operational Technology systems, and multi-factor authentication. (e) Additional systems. If notified by TSA, the owner/operator must include additional Critical Cyber Systems identified by TSA not previously identified by the owner/operator. (f) Changes in Critical Cyber Systems. Any substantive changes to Critical Cyber Systems require an amendment to the COIP subject to the procedures in § 1570.107 of this subchapter. (Proposed 1580.313, 1582.213, and 1586.213.)
	Risk Assessment (ID.RA): The cybersecurity risk to the organization, assets, and individuals is understood by the organization	**1.E. Mitigating Known Vulnerabilities.** Reduce the likelihood of threat actors exploiting known vulnerabilities to breach organizational networks.	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: 1. A patch management strategy that ensures all critical security patches and updates on Critical Cyber Systems are current. This strategy must include (a) the risk methodology for categorizing and determining criticality of patches and updates, and an implementation timeline based on categorization and criticality; and (b) prioritization of all security patches and updates on the Cybersecurity and Infrastructure Security Agency's Known Exploited Vulnerabilities Catalog. 2. 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. (SD 1580/82-2022-01 and SD Pipeline-2021-02)	PROTECTION OF CRITICAL SYSTEMS/**PATCH MANAGEMENT.** Measures that 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: (1) A patch management strategy that ensures all critical security patches and updates on Critical Cyber Systems are current. This strategy must include: (i) The risk methodology for categorizing and determining criticality of patches and updates, and an implementation timeline based on categorization and criticality; and (ii) Prioritization of all security patches and updates on CISA's Known Exploited Vulnerabilities Catalog. (2) In instances where 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 owner/operator must provide an explanation for why the actions cannot be taken and a description and timeline of additional mitigations that address the risk created by not installing the patch or update within the recommended timeframe. (Proposed paragraph (c) of 1580.317, 1582.217, and 1586.217.)

NIST CSF v2.0 - Function	NIST CSF v2.0 - Category	CISA CPG (March 2023)	TSA SDs	TSA's Proposed CRM Rule Requirements
IDENTIFY (ID)			Develop a Cybersecurity Assessment Plan for proactively assessing and auditing cybersecurity measures. 1. 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. 2. The Cybersecurity Assessment Plan ... must – a. Assess the effectiveness of the Owner/Operator's TSA-approved Cybersecurity Implementation Plan; b. Include a cybersecurity architecture design review to be conducted within the first 12 months after the Cybersecurity Implementation Plan approval and at least once every two years thereafter. A cybersecurity architecture 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 inter-connectivity to internal and external systems; and c. 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. d. Include a schedule for assessing and auditing specific cybersecurity measures and/or actions required by [the SD]. The schedule must ensure that 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 e. Ensure an annual report of the results of assessments conducted in accordance with the Cybersecurity Assessment Plan is submitted to TSA[.] 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. 3. The Owner/Operator must review and update its Cybersecurity Assessment Plan on an annual basis and submit it to TSA for approval no later than 12 months from the date the Owner/Operator submitted its first Cybersecurity Assessment Plan under Security Directive 1580/82-2022-01. The next Cybersecurity Assessment Plan submitted under this Security Directive, and all other Cybersecurity Assessment Plans thereafter, must be submitted to TSA no later than 12 months from the date of TSA's approval of the most recent Cybersecurity Assessment Plan. 4. The Owner/Operator must submit the Cybersecurity Assessment Plan report required by ... this section on an annual basis but no later than 12 months from the date the Owner/Operator submitted its first Cybersecurity Assessment Plan[.] The next Cybersecurity Assessment Plan report submitted under this Security Directive, and all other Cybersecurity Assessment Plan reports thereafter, must be submitted to TSA no later than 12 months from the date of TSA's approval of the most recent Cybersecurity Assessment Plan. (SD 1580/82-2022-01 and SD Pipeline-2021-02)	**CYBERSECURITY ASSESSMENT PLAN.** (a) Requirement for a Cybersecurity Assessment Plan. No later than 90 days from TSA's approval of the owner/operator's COIP, the owner/operator must submit to TSA a Cybersecurity Assessment Plan (CAP) sufficient to— (1) Proactively assess the effectiveness of the COIP; and (2) Identify and resolve device, network, and/or system vulnerabilities associated with Critical Cyber Systems. (b) Contents of the CAP. At a minimum, the CAP must describe in detail: (1) The plan to assess the effectiveness of the owner/operator's TSA-approved COIP; (2) Schedule and scope of an architectural design review within 12 months either before or after TSA's approval of the owner/operator's COIP, to be repeated at least once every two years thereafter. The architectural design review required by this paragraph must include 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; (3) Other assessment capabilities designed to identify vulnerabilities to Critical Cyber Systems 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. (c) Specific Schedule. The CAP must include a schedule for conducting the assessments required by paragraph (b). At a minimum, the schedule must ensure: (i) Compliance with the biennial architecture design review required by paragraph (b)(2); and (ii) At least one-third of the policies, procedures, measures, and capabilities in the TSA-approved COIP are assessed each year, with 100 percent assessed over a 3-year period..... (Proposed 1580.329, 1582.219, and 1586.219.)
			See ***CYBERSECURITY EVALUATION*** *(above).*	
			See also ***SUPPLY CHAIN SECURITY*** (above).	
