Enhancing Surface Cyber Risk Management Instructions

CRM Requirement	Summary of Requirement
Conduct an enterprise-wide Cybersecurity Evaluation (CSE) - 1580.305, 1582.205, and 1586.205	Record keeping. Owner/operators would be required to maintain documentation of the completion of an annual CSE; which must be made available to TSA upon request. The CSE must be sufficient to determine the owner/operator's current enterprise-wide cybersecurity profile of logical/virtual and physical security controls and assess their current cybersecurity posture consistent with the target profile established through this rulemaking.
Develop and obtain TSA approval of a COIP – 1580.307, 1582.207, and 1586.207	Reporting. Owner/operators would be required to develop and submit for TSA approval a COIP that meets the security outcomes specified in the rule. This plan aligns with the existing requirements for a Cybersecurity Implementation Plan (CIP) required by the SD Pipeline-2021-02 and SD 1580/82-21-02 series. The COIP must include specific detail on exactly how the owner/operator meets the requirements for (a) governance; (b) identification of Critical Cyber Systems (CCS), network architecture, and interdependencies; (c) procedures, policies, and capabilities to protect CCSs; and (d) procedures, policies, and capabilities to detect cybersecurity incidents. The COIP must include a Plan of Action and Milestones (POAM) that identifies a schedule for the specific measures to be implemented, within 3 years, to meet all required outcomes, and any measures in place to mitigate the risks associated with not fully complying with the requirements or security outcomes.
*Designate an Accountable Executive for CRM Program – 1580.309(a), 1582.209(a), and 1586.209(a)	Reporting. Owner/operators would be required to designate an accountable executive for their CRM program in their COIP and provide that information to TSA. The information collection would include the names, titles, business telephone numbers, and business email addresses. The accountable executive is the primary individual to be contacted with regard to the owner/operator's CRM program.
Designate a Cybersecurity Coordinator – 1580.311, 1582.211, and 1586.211	Reporting. Owner/operators would be required to appoint a Primary and Alternate Cybersecurity Coordinator and submit their contact information to TSA. The Cybersecurity Coordinator, or alternate, serves as the primary contact for cyber-related intelligence information and cybersecurity-related activities and communications with TSA and CISA and must be accessible to TSA and CISA 24 hours a day, 7 days a week. The primary Cybersecurity Coordinator must be a U.S. citizen.
*Develop and submit to TSA for approval a Cybersecurity Training Program and maintain cybersecurity training records – 1580.319, 1582.219, and 1586.219.	Reporting. Owner/operators would be required to develop and submit to TSA for approval a cybersecurity training program. The program would be required to meet the requirements specified in the rule. Record Keeping. Owner/operators would be required to maintain training records for all employees and contractors with access to owner/operator IT or OT systems demonstrating employee completion of basic cybersecurity training. Owner/operators would be required to maintain training records demonstrating completion of role-based cybersecurity training for individuals designated as cybersecurity-sensitive employees.
Report Cybersecurity Incidents to CISA – 1580.325, 1582.225, 1584.107, and 1586.225	Reporting. Owner/operators would be required to report cybersecurity incidents as defined in the TSA Cybersecurity Lexicon, to CISA within 24 hours of identification. Owner/operators may be requested to provide follow-up information to CISA (as needed). Cybersecurity incident reports are submitted using the CISA Reporting System form at: . Incident reports can also be reported by calling (888) 282-0870. This collection is covered by an OMB-approved CISA information collection for cybersecurity incident reporting. See OMB control number 1670-0037. TSA would require certain OTRB owner/operators to report cybersecurity incidents; but is not proposing to require OTRB owner/operators to develop and implement a full CRM program.
Develop and Implement a Cybersecurity Incident Response Plan (CIRP) – 1580.327, 1582.227, and 1586.227	Record keeping. Owner/operators would be required to maintain documentation of a CIRP that addresses the security outcomes specified in the rule.
Develop and submit to TSA for approval a Cybersecurity Assessment Plan (CAP) that assesses effectiveness of cybersecurity measures in place and document this in a CAP annual report – 1580.329, 1582.229, 1586.229	Reporting (CAP). Owner/operators would be required to develop and submit to TSA for approval a CAP that meets the requirements specified in the rule.
Maintain documentation to establish compliance – 1580.331, 1582.231, and 1586.231 (Related to 1570.117)	Recordkeeping. TSA may request to inspect or copy documents to establish compliance as specified in the rule.

CRM Requirement	Summary of Requirement
Designate a Physical Security Coordinator (Primary and Alternate) – 1580.103, 1582.103, 1584.103, and 1586.103	Reporting. Each owner/operator is required to designate and provide to TSA the contact information of a primary and at least one alternate Physical Security Coordinator.
Report Significant Physical Security Concerns to TSA –1580.105, 1582.105, 1584.105[1], and 1586.105	Reporting. Each owner/operator is required to report Significant Physical Security Concerns to TSA. TSA is proposing a new requirement for the pipeline facilities and systems within the applicability of the CRM program to report significant physical security concerns. .

Paperwork Reduction Act Burden Statement: This is a mandatory collection of information. TSA estimates that the total average burden per response associated with this collection is approximately: 40 hours for Cybersecurity Evaluation (CSE) for Freight Rail/PTPR and 120 hours for Pipeline; 4 hours to report the COIP; 3 hours to designate an Accountable Executive for CRM Program; 3-6 hours to Designate a Cybersecurity Coordinator; 68 hours to develop a Cybersecurity Training Program; 18.75 hours to modify a Cybersecurity Training Program; 0.017 hours to maintain Cybersecurity Training records; 80 hours to develop the Cybersecurity Incident Response Plan; 14 hours to develop the Cybersecurity Assessment Plan, 2 hours for the Compliance Documentation; 0.5 hours to designate a Physical Security Coordinator; and 0.05 hours to report Significant Physical Security. An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a valid OMB control number. The control number assigned to this collection is OMB 1652-xxxx, which expires on x/xx/xxxx. Send comments regarding this burden estimate or collection to: TSA-11, Attention: PRA 1652-xxxx *Enhancing Surface Cyber Risk Management*, 6565 Springfield Center Drive, Springfield, VA 20598-6011.

1