Rail and intermodal interface security checklist

For: Rail planners, IT and security leads of a terminal with on-dock or near-dock rail, and the railroad and rail-operator teams that exchange data with it

One line per point, in five families. Walk the list with whoever runs the terminal operating system (TOS) and the rail interface, whoever runs the train appointment or slot system, and the person who signs the agreements with the railroads. For each line, write who owns it, where the evidence is kept and its status. Start with the register of rail partners and channels (G1) and the per-partner accounts (A1): most of the rest depends on knowing which railroad or rail operator is connected, by which channel, with which account. For the EDI and API channel mechanics, the crane OT and the truck side, follow the links in each family to the pages that cover them in full.

Scope. Covers the seam between a terminal and the railroads and rail operators that serve it: the EDI and API messages they exchange about railcars and trains, the train appointment or slot system, the accounts the railroads and on-dock rail operators hold on the terminal's systems, the on-dock rail interface (rail-mounted gantry cranes and the automatic rail gate or OCR that reads railcar and container identifiers), and the rail-specific obligations that bind a rail or intermodal operator. It does not replace the port facility security plan, the contracts with the railroads or legal advice on your own jurisdiction. It is the rail layer on top of three other pages: the EDI and API integration security checklist (channels, keys, replay), the OT security checklist for cranes and yard equipment, and the truck appointment portal security checklist.

The five families

• **G · The terminal and rail data seam**: One known gateway for the rail messages, release and hold references kept secret, each railroad authorised only for its own railcars, every message validated and reconciled with the physical interchange.

• **S · Train appointment and slot systems**: One named account per rail operator, slot and window changes recorded, the booking API rate-limited and watched for bots, and no slot that opens a gate or interchange on its own.

• **A · Railroad and rail-operator access**: Every railroad and rail-operator user and service account is known, sees only its own trains and cars, uses multi-factor authentication, and is removed the day the person or the contract leaves.

• **I · The on-dock rail interface and OT**: The rail-mounted gantry cranes, the automatic rail gate or OCR and the rail yard network are segmented from IT and the Internet, and the rail interface goes to a safe state when the data link drops.

• **R · Rail obligations and incident reporting**: Know which rail and port regime applies, keep a cyber point of contact reachable by the authority, report significant incidents on time, segment OT from IT as the directives ask, and test and audit the measures.

Status

• in place · the evidence exists, is dated and someone owns it

• partial · the practice exists but the evidence is missing, out of date or covers only some partners or trains