		1.F. Third-Party Validation of Cybersecurity Control Effectiveness. Identify TTPs that lack proper defenses and establish confidence in organizational cyber defenses.	Develop a Cybersecurity Assessment Plan for proactively assessing and auditing cybersecurity measures. 1. 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. (SD 1580/82-2022-01 and SD Pipeline-2021-02)	**CYBERSECURITY ASSESSMENT PLAN.** No later than 90 days from TSA's approval of the owner/operator's COIP, the owner/operator must submit to TSA a Cybersecurity Assessment Plan (CAP) sufficient to (1) Proactively assess the effectiveness of the COIP; and (2) Identify and resolve device, network, and/or system vulnerabilities associated with Critical Cyber Systems. .... (d) Independence of assessors and auditors. Owner/operators must ensure that the assessments, audits, testing, and other capabilities to assess the effectiveness of its TSA-approved COIP are not conducted by individuals who have oversight or responsibility for implementing the owner/operator's CRM program and have no vested or other financial interest in the results of the CAP....(Proposed 1580.329, 1582.229, and 1586.229.)
	Improvement (ID.IM): Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions		*See* ***CYBERSECURITY ASSESSMENT PLAN*** *(above, NIST ID.AM and CPG 1.A).*	
		2.S. Incident Response (IR) Plans. Organizations maintain, practice, and update cybersecurity incident response plans for relevant threat scenarios.	*See* ***CYBERSECURITY INCIDENT RESPONSE PLAN*** *(below).*	
		5.A. Incident Planning and Preparedness. Organizations are capable of safely and effectively recovering from a cybersecurity incident.		

NIST CSF v2.0 - Function	NIST CSF v2.0 - Category	CISA CPG (March 2023)	TSA SDs	TSA's Proposed CRM Rule Requirements
	Identity Management, Authentication, and Access Control (PR.AA): Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access	**2.E. Separating User and Privileged Accounts.** Make it harder for threat actors to gain access to administrator or privileged accounts, even if common user accounts are compromised.	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: 3. 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. (SD 1580/82-2022-01 and SD Pipeline-2021-02)	PROTECTION OF CRITICAL SYSTEMS/ACCESS CONTROL/**PRIVILEGE.** The owner/operator must incorporate into its COIP policies, procedures, controls and capabilities to protect Critical Cyber Systems that meet security performance objectives in the following areas....(b) Access control. Access control measures for Critical Cyber Systems, including for local and remote access, that secure and defend against unauthorized access to Critical Cyber Systems. These measures must, at a minimum, incorporate the following policies, procedures, and controls: (3) Management of 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 compensating controls that the owner/operator applies. (Proposed 1580.317, 1582.217, and 1586.217.)
		2.A. Changing Default Passwords. Prevent threat actors from using default passwords to achieve initial access or move laterally in a network.	Implement access control measures, including for local and remote access, to secure and prevent unauthorized access to Critical Cyber Systems. These measures must incorporate: (1) identification and authentication policies and procedures designed to prevent unauthorized access to Critical Cyber Systems that include (a) a policy for memorized secret authenticator resets that includes criteria for when resets must occur; and (b) documented and defined mitigation measures for components of Critical Cyber Systems that will not fall under the policy for memorized secret authenticator resets and a timeframe to complete these mitigations. (SD 1580/82-2022-01 and SD Pipeline-2021-02)	PROTECTION OF CRITICAL SYSTEMS/ACCESS CONTROL/**PASSWORD SECURITY.** The owner/operator must incorporate into its COIP policies, procedures, controls and capabilities to protect Critical Cyber Systems that meet security performance objectives in the following areas—(b) Access control. Access control measures for Critical Cyber Systems, including for local and remote access, that secure and defend against unauthorized access to Critical Cyber Systems. These measures must, at a minimum, incorporate the following policies, procedures, and controls: (1) Identification and authentication requirements designed to prevent unauthorized access to Critical Cyber Systems, to include: (i) A policy for memorized secret authenticator resets that includes criteria for passwords and when resets must occur, including procedures to ensure implementation of these requirements, such as password lockouts[.] (Proposed 1580.317, 1582.217, and 1586.217.)
		2.B. Minimum Password Strength. Organizational passwords are harder for threat actors to guess or crack.		
		2.C. Unique Credentials. Attackers are unable to reuse compromised credentials to move laterally across the organization, particularly between IT and OT networks.	Implement access control measures, including for local and remote access, to secure and prevent unauthorized access to Critical Cyber Systems. These measures must incorporate: 4. 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—a. Access to shared accounts is limited through account management that uses principles of least privilege and separation of duties; and b. Individuals who no longer need access do not have knowledge of the password necessary to access the shared accounts. (SD 1580/82-2022-01 and SD Pipeline-2021-02)	PROTECTION OF CRITICAL SYSTEMS/ACCESS CONTROL/**SHARED ACCOUNTS**. The owner/operator must incorporate into its COIP policies, procedures, controls and capabilities to protect Critical Cyber Systems that meet security performance objectives in the following areas....(b) Access control. Access control measures for Critical Cyber Systems, including for local and remote access, that secure and defend against unauthorized access to Critical Cyber Systems. These measures must, at a minimum, incorporate the following policies, procedures, and controls: (4) Policies and procedures limit 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: (i) Access to shared accounts is limited through account management that uses principles of least privilege and separation of duties; (ii) Any individual who no longer needs access does not have knowledge of the memorized secret authenticator necessary to access the shared account; and (iii) Logs are maintained sufficient to enable positive user identification of access to shared accounts to enable forensic investigation following a cybersecurity incident. (Proposed 1580.317, 1582.217, and 1586.217.)
