DRAGOS
SAFEGUARDING CIVILIZATION

The Challenge of a New Directive for Railroad Carriers

U.S. Transportation Security Administration (TSA) Security Directive 1580/82-2022-01 for Rail Cybersecurity Mitigation Actions and Testing

This directive is an extension of Security Directive 1580-21-01 and includes additional guidance for implementing cybersecurity measures and controls to segregate and secure both Information Technology (IT) and Operational Technology (OT) networks through implementation of technical (network segmentation, monitoring and detection, secure remote access, vulnerability management, et al.) and procedural (asset inventory procedures, access control policies, IT-OT inter-communication identification, patch management procedures, et al.) security controls. A requirement for development of a cybersecurity assessment program has also been added that includes the execution of a Cybersecurity Architecture Design Review (CADR) to validate that the network architecture effectively isolates critical OT cyber systems from potential threats.

How Can Dragos Help Meet 1580/82-2022-01 Requirements?

Our Platform technology and Services perform or support most of the requirements for the Cybersecurity Implementation, Incident Response, and Assessment plans.

1580/82-2022-01 REQUIREMENT		DRAGOS RESOURCES
III. A.:	Identify the Owner/Operator's Critical Cyber System	Dragos Services leverages the Crown Jewel Analysis Methodology and can provide as part of an Architecture Review.
III. B. 1a:	List and descriptions of Informational Technology (IT) and Operational Technology (OT) system interdependencies	Dragos Services leverages the Crown Jewel Analysis Methodology and can provide as part of an Architecture Review.
III. B. 1b:	All external connections to the OT system	Dragos Platform performs – monitors all external connections to OT systems. Dragos Services can provide point-in-time analysis as part of an Architecture Review.
III. B. 1c:	Zone boundaries and descriptions based on criticality	Dragos Platform performs – organizes assets into zones. Integrates with firewall to enable network segmentation.

1580/82-2022-01 REQUIREMENT		DRAGOS RESOURCES
III. C.:	Implement access control measures, including for local and remote access, to secure and prevent unauthorized access to Critical Cyber Systems.	Dragos Platform detects Windows domain traffic and can help identify domain trusts across zone boundaries.
III. D. 1a:	Prevent malicious email	Not applicable.
III. D. 1b:	Prohibit malicious ingress/egress communications	Dragos Platform integrates asset addresses with firewalls for policies to block malicious communication.
III. D. 1c:	Control impact of malicious web traffic	Dragos Platform supports by monitoring for threat behaviors resulting from malicious web traffic.
III. D. 1d:	Block and prevent unauthorized code	Dragos Platform integrates asset addresses with firewall for policies to inspect code delivered to OT assets.
III. D. 1c:	Control impact of malicious web traffic	Dragos Platform supports by monitoring for threat behaviors resulting from malicious web traffic.
III. D. 1e:	Monitor and/or block connections from malicious Command and Control (C&C) servers	Dragos Platform monitors and integrates asset addresses with firewalls for policies to block C&C servers
III. D. 2a:	Audit unauthorized access to internet domains/ addresses	Dragos Platform monitors/audits access to internet domains/ addresses; integrates with firewall to prevent access.
III. D. 2b:	Document external communications between the OT system and baseline	Dragos Platform performs by logging communications and creating baselines.
III. D. 2c:	Identify and respond to execution of unauthorized code	Dragos Platform supports by identifying threat behaviors that may result from unauthorized code.
III. D. 2d:	Implement capabilities to define, prioritize, and drive standardized incident response (IR)	Dragos Platform performs by prioritizing alerts and providing playbooks to prescribe actions
III. D. 3a:	Continuous collection and analysis of data for intrusions and anomalies	Dragos Platform performs by logging and analyzing network traffic for threat behaviors, anomalies, and intrusions.
III. D. 3b:	Ensure data is maintained for sufficient periods to allow for investigations	Dragos Platform performs by capturing historical data events that can be replayed in a timeline view and by integrating with Security Information and Event Management (SIEM) technologies for longer term data management.
III. E. 1:	Patch management strategy	Dragos Platform supports by providing vulnerability data, corrected Common Vulnerability Scoring System (CVSS), alternative mitigation strategies, and vulnerability resolution tracking.
III. E. 2a:	Categorization methodology for patches and updates	Dragos Platform performs by providing level of severity/ criticality of vulnerabilities, alternative mitigation, and vulnerability resolution tracking.
III. F. 2a:	Assess the effectiveness of the Cybersecurity Implementation Plan	Dragos Services provides as part of the Architecture Review Suite.

1580/82-2022-01 REQUIREMENT		DRAGOS RESOURCES
III. F. 2b:	Include an architectural design review **at least once every two years**	Dragos Services provides as part of the Architecture Review Suite.
III. F. 2c:	Includes other assessment capabilities, including penetration testing and red/purple team testing	Dragos Services can provide Network Penetration Testing, Purple Team, Vulnerability Assessments, and more.
IV. C. 2a:	Hardware/software asset inventory including OT	Dragos Platform performs OT asset inventory and monitoring.
IV. C. 2b:	Firewall rules	Dragos Platform integrates asset addresses with firewall for policies.
IV. C. 2c:	Network diagrams, switch/router configs, architecture diagrams, IP addresses, VLANs	Dragos Platform supports by providing maps with asset information, including network addressing.
IV. C. 2d:	Policy, procedural, and other documents for Implementation Plan, IR Plan, and Assessment Program	Dragos Services provides through the Architecture Review Suite and Capability Maturity Assessments.
IV. C. 2e:	"Snapshot" of activity between IT and OT systems	Dragos Platform performs by monitoring all traffic to, from, and within OT networks.

If you're interested in further guidance or support in implementing an OT cybersecurity strategy based on Security Directive 1580/82-2022-01 and how the Dragos Platform technology can help you effectively and efficiently reach compliance and security, connect with us at sales@dragos.com, reach out to your current account executive at Dragos, or use our contact us form.

About Dragos, Inc.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

To learn more about our technology, services, and threat intelligence offerings, visit **dragos.com** or connect with us at **sales@dragos.com**.