• missing · nothing yet

• not applicable · write down why

Summary sheet · terminal: _____ · rail partner: _____ · date: _____

Check	References	Status	Owner
G1 · One register of rail partners and channels	NIS2 Art. 21(2)(d) · 33 CFR 101.650 · EDI and API checklist A1		
G2 · Release and hold references are secrets	NIST SP 800-82r3 6.2 · IMO Rev.4 3.5.3 · EDI and API checklist D		
G3 · Each railroad authorised only for its own railcars	OWASP API Security Top 10 2023 (API1) · NIS2 Art. 21(2)(i) · EDI and API checklist D2		
G4 · Rail messages validated before they are acted on	NIST SP 800-82r3 6.2 · IMO Rev.4 3.5.3 · EDI and API checklist D1		
G5 · The data is reconciled with the physical interchange	IMO Rev.4 3.5.4 · NIST SP 800-82r3 5.3		
S1 · One named account per rail operator	33 CFR 101.650 · NIS2 Art. 21(2)(i)(j) · Truck appointment checklist A1		
S2 · Slot and window changes recorded	OWASP Automated Threats (OAT-021, OAT-005) · NIS2 Art. 21 · GDPR Art. 5, 32 · Truck appointment checklist C		
S3 · The booking API rate-limited and watched for bots	OWASP API Security Top 10 2023 (API4, API6) · OWASP Automated Threats (OAT-005) · Truck appointment checklist D, F		
S4 · A slot never opens a gate or interchange on its own	IMO Rev.4 3.5.3 · 33 CFR 101.650 · Gate and OCR security page		
A1 · Every rail user and service account is known	NIST SP 800-82r3 6.2 · NIS2 Art. 21(2)(i) · TOS access checklist		
A2 · Each account sees only its own trains and cars	NIS2 Art. 21 · 33 CFR 101.650 · OWASP API Security Top 10 2023 (API1, API5)		
A3 · Multi-factor authentication and named accounts	33 CFR 101.650 · NIS2 Art. 21(2)(j) · TSA SD 1580/82-2022-01 · EDI and API checklist C		
A4 · Joiners, movers and leavers handled on the day	33 CFR 101.650 · NIS2 Art. 21(2) · EDI and API checklist A5		
A5 · Railroad remote access requested and logged	NIST SP 800-82r3 6.2.10 · 33 CFR 101.650(h) · TOS access checklist		
I1 · Rail-mounted gantries on their own OT segment	NIST SP 800-82r3 6.1, 5.2.3.1 · CLC/TS 50701 (general ref) · OT security checklist for cranes and yard equipment		
I2 · The automatic rail gate and OCR treated as network devices	33 CFR 101.650 · NIST SP 800-82r3 6.1 · Gate and OCR security page		
I3 · The rail yard network segmented from IT and the Internet	IMO Rev.4 3.5.3.3 · 33 CFR 101.650(e)(h) · TSA SD 1580/82-2022-01		
I4 · A safe state when the rail data link drops	NIST SP 800-82r3 5.3.1, 3.3.9 · OT security checklist (S2, D3)		
R1 · Know which rail and port regime applies	TSA SD 1580/82-2022-01 · 49 CFR 1580 · NIS2 · Dir. (EU) 2022/2557 · 33 CFR 101.650 · IMO Rev.4		
R2 · A cyber point of contact reachable by the authority	TSA SD 1580/82-2022-01 · 49 CFR 1580 · NIS2 · IMO Rev.4		
R3 · Report significant incidents on time	NIS2 Art. 23 · TSA SD 1580/82-2022-01 · 49 CFR 1580 · 33 CFR 101.650		
R4 · Segment OT from IT as the directives ask	TSA SD 1580/82-2022-01 · 33 CFR 101.650(e) · NIS2 Art. 21 · Dir. (EU) 2022/2557		

Check	References	Status	Owner
R5 · Test and audit the measures	TSA SD 1580/82-2022-01 · NIS2 Art. 21 · TSA NPRM 89 FR 88488 (7 Nov 2024)		

G · The terminal and rail data seam

One known gateway for the rail messages, release and hold references kept secret, each railroad authorised only for its own railcars, every message validated and reconciled with the physical interchange.

G1 · One register of rail partners and channels *(NIS2 Art. 21(2)(d) · 33 CFR 101.650 · EDI and API checklist A1)*

What to check: The terminal keeps a register of every railroad and rail operator it exchanges data with, and of every channel used (EDI interchanges for railcar consists, waybills, interchange and release or hold messages; any REST API; any file transfer), with the owner on each side and the environment (test or production).

Why: A seam you have not listed is a seam you cannot protect. The EDI and API integration security checklist asks for a register of every connected partner before anything else; NIS2 lists supply chain security and asset management among the minimum risk measures (Article 21(2)); the US Coast Guard rule asks for a Cybersecurity Assessment that identifies the systems and their connections.

Evidence to hold: [ ] The register of rail partners and channels, with the date of the last update · [ ] For each channel, the owner on the terminal side and on the railroad side, and the environment

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

G2 · Release and hold references are secrets *(NIST SP 800-82r3 6.2 · IMO Rev.4 3.5.3 · EDI and API checklist D)*

What to check: The references that let a railcar or a container move or leave (release orders, holds, pin or reference numbers in the rail messages) are treated as secrets: not shown in error pages, logs, support tickets or e-mails, and not guessable in sequence.

Why: Whoever holds a valid release reference can move a box. The EDI and API integration security checklist treats release references as secrets to prevent misdelivery; NIST SP 800-82 Rev. 3 asks to protect the confidentiality and integrity of OT information in transit and at rest; IMO Rev.4 covers the protection of data exchanged with external parties.

Evidence to hold: [ ] Where release and hold references appear, and the rule that keeps them out of logs, errors and e-mails · [ ] A check that references are random, not sequential

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

G3 · Each railroad authorised only for its own railcars *(OWASP API Security Top 10 2023 (API1) · NIS2 Art. 21(2)(i) · EDI and API checklist D2)*

What to check: A railroad or rail operator can read and act on the railcars, trains and containers that belong to its own moves only, never on another carrier's. The terminal checks the sender of each message against what it is allowed to say about a given railcar or container.