		2.D. Revoking Credentials for Departing Employees. Prevent unauthorized access to organizational accounts or resources by former employees.	Implement access control measures, including for local and remote access, to secure and prevent unauthorized access to Critical Cyber Systems. (SD 1580/82-2022-01 and SD Pipeline-2021-02)	PROTECTION OF CRITICAL SYSTEMS/ACCESS CONTROL/**PREVENTING UNAUTHORIZED ACCESS.** The owner/operator must incorporate into its COIP policies, procedures, controls and capabilities to protect Critical Cyber Systems that meet security performance objectives in the following areas—(b) Access control. Access control measures for Critical Cyber Systems, including for local and remote access, that secure and defend against unauthorized access to Critical Cyber Systems. (Proposed 1580.317, 1582.217, and 1586.217.) [Note specific exception to access control requirements only applicable to freight railroads: (f) Exception for PTC hardware and software components installed on locomotive. (1) For hardware and software components of a PTC system installed on a locomotive, owner/operators in compliance with requirements in 49 CFR 232.105(h)(1-4) (General requirements for locomotives), 49 CFR 236.3 (Locking of signal apparatus housings), and 49 CFR 256.553 (Seal, where required), may rely on the physical security measures used to comply with these requirements, as applicable, in lieu of implementing the requirements in paragraph (b). (2) If relying on the exception in paragraph (f)(1), the owner/operator must list the applicable PTC system as a Critical Cyber System; maintain compliance with the requirements specified in 49 CFR 232.105(h)(1-4), 49 CFR 236.3, and 49 CFR 256.553, as applicable; and include in the COIP a description of the physical security measures used to prevent unauthorized access to the identified PTC components. (Proposed 1580.319(f)).
		2.G. Detection of Unsuccessful (Automated) Login Attempts. Protect organizations from automated, credential-based attacks.	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...2. Procedures to...a. Audit unauthorized access to internet domains and addresses; b. 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[.] (SD 1580/82-2022-01 and SD Pipeline-2021-02)	*See* ***DETECTION OF CYBERSECURITY INCIDENTS*** *(below).*

NIST CSF v2.0 - Function	NIST CSF v2.0 - Category	CISA CPG (March 2023)	TSA SDs	TSA's Proposed CRM Rule Requirements
PROTECT (PR)		**2.H. Phishing-Resistant Multifactor Authentication (MFA).** Add a critical, additional layer of security to protect assets accounts whose credential shave been compromised.	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 ... 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. (SD 1580/82-2022-01 and SD Pipeline-2021-02)	PROTECTION OF CRITICAL SYSTEMS/ACCESS CONTROL/**MFA.** Access control measures for Critical Cyber Systems, including for local and remote access, that secure and defend against unauthorized access to Critical Cyber Systems. These measures must, at a minimum, incorporate the following policies, procedures, and controls: (2) Multi-factor authentication, or other logical/virtual and physical security controls to supplement memorized secret authenticators (such as passwords) 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. (Proposed 1580.317, 1582.217, and 1586.217.)
				PROTECTION OF CRITICAL SYSTEMS/ACCESS CONTROL/**PASSWORD SECURITY (Physical Security Controls).** The owner/operator must incorporate into its COIP policies, procedures, controls and capabilities to protect Critical Cyber Systems that meet security performance objectives in the following areas—(b) Access control. Access control measures for Critical Cyber Systems, including for local and remote access, that secure and defend against unauthorized access to Critical Cyber Systems. These measures must, at a minimum, incorporate the following policies, procedures, and controls: ....(1) (ii) Documented and defined logical/virtual and physical security controls for components of Critical Cyber Systems that will not be subject to the requirements in paragraph (b)(1)(i) of this section. (Proposed 1580.317, 1582.217, and 1586.217.)
	Awareness and Training (PR.AT): The organization's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks	**2.I. Basic Cybersecurity Training.** Organizational users learn and perform more secure behaviors.		**GENERAL CYBERSECURITY TRAINING.** (1) Owner/operators required to have a CRM program under this subchapter must provide basic cybersecurity training to all employees, with access to the owner/operator's Information or Operational Technology systems. (2) No owner/operator required to have a CRM program under this subpart may permit a cybersecurity-sensitive employee to access, or have privileges to access, a Critical Cyber System or an Information or Operational Technology system that is interdependent with a Critical Cyber System, unless that individual has received basic and role-based cybersecurity training. (b) General curriculum requirements. The cybersecurity training program must include a curriculum or lesson plan, including learning objectives and method of delivery (such as instructor-led or computer-based training) for each course used to meet the requirements in paragraphs (d) and (e) of this section. TSA may request additional information regarding the curriculum during the review and approval process. If recurrent training under paragraph (e) of this section is not the same as initial training, a curriculum or lesson plan for the recurrent training will need to be submitted and approved by TSA. (c) Specific curriculum requirements. (1) Basic cybersecurity training. All employees and contractors with access to the owner/operator's Information or Operational Technology systems, must receive basic cybersecurity training that includes cybersecurity awareness to address best practices, acceptable use, risks associated with their level of privileged access, and awareness of security risks associated with their actions. This training must address the following topics: (i) Social engineering, including phishing; (ii) Password best practices; (iii) Remote work security basics; (iv) Safe internet and social media use; (v) Mobile device (wireless) vulnerabilities and network security; (vi) Data management and information security, including protecting business email, confidential information, trade secrets, and privacy; and (vii) How and to whom to report suspected inappropriate or suspicious activity involving Information or Operational Technology systems, including mobile devices provided by or connected to the owner/operator's Information or Operational Technology systems. (Proposed 1580.319, 1582.219, and 1586.219.)
