SmartSuite

Framework / Cybersecurity / Other

TSA Security Directive 1580/82-2022-01

TSA Security Directive 1580/82-2022-01 requires U.S. surface transportation entities to implement cybersecurity measures protecting critical infrastructure.

What it is

U.S. TSA / DHS Security Directive 1580/82-2022-01 is a regulatory directive that sets mandatory cybersecurity requirements for designated Surface Transportation Owners and Operators to strengthen infrastructure resilience and protect against cyber threats. The directive aims to enhance cybersecurity posture, reduce risk exposure, and ensure operational continuity within the surface transportation sector.

Issued by the Transportation Security Administration (TSA) and the Department of Homeland Security (DHS), this regulation applies to key freight and passenger railroads, rail transit operations, and other critical transportation systems in the United States. It covers areas including baseline cybersecurity controls, incident reporting, mitigation measures, and the development of cybersecurity implementation plans.

At a glance

PUBLISHER U.S. Department of Homeland Security (DHS)	TYPE Regulation	VERSION 2022
EFFECTIVE May 3, 2025	DOMAIN Cybersecurity	FAMILY Other
REGION United States	INDUSTRY Transportation & Logistics	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: https://www.tsa.gov/sites/default/files/tsa-security-directive-1580_82-2022-01c-and-memo-508c.pdf

Why it matters

- **Strengthen cybersecurity governance** Provide clear requirements and leadership structures to improve oversight and accountability for transportation sector cybersecurity initiatives.
- **Enhance regulatory alignment** Support compliance with federal mandates by aligning surface transportation cybersecurity practices with national security and regulatory priorities.
- **Improve threat response capabilities** Promote consistent incident reporting and response protocols, enabling faster detection and mitigation of security incidents across the sector.
- **Increase audit readiness** Standardize risk management processes and documentation to help organizations proactively prepare for regulatory audits and reviews.

© 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports TSA SD 1580/82-2022-01

TSA Directive Control Library

Structure required cybersecurity measures including access control, monitoring, segmentation, and incident reporting obligations.

Critical Systems and Asset Identification

Track systems supporting critical transportation operations and define security boundaries.

Risk Assessments and Security Planning

Manage cybersecurity risk assessments and required security implementation plans for regulated systems.

Access Control and Network Segmentation Governance

Manage user access, authentication controls, and segmentation of critical operational networks.

Cybersecurity Incident Reporting to TSA and CISA

Track cybersecurity incidents and manage mandatory reporting to TSA and CISA.

TSA Cybersecurity Directive Compliance Reporting

Provide dashboards summarizing directive compliance status, control implementation, and audit readiness.

Common framework mappings

CIS Controls v8.1 | COBIT 2019 | ISO 27001:2022 | NIST CSF 2.0 | NIST 800-53 Rev.5 | PCI DSS 4.0.1 | SOC 2

Official resources

Security Directive 1580/82-2022-01D – Rail Cybersecurity Mitigation Actions and Testing

Defines the current performance-based cybersecurity requirements and renewal for rail operators, effective May 3, 2025 to May 2, 2026.

tsa.gov/sites/default/files/tsa-security-directive-1580_82-2022-01d-and-memo-508c.pdf

Security Directive 1580/82-2022-01C – Rail Cybersecurity Mitigation Actions and Testing

Specifies inclusion of Positive Train Control (PTC) systems as Critical Cyber Systems under performance-based cybersecurity requirements, effective July 1, 2024 to May 2, 2025.

tsa.gov/sites/default/files/tsa-security-directive-1580_82-2022-01c-and-memo-508c.pdf

TSA Security Directives and Emergency Amendments – Cybersecurity

Provides an official listing and timeline of the applicable TSA surface transportation cybersecurity directives, including the 1580/82-2022-01 series.

tsa.gov/sd-and-ea

Frequently asked questions

What is TSA Security Directive 1580/82-2022-01 used for?

This directive establishes mandatory cybersecurity measures for surface transportation owner/operators, including rail and other key infrastructure providers. It aims to strengthen defenses against cyber threats by requiring specific risk management and incident response practices to protect critical systems used in transportation.

Is TSA Security Directive 1580/82-2022-01 mandatory or voluntary?

TSA Security Directive 1580/82-2022-01 is a mandatory regulatory requirement for designated U.S. surface transportation entities. Failure to comply with the directive may result in enforcement actions and penalties from the Transportation Security Administration or Department of Homeland Security.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

Who does TSA Security Directive 1580/82-2022-01 apply to?

The directive applies to owners and operators of specified U.S. freight and passenger railroad carriers, rail transit systems, and certain other surface transportation systems. Entities designated as “critical infrastructure” within the transportation sector must adhere to its provisions.

What key cybersecurity measures does the directive require?

The directive requires organizations to develop and submit a Cybersecurity Implementation Plan, conduct annual cybersecurity assessments, report significant cybersecurity incidents within 24 hours, and designate a Cybersecurity Coordinator. Additional requirements include network segmentation, access control, and ongoing vulnerability management.

How should organizations implement TSA Security Directive 1580/82-2022-01?

Implementation involves conducting a detailed risk assessment, establishing cybersecurity policies and technical controls, and maintaining documentation as required by the TSA. Organizations must also train their workforce, implement incident response capabilities, and ensure continuous monitoring for compliance.

How does TSA Security Directive 1580/82-2022-01 relate to other cybersecurity frameworks?

The directive aligns with principles found in NIST Cybersecurity Framework (NIST CSF) and other federal requirements, but it contains sector-specific obligations and stricter reporting timelines. Organizations may leverage compliance with existing frameworks, but must ensure all TSA-specific directives are fully addressed.

What are the ongoing compliance and audit requirements for TSA Security Directive 1580/82-2022-01?

Ongoing compliance includes maintaining up-to-date cybersecurity plans, submitting incident reports, participating in audits or assessments by TSA, and promptly remediating identified deficiencies. Documentation and evidence of compliance activities must be kept current and accessible for regulatory inspections.

How would SmartSuite support TSA Security Directive 1580/82-2022-01?

SmartSuite can help organizations manage compliance with TSA Security Directive 1580/82-2022-01 by providing centralized tools for risk tracking, control management, and evidence collection. It facilitates the documentation of cybersecurity assessments, supports audit readiness through workflow automation, and generates compliance reports for effective oversight and regulatory response.

License included / downloadable: Yes TSA Security Directive 1580/82-2022-01 is publicly available from TSA/DHS official publications. License included with platform

Full framework page and mappings: smartsuite.com/frameworks/tsa-security-directive-1580-82-2022-01-surface-transportation

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.