Why: Broken object level authorisation (one partner reaching another's objects) is the first risk of the OWASP API Security Top 10 (2023). The EDI and API integration security checklist asks to check the sender against what it may say about each container; NIS2 lists access control among the minimum measures.

Evidence to hold: [ ] The authorisation rule that binds a railroad or rail operator to its own railcars and trains · [ ] A test that one partner cannot read or change another's railcars

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

G4 · Rail messages validated before they are acted on *(NIST SP 800-82r3 6.2 · IMO Rev.4 3.5.3 · EDI and API checklist D1)*

What to check: Each inbound rail message (consist or car-location message, waybill, interchange report, release or hold) is checked for structure, for the fields that must be present, and for a sender that is allowed to send it, before the TOS acts on it. A malformed or unexpected message is rejected and logged, not half-processed.

Why: NIST SP 800-82 Rev. 3 asks to validate the syntactic and semantic correctness of inputs to OT systems. The EDI and API integration security checklist validates every interchange before processing; IMO Rev.4 asks to protect the integrity of data used by critical systems.

Evidence to hold: [ ] The validation rules per rail message type and where rejects are logged · [ ] A sample of rejected messages and what happened next

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

G5 · The data is reconciled with the physical interchange *(IMO Rev.4 3.5.4 · NIST SP 800-82r3 5.3)*

What to check: What the rail messages say (the cars on the train, their holds and releases) is reconciled with what is physically interchanged at the rail gate or on the rail tracks, and a mismatch stops the move until a person clears it, rather than letting the data or the barrier decide alone.

Why: A confident wrong answer is worse than a crash: the feed says one thing, the yard does another. IMO Rev.4 asks to detect events that could affect operations; NIST SP 800-82 Rev. 3 describes the need to verify that the process state matches the control information, with a human in the loop for consequential decisions.

Evidence to hold: [ ] The reconciliation step between the rail data and the physical interchange, and who clears a mismatch · [ ] A record of the last mismatches and how they were resolved

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

S · Train appointment and slot systems

One named account per rail operator, slot and window changes recorded, the booking API rate-limited and watched for bots, and no slot that opens a gate or interchange on its own.

S1 · One named account per rail operator *(33 CFR 101.650 · NIS2 Art. 21(2)(i)(j) · Truck appointment checklist A1)*

What to check: Every person who books, changes or cancels a train slot or a rail delivery or pick-up window has a personal account; no login is shared by a planning desk, a shift or a group, and no account is lent to a third party. The terms of use say so.

Why: A shared login cannot be traced to a person, cannot be removed when one person leaves and cannot carry multi-factor authentication properly. The truck appointment portal security checklist makes the same point for trucking companies; the US Coast Guard rule asks for separate credentials and the removal of a user's credentials when the user leaves; NIS2 lists access control among the minimum measures.

Evidence to hold: [ ] The terms of use with the one-person-one-account rule for rail bookings · [ ] A list of accounts showing one named person per account, no generic names

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

S2 · Slot and window changes recorded *(OWASP Automated Threats (OAT-021, OAT-005) · NIS2 Art. 21 · GDPR Art. 5, 32 · Truck appointment checklist C)*

What to check: A train slot or rail window belongs to the operator that booked it; every change of operator, train or time is recorded with who made it and when, so that hoarding, resale and last-minute swaps are visible.

Why: The truck appointment portal security checklist treats a slot as belonging to the company that booked it and keeps a history of every change; OWASP Automated Threats describes denial of inventory and scalping, where slots are hoarded or resold; NIS2 asks for logging and traceability. The change history holds personal data of the people who book, so the GDPR asks to keep it only as long as needed and to secure it (Articles 5 and 32).

Evidence to hold: [ ] The change history of slots and windows, kept for a stated period · [ ] A review of hoarding, resale or repeated last-minute changes

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

S3 · The booking API rate-limited and watched for bots *(OWASP API Security Top 10 2023 (API4, API6) · OWASP Automated Threats (OAT-005) · Truck appointment checklist D, F)*

What to check: The booking flows, on the web and through any API used by a rail operator's planning system, are rate-limited per account and per key, and watched for non-human patterns (bursts of bookings, mass cancellations, scraping of availability). One operator's flood cannot stop the others.