		2.J. OT Cybersecurity Training. Personnel responsible for security OT assets received specialized OT-focused cybersecurity training.		**ROLE-BASED CYBERSECURITY TRAINING.** Cybersecurity-sensitive employees must be provided cybersecurity training that specifically addresses their role as a privileged user to prevent and respond to a cybersecurity incident, acceptable uses, and the risks associated with their level of access and use as approved by the owner/operator. This training must address the following topics as applicable to the specific role: (i) Security measures and requirements in the COIP including how the requirements affect account and access management, server and application management, and system architecture development and assessment; (ii) Recognition and detection of cybersecurity threats, types of cybersecurity incidents, and techniques used to circumvent cybersecurity measures; (iii) Incident handling, including procedures for reporting a cybersecurity incident to the Cybersecurity Coordinator and understanding their roles and responsibilities during a cybersecurity incident and implementation of the owner/operator's Cybersecurity Incident Response Plan required by [§§ 1580.327, 1582.227, or 1586.227, as applicable]; (iv) Requirements and sources for staying aware of changing cybersecurity threats and countermeasures; and (v) Operational Technology-specific cybersecurity training for all personnel whose duties include access to Operational Technology systems. (Proposed paragraph (c)(2) of 1580.319, 1582.219, and 1586.219.)

NIST CSF v2.0 - Function	NIST CSF v2.0 - Category	CISA CPG (March 2023)	TSA SDs	TSA's Proposed CRM Rule Requirements
				GENERAL TRAINING PROGRAM REQUIREMENTS. (d) Initial cybersecurity training. (1) Each owner/operator must provide initial cybersecurity training (basic and role-based, as applicable) to employees and contractors, using the curriculum approved by TSA no later than 60 days after the effective date of the owner/operator's TSA-approved COIP required by this subpart. (2) For individuals who onboard or become cybersecurity-sensitive employees after the effective date of the owner/operator's TSA-approved COIP who did not receive training within the period identified in paragraph (d)(1) of this section, the individual must receive the applicable cybersecurity training no later than 10 days after onboarding. (e) Recurrent cybersecurity training. Employees and contractors must receive annual recurrent cybersecurity training no later than the anniversary calendar month of the employee's initial cybersecurity training. If the owner/operator provides the recurrent cybersecurity training in the month of, the month before, or the month after it is due, the employee is considered to have taken the training in the month it is due. (f) Recognition of prior or established cybersecurity training. Previously provided cybersecurity training may be credited towards satisfying the requirements of this section provided the owner/operator...(1) Obtains a complete record of such training and validates the training meets requirements of this section as it relates to the role of the individual employee, and the training was provided within the schedule required for recurrent training; and (2) Retains a record of such training in compliance with the requirements in paragraph (g) of this section. (g) Retention of cybersecurity training records. The owner/operator must retain records of initial and recurrent cybersecurity training records for each individual required to receive cybersecurity training under this section for no less than five (5) years from the date of training that, at a minimum...(1) Includes the employee's full name, job title or function, date of hire, and date of initial and recurrent cybersecurity training; and (2) Identifies the date, course name, course length, and list of topics addressed for the cybersecurity training most recently provided in each of the areas required under paragraph (c) of this section. (h) Availability of records to employees. The owner/operator must provide records of cybersecurity training to current and former employees upon request and at no charge as necessary to provide proof of training. (Proposed paragraphs (d) through (h) of 1580.319., 1592.219, and 1596.219.)
	Data Security (PR.DS): Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information	**2.K. Strong and Agile Encryption.** Effective encryption deployed to maintain confidentiality of sensitive data and integrity of IT and OT traffic.	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 ...2. An identification and description of measures for securing and defending zone boundaries, that includes security controls...b. 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. (SD 1580/82-2022-01 and SD Pipeline-2021-02) (NOTE: The Pipeilne SD includes does not include the option for other methods. This exception was added for rail due to specific operational issues. The proposed rule would apply the same language for all operations.)	PROTECTION OF CRITICAL SYSTEMS/ACCESS CONTROL/**ENCRYPTION.** The owner/operator must incorporate into its COIP policies, procedures, controls and capabilities to protect Critical Cyber Systems that meet security performance objectives in the following areas: . . . . (2) Secure and defend zone boundaries with security controls.... (ii) To prohibit Operational Technology system services from traversing the Information Technology system, and vice-versa, unless the content is encrypted at a level sufficient to secure and protect integrity of data and prevent corruption or compromise while in transit. If encryption is not technologically feasible, ensure content is otherwise secured and protected using compensating controls that provide the same level of security as encryption for data in transit. (Proposed 1580.317, 1582.217, and 1586.217.)
