SmartSuite

Framework / Cybersecurity / Other

TSA Security Directive 1580/82-2022-01, Rail Cybersecurity Mitigation Actions and Testing

TSA Security Directive 1580/82-2022-01 requires designated freight and passenger railroads to run a TSA-approved cybersecurity plan for segmentation, access control, monitoring and patching.



What it is

TSA Security Directive 1580/82-2022-01, "Rail Cybersecurity Mitigation Actions and Testing," is a Transportation Security Administration directive that requires freight railroads identified in 49 CFR 1580.101, and other TSA-designated freight and passenger railroads, to run a TSA-approved Cybersecurity Implementation Plan and a Cybersecurity Assessment Plan for their Critical Cyber Systems. TSA first issued it on October 18, 2022 and renews it each year; the current revision, 01E, is effective May 3, 2026 through May 2, 2027 and supersedes 01D.

At a glance

PUBLISHER
Transportation Security Administration (TSA), U.S. Department of Homeland Security

TYPE
Regulation

VERSION
SD 1580/82-2022-01E (supersedes 01D)

EFFECTIVE
May 3, 2026 through May 2, 2027 (revision 01E); series first effective October 24, 2022

DOMAIN
Cybersecurity

FAMILY
Other

REGION
United States

INDUSTRY
Transportation & Logistics

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

Source: tsa.gov/sd-and-ea

Why it matters

- **Outcomes, not a control list** Section III states four outcomes and lets each railroad describe its own measures in a plan TSA approves, so the plan becomes the standard TSA inspects against.
- **OT and IT separation** Zone boundaries, interdependencies and external connections must be listed, and OT services may not traverse the IT system unless encrypted or otherwise secured.
- **Named detection and patching duties** Section III.D lists capabilities such as blocking malicious email and unauthorized code, and III.E requires prioritizing the CISA Known Exploited Vulnerabilities Catalog.
- **Assessment with a fixed rhythm** Section III.F requires an architecture design review within 12 months of plan approval and every two years after, and at least one-third of measures assessed each year.

© 2026 SmartSuite Inc. All rights reserved.

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

Critical Cyber System Register

Record each IT and OT system, its interdependencies, external connections and whether it counts as a Critical Cyber System, including PTC systems.

Implementation Plan Requirements

Break the TSA-approved plan into section III.B to III.E measures with owners, schedule dates and implementation status.

Segmentation and Access Control

Track zone boundaries, multi-factor authentication or compensating controls for OT, shared accounts and domain trust reviews.

Patching and Vulnerability Tracking

Log patch decisions, Known Exploited Vulnerabilities priorities and the mitigations and timelines for OT systems that cannot be patched.

Assessment Plan Calendar

Schedule the architecture design review and the one-third annual coverage, record results and assemble the annual report to TSA.

TSA Records and Amendments

Keep the records section IV lists, the plan amendment requests due within 50 days and the revision and expiration dates of each directive renewal.

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

TSA Security Directive 1580/82-2022-01E (May 2026)

The current revision of the rail cybersecurity directive, with its transmittal memo.

tsa.gov/sites/default/files/signed_security_directive_1580_82-2022-01e_and_transmittal_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

Who must comply with TSA SD 1580/82-2022-01?

Section II.A applies the directive to freight railroad owner/operators subject to 49 CFR 1580.101 and to additional freight and passenger railroad owner/operators that TSA designates and notifies, with specific compliance deadlines. The requirements attach to Critical Cyber Systems. An owner/operator with none must notify TSA in writing within 60 days of the effective date.

Which revision is current, and does it change the requirements?

Revision 01E is effective May 3, 2026 through May 2, 2027 and supersedes 01D. TSA's transmittal memo of May 1, 2026 says there are no substantive revisions: changes are limited to the effective date, expiration date, series letter and formatting. The series was first issued in October 2022 and is renewed annually.

What must the Cybersecurity Implementation Plan cover?

Section II.B requires a TSA-approved plan describing, in detail, the defense-in-depth measures for sections III.A to III.E: identification of Critical Cyber Systems, network segmentation, access control, continuous monitoring and detection, and patching. After approval the railroad implements the plan on its own schedule, and it must request an amendment within 50 days of a permanent change under section VI.

How often must measures be assessed and reported?

Section III.F requires a Cybersecurity Assessment Plan submitted within 60 days of plan approval and updated annually for TSA approval. It must include an architecture design review within the first 12 months and at least every two years after, a schedule that assesses at least one-third of the measures each year and 100 percent over any three years, and an annual report of results to TSA.

Is there a final rule that replaces the directive?

Not as far as TSA's pages and the Federal Register show. TSA's November 7, 2024 proposed rule, Enhancing Surface Cyber Risk Management (89 FR 88488), would impose cyber risk management requirements on certain rail and pipeline owner/operators, and the directive says TSA intends to codify its requirements through rulemaking. Until a final rule is published, the renewed directive remains the instrument railroads follow.

License included / downloadable: Yes The directive is a U.S. government document that TSA publishes free on tsa.gov and has not marked as Sensitive Security Information. Plans, reports and results that railroads submit to TSA are Sensitive Security Information under 49 CFR part 1520. The platform links to TSA's page.

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

© 2026 SmartSuite Inc. All rights reserved.