Why: OWASP lists unrestricted resource consumption and unrestricted access to sensitive business flows among the API Security Top 10 (2023), and automated slot-booking bots among the automated threats (OAT-005). The truck appointment portal security checklist asks for quotas per key and per partner.

Evidence to hold: [ ] The rate limits per account and per key, and the alert on non-human patterns · [ ] A record of the last bot or scraping events and what was done

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

S4 · A slot never opens a gate or interchange on its own *(IMO Rev.4 3.5.3 · 33 CFR 101.650 · Gate and OCR security page)*

What to check: A booked slot or window is one condition, not the whole decision: a rail move through a gate or an interchange is still checked against the release or hold, the identity of the railcar or container and the operator, and a failed check never opens a barrier silently.

Why: The gate camera and OCR security page makes the same rule for trucks: no silent barrier opening on a failed check. IMO Rev.4 asks to keep a human decision for consequential actions; the US Coast Guard rule asks to control access to critical systems.

Evidence to hold: [ ] The rule that lists what is checked before a rail move, beyond the booking · [ ] The behaviour on a failed check (hold, manual lane, no silent opening)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

A · Railroad and rail-operator access

Every railroad and rail-operator user and service account is known, sees only its own trains and cars, uses multi-factor authentication, and is removed the day the person or the contract leaves.

A1 · Every rail user and service account is known *(NIST SP 800-82r3 6.2 · NIS2 Art. 21(2)(i) · TOS access checklist)*

What to check: The terminal has a list of every railroad and rail-operator user and every service account (machine login, API key, SFTP account) that can read or write its systems, with the holder, the partner, the purpose and the systems it reaches.

Why: The TOS access hardening checklist asks for a list of every privileged and interface account before anything else; NIST SP 800-82 Rev. 3 makes a complete account inventory part of access control; NIS2 lists access control among the minimum measures.

Evidence to hold: [ ] The list of rail users and service accounts, dated, with holder, partner and systems · [ ] The owner on the terminal side of each service account

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

A2 · Each account sees only its own trains and cars *(NIS2 Art. 21 · 33 CFR 101.650 · OWASP API Security Top 10 2023 (API1, API5))*

What to check: A railroad or rail-operator account is given the least privilege it needs: it reads and acts on its own trains, railcars and containers only, and cannot see another carrier's data or reach systems it has no business with.

Why: Least privilege is a minimum measure of NIS2 (Article 21) and of the US Coast Guard rule; broken object level and function level authorisation are the first risks of the OWASP API Security Top 10 (2023). The TOS access hardening checklist asks that each partner sees only its own data.

Evidence to hold: [ ] The role or scope given to each rail account, matched to least privilege · [ ] A test that an account cannot reach another carrier's data or an admin function

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

A3 · Multi-factor authentication and named accounts *(33 CFR 101.650 · NIS2 Art. 21(2)(j) · TSA SD 1580/82-2022-01 · EDI and API checklist C)*

What to check: Each human rail user signs in with a named account and multi-factor authentication; service accounts use keys or tokens kept in a vault, not a person's password, and the keys are rotatable and revocable.

Why: The US Coast Guard rule and NIS2 (Article 21(2)(j)) ask for multi-factor authentication; the TSA rail cybersecurity directive asks to control access to critical cyber systems to prevent unauthorised access. The EDI and API integration security checklist keeps one scoped credential per integration in a vault.

Evidence to hold: [ ] The MFA setting for rail users, and where the service keys and tokens are kept · [ ] The rotation and revocation procedure for rail service credentials

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

A4 · Joiners, movers and leavers handled on the day *(33 CFR 101.650 · NIS2 Art. 21(2) · EDI and API checklist A5)*

What to check: When a railroad or rail-operator person joins, changes role or leaves, their access is created, changed or removed the same day; when a contract with a railroad or rail operator ends, all of its accounts, keys and SFTP logins are closed.

Why: The US Coast Guard rule asks for the removal of a user's credentials when the user leaves; the EDI and API integration security checklist removes a partner on the day it leaves; NIS2 lists access control and asset management among the minimum measures. An account nobody closed is the way back in.