		2.L. Secure Sensitive Data. Protect sensitive information from unauthorized access.		
		2.M. Email Security. Reduce risk from common email-based threats, such as spoofing, phishing, and interception.	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. These measures must include: (1) capabilities to (a) defend against malicious email, such as spam and phishing emails, to preclude or mitigate adverse impacts to operations; (b) block ingress and egress communications with known or suspected malicious IP addresses; (c) control impact of known or suspected malicious web domains or web applications, such as by preventing users and devices from accessing malicious websites; (d) block and prevent unauthorized code, including macro scripts, from executing; and (e) monitor and/or block connections from known or suspected malicious command and control services. (SD 1580/82-2022-01 and SD Pipeline-2021-02, Section III.D.)	**DETECTION OF CYBERSECURITY EVENTS.** The owner/operator must incorporate into its COIP policies, procedures, and capabilities sufficient to detect and respond to cybersecurity threats to, and anomalies on, Critical Cyber Systems that, at a minimum...(a) Defend against malicious email, such as spam and phishing emails, to preclude or mitigate against adverse impacts to operations; (b) Block ingress and egress communications with known or suspected malicious Internet Protocol addresses; (c) Control impact of known or suspected malicious web domains or web applications, such as by preventing users and devices from accessing malicious websites; (d) Block and defend against unauthorized code, including macro scripts, from executing; (e) Monitor and/or block connections from known or suspected malicious command and control servers (such as Tor exit nodes, and other anonymization services); and (f) Ensure continuous collection and analysis of data for potential intrusions and anomalous behavior on Critical Cyber Systems and other Information and Operational Technology systems that directly connect with Critical Cyber Systems. (Proposed 1580.321, 1582.221, and 1586.221.) *See also* proposed 1580.323, 1582.223, and 1586.223.
		2.R. System Backups. Organizations reduce the likelihood and duration of data loss at loss of service delivery or operations.	1. Owner/Operators must have an up-to-date Cybersecurity Incident Response Plan for their Critical Cyber Systems, as defined in the SD 1580/82-2022-01 series, that includes measures to reduce the risk of operational disruption, or other significant impacts on business critical functions, should their rail system or facility experience a cybersecurity incident. The Cybersecurity Incident Response Plan must provide specific measures sufficient to ensure the following objectives, as technically applicable and feasible: b. Security and integrity of backed-up data, including measures to secure and safely maintain backups offline, and implement procedures requiring scanning of stored backup data with host security software to check that it is free of malicious artifacts when the backup is made and when tested for restoration. (SD 1580-21-01, 1582-21-01 and SD Pipeline-2021-02)	PROTECTION OF CRITICAL SYSTEMS/**SECURE BACK-UPS.** Policies that ensure all Critical Cyber Systems are backed-up on a regular basis consistent with operational need for the information, the back-ups are securely stored separate from the system, and policies that require testing the integrity of back-ups to ensure that the data is free of known malicious code when the back-ups are made. (Proposed paragraph (e) of 1580.317, 1582.217, and 1586.217.)

NIST CSF v2.0 - Function	NIST CSF v2.0 - Category	CISA CPG (March 2023)	TSA SDs	TSA's Proposed CRM Rule Requirements
	Platform Security (PR.PS): The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability	**2.F. Network Segmentation.** Reduce the likelihood of threat actors accessing the OT network after compromising the IT network.	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: 2. An identification and description of measures for securing and defending zone boundaries, that includes security controls—a. To prevent unauthorized communications between zones[.] (SD 1580/82-2022-01 and SD Pipeline-2021-02)	PROTECTION OF CRITICAL SYSTEMS/ACCESS CONTROL/**NETWORK SEGMENTATION.** The owner/operator must incorporate into its COIP policies, procedures, controls and capabilities to protect Critical Cyber Systems that meet security performance objectives in the following areas: (a) Network segmentation. Network segmentation measures that protect against access to, or disruption of, the Operational Technology system if the Information Technology system is compromised or vice versa. These measures must be sufficient to...(1) Ensure Information and Operational Technology system-services transit the other only when necessary for validated business or operational purposes; (2) Secure and defend zone boundaries with security controls...(i) To defend against unauthorized communications between zones[.] (Proposed 1580.317, 1582.217, and 1586.217.)
		2.P. Document Network Topology. More efficiently and effectively respond to cyberattacks and maintain service continuity.		
		2.N. Disable Macros by Default. Reduce the risk from embedded macros and similar executive code, a common and highly effective threat actor TTP.	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. These measures must include: (1) capabilities to (a) defend against malicious email, such as spam and phishing emails, to preclude or mitigate adverse impacts to operations; (b) block ingress and egress communications with known or suspected malicious IP addresses; (c) control impact of known or suspected malicious web domains or web applications, such as by preventing users and devices from accessing malicious websites; (d) block and prevent unauthorized code, including macro scripts, from executing; and (e) monitor and/or block connections from known or suspected malicious command and control services. (SD 1580/82-2022-01 and SD Pipeline-2021-02)	**DETECTION OF CYBERSECURITY EVENTS.** The owner/operator must incorporate into its COIP policies, procedures, and capabilities sufficient to detect and respond to cybersecurity threats to, and anomalies on, Critical Cyber Systems that, at a minimum...(a) Defend against malicious email, such as spam and phishing emails, to preclude or mitigate against adverse impacts to operations; (b) Block ingress and egress communications with known or suspected malicious Internet Protocol addresses; (c) Control impact of known or suspected malicious web domains or web applications, such as by preventing users and devices from accessing malicious websites; (d) Block and defend against unauthorized code, including macro scripts, from executing; (e) Monitor and/or block connections from known or suspected malicious command and control servers (such as Tor exit nodes, and other anonymization services); and (f) Ensure continuous collection and analysis of data for potential intrusions and anomalous behavior on Critical Cyber Systems and other Information and Operational Technology systems that directly connect with Critical Cyber Systems. (Proposed 1580.321, 1582.221, and 1586.221.) *See also* proposed 1580.323, 1582.223, and 1586.223.
		2.O. Document Device Configurations. More efficiently and effectively manage, respond to, and recover from cyberattacks against the organization and maintain service continuity.		
		2.Q. Hardware and Software Approval Process. Increase visibility into deployed technology assets, and reduce the likelihood of breach by users installing unapproved hardware, firmware, or software.		
		2.V. Prohibit Connection of Unauthorized Devices. Prevent malicious actors from achieving initial access or data exfiltration via unauthorized portable media devices.		
			See also ***CYBERSECURITY INCIDENT RESPONSE PLAN*** *(below).*	
		2.T. Log Collection. Achieve better visibility to detect and effectively respond to cyberattacks.	Implement continuous monitoring and detection polices and procedures that are designed to prevent, detect, and respond to cybersecurity threats and anomalies affecting Critical Cyber Systems. These measures must include (3) logging policies that (1) require continuous collection and analyzing of data for potential intrusions and anomalous behavior on Critical Cyber Systems and other OT systems that directly connect with Critical Cyber Systems; and (b) ensure data is maintained for sufficient periods to provide effective investigation of cybersecurity incidents. (SD 1580/82-2022-01 and SD Pipeline-2021-02)	PROTECTION OF CRITICAL SYSTEMS/**LOGGING POLICIES**. Logging policies sufficient to ensure logging data is—(1) Stored in a secure and centralized system, such as a security information and event management tool or database on a segmented network that can only be accessed or modified by authorized and authenticated users; and (2) Maintained for a duration sufficient to allow for investigation of cybersecurity incidents as supported by a risk analysis and applicable standards or regulatory guidelines. (Proposed paragraph(d) of 1580.317, 1582.217, and 1586.217.)
		2.U. Secure Log Storage. Organizations' security logs are protected from unauthorized access and tampering.		
	Technology Infrastructure Resilience (PR.IR): Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience	**2.F. Network Segmentation.** Reduce the likelihood of threat actors accessing the OT network after compromising the IT network.	*See* ***NETWORK SEGMENTATION*** *(above).*	
		2.W. No Exploitable Services on the Internet. Unauthorized users cannot gain an initial system foothold by exploiting known weaknesses in public-facing assets.	Implement access control measures, including for local and/or remote access, to secure and prevent unauthorized access to Critical Cyber Systems. These measures must incorporate the ... (5) [regularly updated] schedule for review of existing domain trust relationships to ensure their necessity and establish policies to manage these relationships. (SD 1580/82-2022-01 and SD Pipeline-2021-02) (NOTE: Bracketed langauge is not in SD Pipeline 2021-02.)	PROTECTION OF CRITCIAL SYSTEMS/**DOMAIN TRUST.** The owner/operator must incorporate into its COIP policies, procedures, controls and capabilities to protect Critical Cyber Systems that meet security performance objectives in the following areas...(5) Regularly updated schedule for review of existing domain trust relationships to ensure their necessity and established and enforced policies to manage these relationships. (Proposed paragraph (b)(5) of 1580.317, 1582.217, and 1586.217; *see also crosswalk for CPG 1.A. and 2.F.)*
		2.X. Limit OT Connections to Public Internet. Reduce the risk of threat actors exploiting or interrupting OT assets connected to the public internet.		
DETECT (DE)	**Continuous Monitoring (DE.CM):** Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events	**3.A. Detecting Relevant Threats and TTPs.** Organizations are aware of and able to detect relevant threats and TTPs.	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. These measures must include: (1) capabilities to (a) defend against malicious email, such as spam and phishing emails, to preclude or mitigate adverse impacts to operations; (b) block ingress and egress communications with known or suspected malicious IP addresses; (c) control impact of known or suspected malicious web domains or web applications, such as by preventing users and devices from accessing malicious websites; (d) block and prevent unauthorized code, including macro scripts, from executing; and (e) monitor and/or block connections from known or suspected malicious command and control services. (SD 1580/82-2022-01 and SD Pipeline-2021-02)	**DETECTION OF CYBERSECURITY EVENTS.** The owner/operator must incorporate into its COIP policies, procedures, and capabilities sufficient to detect and respond to cybersecurity threats to, and anomalies on, Critical Cyber Systems that, at a minimum...(a) Defend against malicious email, such as spam and phishing emails, to preclude or mitigate against adverse impacts to operations; (b) Block ingress and egress communications with known or suspected malicious Internet Protocol addresses; (c) Control impact of known or suspected malicious web domains or web applications, such as by preventing users and devices from accessing malicious websites; (d) Block and defend against unauthorized code, including macro scripts, from executing; (e) Monitor and/or block connections from known or suspected malicious command and control servers (such as Tor exit nodes, and other anonymization services); and (f) Ensure continuous collection and analysis of data for potential intrusions and anomalous behavior on Critical Cyber Systems and other Information and Operational Technology systems that directly connect with Critical Cyber Systems. (Proposed 1580.321, 1582.221, and 1586.221.) *See also* proposed 1580.323, 1582.223, and 1586.223.