Evidence to hold: [ ] The joiner, mover and leaver procedure for rail partners, with the last leavers handled · [ ] The offboarding record for the last railroad or rail-operator contract that ended

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

A5 · Railroad remote access requested and logged *(NIST SP 800-82r3 6.2.10 · 33 CFR 101.650(h) · TOS access checklist)*

What to check: When a railroad or a rail-operator supplier needs to reach a terminal system from outside (to read a feed, run a diagnostic or support an interface), the access is requested, limited to the stated job, authenticated, logged and switched off at the end.

Why: NIST SP 800-82 Rev. 3 asks that remote access be provided only if justified and limited to the business need, requested through a known process, and never allowed to bypass safety or security controls. The TOS access hardening checklist records every third-party session; the US Coast Guard rule logs IT connections.

Evidence to hold: [ ] The remote access procedure for railroads and rail suppliers · [ ] The record of the last sessions (who, which system, why, start and end)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

I · The on-dock rail interface and OT

The rail-mounted gantry cranes, the automatic rail gate or OCR and the rail yard network are segmented from IT and the Internet, and the rail interface goes to a safe state when the data link drops.

I1 · Rail-mounted gantries on their own OT segment *(NIST SP 800-82r3 6.1, 5.2.3.1 · CLC/TS 50701 (general ref) · OT security checklist for cranes and yard equipment)*

What to check: The rail-mounted gantry cranes and any automation at the rail head are on their own operational technology (OT) segment, with the inventory, zoning, vendor access, patching and safety rules of the OT security checklist for cranes and yard equipment applied to them.

Why: A rail-mounted gantry is OT like any other crane: NIST SP 800-82 Rev. 3 asks to group it into a zone, keep an inventory and control vendor remote access and patching. The OT security checklist for cranes and yard equipment covers all of this; this line is the reminder to apply it to the rail head too. For the railway side of such equipment, CLC/TS 50701 adapts the IEC 62443 industrial-cybersecurity approach to rail (general reference).

Evidence to hold: [ ] The rail-head equipment in the OT inventory and zone model · [ ] The OT checklist run for the rail-mounted gantries

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

I2 · The automatic rail gate and OCR treated as network devices *(33 CFR 101.650 · NIST SP 800-82r3 6.1 · Gate and OCR security page)*

What to check: The cameras and OCR that read railcar numbers, container identifiers and seals at the rail gate or on the tracks are inventoried, segmented, patched and access-controlled as network devices, and the data they capture is kept to what is needed, as on the gate camera and OCR security page.

Why: The gate camera and OCR security page treats cameras and OCR as network devices with default passwords, firmware, remote vendor access and logs to manage, and limits the personal data captured. 33 CFR 101.650 asks to segment and log; NIST SP 800-82 Rev. 3 asks to inventory and patch every device.

Evidence to hold: [ ] The rail gate cameras and OCR in the device inventory and network diagram · [ ] The retention rule for what the rail OCR captures

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

I3 · The rail yard network segmented from IT and the Internet *(IMO Rev.4 3.5.3.3 · 33 CFR 101.650(e)(h) · TSA SD 1580/82-2022-01)*

What to check: The network that carries the rail interface (the gantry controls, the rail gate and OCR, the positioning and the link to the TOS) is segmented from the office network and from the Internet, with only the documented flows crossing the boundary, each of them logged.

Why: IMO Rev.4 asks to segment OT networks from IT networks and to limit exploitable services on the Internet; 33 CFR 101.650 requires segmentation between IT and OT, with every IT-OT connection logged and monitored, and a written justification for any remotely accessible OT; the TSA rail cybersecurity directive asks to segment so OT can keep operating if IT is compromised.

Evidence to hold: [ ] The network diagram showing the rail segment separated from IT, with the conduits · [ ] The log of the IT-OT connections of the rail interface and who reviews it

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

I4 · A safe state when the rail data link drops *(NIST SP 800-82r3 5.3.1, 3.3.9 · OT security checklist (S2, D3))*

What to check: It is written what the rail interface does when the link to the TOS or the rail data feed is lost: the rail-head equipment goes to or stays in a safe state, moves stop rather than run on stale data, and the restart order puts safety first.

Why: NIST SP 800-82 Rev. 3 describes fail-safe design and asks organisations to define the thresholds at which components operate with reduced capability, and to prioritise safety before restarting after an incident. A rail move on stale or missing data is how the wrong car leaves.

Evidence to hold: [ ] The documented behaviour of the rail interface on loss of the data link · [ ] The result of the last test, done in a maintenance window, and the restart order

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

R · Rail obligations and incident reporting

Know which rail and port regime applies, keep a cyber point of contact reachable by the authority, report significant incidents on time, segment OT from IT as the directives ask, and test and audit the measures.