	Anomalies and Events (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents			

NIST CSF v2.0 - Function	NIST CSF v2.0 - Category	CISA CPG (March 2023)	TSA SDs	TSA's Proposed CRM Rule Requirements
RESPOND (RS)	**Incident Management (RS.MA):** Responses to detected cybersecurity incidents are managed	**5.A. Incident Planning and Preparedness.** Organizations are capable of safely and effectively recovering from a cybersecurity incident.	1. Owner/Operators must have an up-to-date Cybersecurity Incident Response Plan for their Critical Cyber Systems, as defined in the SD 1580/82-2022-01 series, that includes measures to reduce the risk of operational disruption, or other significant impacts on business critical function, should their rail system/the covered pipeline or facility experience a cybersecurity incident. The Cybersecurity Incident Response Plan must provide specific measures sufficient to ensure the following objectives, as technically applicable and feasible: a. Prompt identification, isolation and segregation of the infected systems from uninfected systems, networks, and devices to prioritize: i. Limiting the spread of autonomous malware, ii. Denying continued attacker access to systems, iii. Determining extent of compromise, and iv. Preservation of evidence or partially encrypted data system storage. b. Security and integrity of backed-up data, including measures to secure and safely maintain backups offline, and implement procedures requiring scanning of stored backup data with host security software to check that it is free of malicious artifacts when the backup is made and when tested for restoration. c. Established capability and governance for isolating the Information Technology and Operational Technology systems in the event of a cybersecurity incident that arises to the level of potential operational disruption while maintaining operational standards and limits. 2. The Cybersecurity Incident Response Plan must, at a minimum, identify who (by position) is responsible for implementing the specific measures and any necessary resources needed to implement these measures. 3. The Owner/Operator must conduct situational exercises to test the effectiveness of procedures, and personnel responsible for implementing measures, in the Cybersecurity Incident Response Plan, no less than annually. These exercises must...a. Test at least two objectives of the Owner/Operator's Cybersecurity Incident Response Plan required by subparagraphs 1.a. through 1.c. of this section, no less than annually; and b. Include the employees identified (by position) as in paragraph [2.] as active participants in the exercises. (SD 1580-21-01 and SD 1582-21-01) (NOTE: SD Pipeline-2021-02, Section F, contains similar requirements but they are oraganized differently.)	**CYBERSECURITY INCIDENT RESPONSE PLAN.** (a) The owner/operator must incorporate into its COIP an up-to-date Cybersecurity Incident Response Plan (CIRP) for the owner/operator's Critical Cyber Systems to reduce the impacts of a cybersecurity incident that causes, or could cause, operational disruption or significant impacts on business-critical functions. (b) The CIRP must provide specific measures sufficient to ensure the following objectives, as applicable: (1) Promptly identifying, isolating, and segregating the infected systems from uninfected systems, networks, and devices using measures that prioritize: (i) Limiting the spread of autonomous malware; (ii) Denying continued access by a threat actor to systems; (iii) Determining extent of compromise; and (iv) Preserving evidence and data. (2) Only data stored and secured as required by [§§ 1580.317(e), 1582.217(e) or 1586.217(e), as applicable,] is used to restore systems and that all stored backup data is scanned with host security software to ensure the data is free of malicious artifacts before being used for restoration. (3) Established capability and governance for implementing mitigation measures or manual controls that ensure that the Operational Technology system can be isolated when a cybersecurity incident in the Information Technology system creates risk to the safety and reliability of the Operational Technology system. (c) The CIRP must identify who (by position) is responsible for implementing the specific measures in the plan and any necessary resources needed to implement the measures. (d) The owner/operator must conduct an exercise to test the effectiveness of the CIRP no less than annually. (e) Within no more than 90 days after the date of the exercise required by paragraph (d), the owner/operator must update the CIRP as appropriate to address any issues identified during the exercise. (f) The owner/operator must notify TSA within 15 days of any changes to the CIRP. As the owner/operator must separately notify TSA, updating the COIP to align with information provided to TSA under this section does not require an amendment subject to the procedures in § 1570.107 of this subchapter. (Proposed 1580.327, 1582.227, and 1586.227.)
		2.S. Incident Response (IR) Plans. Organizations maintain, practice, and update cybersecurity incident response plans for relevant threat scenarios.		
	Analysis (RS.AN): Investigations are conducted to ensure effective response and support forensics and recovery activities.			
		4.B. Vulnerability Disclosure/Reporting. Organizations more rapidly learn about vulnerabilities or weaknesses in their assets discovered by security researchers; researchers are more incentivized to responsibly share their findings.	*See* ***SUPPLY CHAIN RISK MANAGEMENT (Notifications by vendor)*** *(above).*	
		4.C. Deploy Security.txt Files. Allow security researchers to submit discovered weaknesses or vulnerabilities faster.		

NIST CSF v2.0 - Function	NIST CSF v2.0 - Category	CISA CPG (March 2023)	TSA SDs	TSA's Proposed CRM Rule Requirements
	Incident Response Reporting and Communication (RS.CO): Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies	**4.A. Incident Reporting.** CISA and other organizations are better able to provide assistance or understand the broader scope of a cyberattack.	Owner/Operators must report cybersecurity incidents to CISA involving systems that the Owner/Operator has responsibility to operate and/or maintain including: (a) unauthorized access of an Information or Operational Technology system; (b) discovery of malicious software on an Information or Operational Technology system; (c) activity resulting in a denial of service to any Information or Operational Technology system; and/or (d) any other cybersecurity incident that results in operational disruption to the Owner/Operator's Information or Operational Technology systems or other aspects of the Owner/Operator's rail systems or facilities, or an incident that has the potential to cause impact to a large number of passengers, critical infrastructure or core government functions, or impacts national security, economic security or public health and safety. Owner/Operators must report the incidents required by this section as soon as practicable, but no later than 24 hours after a cybersecurity incident is identified. Reports required by TSA must be made to CISA Central using CISA's Reporting System form at: https://us-cert.cisa.gov/forms/report or by calling (888) 282-0870. All reported information will be protected in a manner appropriate for the sensitivity and criticality of the information. The report to CISA must include the following information, as available to the reporting Owner/Operator at the time of the report: (a) the name of the reporting individual and contact information, including a telephone number and email address; (b) the affected … system(s) or facilities, including identifying information and location; (c) description of the threat, incident, or activity, to include: (i) earliest known date of compromise; (ii) date of detection; (iii) information about who has been notified and what action has been taken; (iv) any relevant information observed or collected by the Owner/Operators, such as malicious IP addresses, malicious domains, malware hashes and/or samples, or the abuse of legitimate software or accounts; and (v.) any known threat information, to include information about the source of the threat or attack, if available; and (d) a description of the incident's impact or potential impact on Information or Operational Technology systems and operations (this information must also include an assessment of actual or imminent adverse impacts to service operations, operational delays, and/or data theft that have or are likely to be incurred, as well as any other information that would be informative in understanding the impact or potential impact of the cybersecurity incident); (e) a description of all responses that are planned or under consideration, to include, for example, a reversion to manual operations of train movement and control, if applicable; and (f) any additional relevant information. If all the required information is not available at the time of reporting, Owner/Operators must submit an initial report within the specified timeframe and provide supplemental information within 24 hours of it becoming available. (SD 1580-21-01, SD 1582-21-01, and SD Pipeline-2021-01)	**REPORTING CYBERSECURITY INCIDENTS.** (a) Unless otherwise directed by TSA, each owner/operator identified in [parts 1580, 1582, 1584, and 1586 as subject to the requirements in this section] must notify CISA of any Reportable Cybersecurity Incidents, as defined in the TSA Cybersecurity Lexicon, as soon as practicable, but no later than 24 hours after a Reportable Cybersecurity Incident is identified. (b) Reports required by this section must be made by the methods prescribed by TSA. All information that must be reported to TSA or CISA under this section is sensitive security information subject to the protections of part 1520 of this chapter. (c) The report to CISA must include the following information, as available to the reporting owner/operator at the time of the report: (1) The name of the reporting individual and contact information, including a telephone number and email address. The report must also explicitly specify that the information is being reported in order to satisfy the reporting requirements in TSA's Regulations. (2) The affected rail system(s) or facilities, including identifying information and location. (3) Description of the threat, incident, or activity, to include: (i) Earliest known date of compromise; (ii) Date of detection; (iii) Information about who has been notified and what action has been taken; (iv) Any relevant information observed or collected by the owner/operators, such as malicious Internet Protocol addresses, malicious domains, malware hashes and/or samples, or the abuse of legitimate software or accounts; and (v) Any known threat information, to include information about the source of the threat or cybersecurity incident, if available. (4) A description of the incident's impact or potential impact on Information or Operational Technology systems and operations. This information must also include an assessment of actual or imminent adverse impacts to service operations, operational delays, and/or data theft that have or are likely to be incurred, as well as any other information that would be informative in understanding the impact or potential impact of the cybersecurity incident. (5) A description of all responses that are planned or under consideration, to include, for example, a reversion to manual operations of train movement and control, if applicable. (6) Any additional information not specifically required by this section, but which is critical to an understanding of the threat and owner/operator's response to a reportable cybersecurity incident. (d) If all the required information is not available at the time of reporting, owner/operators must submit an initial report within the specified timeframe and supplement as additional information becomes available. Reporting cybersecurity incidents. (Proposed 1580.325, 1582.225, 1584.107, and 1586.225.)
	Incident Mitigation (RS.MI): Activities are performed to prevent expansion of an event and mitigate its effects	**5.A. Incident Planning and Preparedness.** Organizations are capable of safely and effectively recovering from a cybersecurity incident.	*See* ***CYBERSECURITY INCIDENT RESPONSE PLAN*** *(above)*	
RECOVER (RC)	**Incident Recovery Plan Execution (RC.RP):** Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents	**5.A. Incident Planning and Preparedness.** Organizations are capable of safely and effectively recovering from a cybersecurity incident.	*See* ***CYBERSECURITY INCIDENT RESPONSE PLAN*** *(above)*	
	Incident Recovery Communication (RC.CO): Restoration activities are coordinated with internal and external parties.			