R1 · Know which rail and port regime applies (TSA SD 1580/82-2022-01 · 49 CFR 1580 · NIS2 · Dir. (EU) 2022/2557 · 33 CFR 101.650 · IMO Rev.4)

What to check: The terminal and its rail partners write down which obligations bind them: in the United States, the TSA rail cybersecurity directive and the freight rail security regulations for designated railroads, and the US Coast Guard cyber rule at the port facility; in the European Union, NIS2 and the critical-entity resilience directive where rail and port transport are covered; and the IMO guidelines and the port facility security plan where the rail interface touches the port.

Why: The duties differ by place and by who you are. The TSA directive binds designated passenger and freight railroads; the freight rail security regulations set the security coordinator and reporting duties; NIS2 covers transport, including rail and ports, as an essential or important sector, and the critical-entity resilience directive adds physical resilience; the US Coast Guard rule and IMO cover the port facility.

Evidence to hold: [ ] The written mapping of which regime applies to the terminal and to each rail partner · [ ] The named owner of rail and port cyber compliance

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

R2 · A cyber point of contact reachable by the authority (TSA SD 1580/82-2022-01 · 49 CFR 1580 · NIS2 · IMO Rev.4)

What to check: Each party keeps a named cybersecurity point of contact (and a deputy) reachable by the relevant authority at all times, and the contact details are kept up to date with that authority.

Why: The TSA freight rail security regulations and the rail cybersecurity directives ask designated railroads to designate a cybersecurity coordinator available to TSA and CISA; NIS2 and the critical-entity resilience directive expect a point of contact for the competent authority; IMO and the US Coast Guard rule expect a security officer at the port facility.

Evidence to hold: [ ] The named cyber point of contact and deputy, and how the authority reaches them · [ ] The date the contact details were last confirmed with the authority

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

R3 · Report significant incidents on time (NIS2 Art. 23 · TSA SD 1580/82-2022-01 · 49 CFR 1580 · 33 CFR 101.650)

What to check: There is a written procedure that says, for a significant cyber incident on the rail or port interface, who is told, by when and how: the national authority or CSIRT under NIS2, CISA under the US rail rules, and the US Coast Guard or National Response Center at the port facility, with the deadlines each one sets.

Why: Reporting is a legal duty with clocks. NIS2 sets staged reporting (an early warning within 24 hours, a notification within 72 hours, a final report within one month); the US rail security rules ask designated railroads to report significant cyber incidents to CISA; the US Coast Guard rule and the National Response Center take reports at the port facility.

Evidence to hold: [ ] The incident reporting procedure with the authorities, deadlines and channels for the rail and port interface · [ ] The result of the last exercise or real report

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

R4 · Segment OT from IT as the directives ask (TSA SD 1580/82-2022-01 · 33 CFR 101.650(e) · NIS2 Art. 21 · Dir. (EU) 2022/2557)

What to check: The rail and port OT (the rail interface, the gantries, the gate and OCR) is segmented from IT so that one can keep operating safely if the other is compromised, as the rail cybersecurity directive and the US Coast Guard rule require; this is the same segmentation as family I, checked here against the obligation.

Why: The TSA rail cybersecurity directive asks designated railroads to segment networks so OT and IT can each keep operating if the other is compromised; the US Coast Guard rule requires segmentation between IT and OT with every connection logged; NIS2 and the critical-entity resilience directive expect proportionate technical and organisational measures.

Evidence to hold: [ ] The segmentation evidence of family I, mapped to the directive and the rule · [ ] The last review of the IT-OT boundary of the rail and port interface

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

R5 · Test and audit the measures *(TSA SD 1580/82-2022-01 · NIS2 Art. 21 · TSA NPRM 89 FR 88488 (7 Nov 2024))*

What to check: The rail and port cyber measures are tested and audited on a schedule, the gaps are tracked to closure, and the results feed the implementation or security plan; a proposed US surface-transportation rule would make such a cyber risk management programme a standing requirement for certain rail operators.

Why: The TSA rail cybersecurity directive asks designated railroads to run a Cybersecurity Assessment Program that regularly tests and audits the measures and resolves vulnerabilities; NIS2 (Article 21) asks for policies to assess the effectiveness of the measures; the US surface cyber risk management proposal of 7 November 2024 would require a cyber risk management programme, assessments and a plan for certain pipeline and rail operators.

Evidence to hold: [ ] The test and audit schedule for the rail and port cyber measures, and the open gaps with owners and dates · [ ] The last assessment report and how it fed the plan

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

Sources (public, dated)

NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security, September 2023.
https://csrc.nist.gov/pubs/sp/800/82/r3/final

IMO, MSC-FAL.1/Circ.3/Rev.4, Guidelines on maritime cyber risk management, 28 May 2026.
https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.4.pdf

eCFR, 33 CFR 101.650, Cybersecurity measures (US Coast Guard rule for the port facility), in force since 16 July 2025, read on 11 November 2026.
https://www.ecfr.gov/current/title-33/chapter-I/subchapter-H/part-101/subpart-F/section-101.650

Directive (EU) 2022/2555 (NIS2): Annex I covers transport incl. rail and ports; Article 21 risk measures (access control (i), multi-factor authentication (j), supply chain (d)); Article 23 incident reporting, 14 December 2022.
https://eur-lex.europa.eu/eli/dir/2022/2555/oj

Directive (EU) 2022/2557 on the resilience of critical entities (CER): transport, incl. rail infrastructure managers, as critical entities; applies from 18 October 2024, 14 December 2022 (OJ L 333, 27 December 2022).
https://eur-lex.europa.eu/eli/dir/2022/2557/oj

US TSA, Security Directive 1580/82-2022-01, Enhancing Rail Cybersecurity (segment OT/IT, access control, continuous monitoring, risk-based patching, Cybersecurity Implementation Plan and Assessment Program), for designated passenger and freight railroads (TSA announcement), issued 18 October 2022, effective 24 October 2022.
https://www.tsa.gov/news/press/releases/2022/10/18/tsa-issues-new-cybersecurity-requirements-passenger-and-freight

eCFR, 49 CFR Part 1580, Freight Rail Transportation Security (TSA): rail security coordinator and reporting of significant security concerns; Appendix B lists security-sensitive functions, read on 11 November 2026.
https://www.ecfr.gov/current/title-49/subtitle-B/chapter-XII/subchapter-D/part-1580

US Federal Register, TSA notice of proposed rulemaking, Enhancing Surface Cyber Risk Management (89 FR 88488), proposing cyber risk management requirements for certain pipeline and rail operators (a proposal, not yet in force), 7 November 2024.
https://www.federalregister.gov/documents/2024/11/07/2024-24704/enhancing-surface-cyber-risk-management

OWASP API Security Top 10, 2023 edition (API1 broken object level authorization, API4 unrestricted resource consumption, API5 broken function level authorization, API6 unrestricted access to sensitive business flows), 5 June 2023.
https://api-security.owasp.org/editions/2023/en/0x11-t10/

OWASP Automated Threats to Web Applications (OAT-005 Scalping incl. slot-booking bots, OAT-021 Denial of Inventory), handbook read on 11 November 2026. https://owasp.org/www-project-automated-threats-to-web-applications/

Regulation (EU) 2016/679, General Data Protection Regulation (Articles 5 and 32), for personal data of rail operators and drivers in bookings and access logs, 27 April 2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj

CLC/TS 50701:2023, Railway applications — Cybersecurity (CENELEC Technical Specification, based on the IEC 62443 series; general reference, no text reproduced), approved 19 June 2023 (CENELEC news on the specification).
https://www.cencenelec.eu/news-events/news/2021/eninthespotlight/2021-06-10-new-clc-ts-50701-railways-cybersecurity/

Licence

Creative Commons Attribution 4.0 International (CC BY 4.0), https://creativecommons.org/licenses/by/4.0/ . You may copy, adapt and share this checklist, including commercially, if you credit Port Cyber Alliance and link to https://portcyberalliance.org/who-we-protect/rail-intermodal-cyber/ . Generic: no terminal, port, client, railroad or vendor is named and no figure is invented. CLC/TS 50701 is cited as a general reference; none of its text is reproduced. This checklist is not legal advice, does not replace the port facility security plan or your contracts with the railroads, and is the rail-specific layer on top of the EDI and API, the cranes, the gate and the truck pages. Port Cyber Alliance does not certify or audit terminals.