Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/resources/transportation-ot-assessment-manual/

TRANSPORTATION OT ASSESSMENT PLANNING MANUAL

Transportation OT Manual for One Evidence Record Across Modes

A port, a rail yard, a pipeline control room and an airfield can share one communications provider while answering to different regulators, different safety authorities and different people who can say stop. This manual keeps the modes and their authorities separate while building one evidence record.

Planning scope and research basis

This manual is built for a controlled assessment of rail and transit movement, road traffic management, port and terminal operations, aviation support and pipeline control at facilities in the United States. It carries the federal and modal research; the companion volume screens all fifty states so you can resolve the state safety oversight, public agency and local ownership questions that decide who must approve the work.

What the assessment produces

An approved scope, an applicability register, a process dependency map, examined evidence, safe activity records, consequence based findings, a corrective plan and a verification record, kept separately for each mode and operator. The workbook and the fillable worksheets carry the work from planning through handover.

Sources current to November 3, 2026

Current public primary sources, official program material and selected peer reviewed research support the text. Effective instruments take precedence over guidance and over this manual. The licensed ISA/IEC 62443 parts, operator security directives, facility permits and private contracts are held by the organization itself, and in transportation the operator's own issued directives and approved security plans are the instruments that matter most, so they are the first records the assessment requests through the designated security official.

Open applicability

The source register sorts binding instruments, guidance, drafts, superseded versions and open questions into their own entries. TSA renewed the pipeline and rail directives in May 2026, Security Directives Pipeline-2021-02G and 1580/82-2022-01E, effective May 3, 2026 through May 2, 2027, and aviation security programs are issued to each operator, so the operator's own issued instruments and approved plans are the first records this manual requests, read in their issued form.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Adoption and review

Complete the facility specific records and obtain the named operating, technical and compliance approvals for each mode. The questions that confirm a date, threshold or clause for each mode are summarized in OT questions to settle before field work.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-82 Rev. 4 initial public draft, Guide to Operational Technology (OT) Security (F02), A survey of cyber security management in industrial control systems (R01), Threat modeling of industrial control systems: A systematic literature review (R02), ICSSIM: A framework for building industrial control systems security testbeds (R03)

A first call to (800) 868-8189 sorts out which modes, operators and instruments a scoped assessment would have to keep apart, and that call is free.

Applying the Updated Audit Workbook

The workbook works as an execution record rather than a checklist. Every procedure row now carries the fields an auditor will read first: the exact criterion tested, the population it was tested against, the period, the sampling rationale, the permitted method, the execution date, the actual observation, the evidence identifiers and the reviewer. A row with those fields filled is a result, a row still being filled is a plan, and the workbook keeps the two visibly apart.

Pre Execution Readiness Checklist

Fill the criterion, population, period and sampling rationale first, ahead of any system work, because those four fields give the eventual observation its meaning. Record the permitted method exactly as the activity permit states it. When the work is done, enter the execution date, what was actually observed and the evidence identifiers that support it, then hand the row to the named reviewer. Keep the source register and the operating authority record apart from the procedure rows, so the directive citations and the operator approvals each keep their own trail.

Pending Scope and Governance Decisions

The open count on the Start sheet counts blank decisions, decision text that needs correcting and resolved selections that need a required record field. Treat Fields present as the prompt for qualified review, which is the step that completes the row. The responsible operating, technical and compliance people sign the approval fields once they have reviewed the work, and those signatures are what mark a workbook as reviewed rather than simply filled.

Engagement Scope and Authorization

Record every proposed exclusion, its reason and the responsible reviewer in Scope decisions so deferred work stays visible to the sponsor. The State research sheet is a separately labelled routing register: its state and sector rows are a client research checklist, and a row becomes a facility conclusion when the controlling

© 2026 Global Digital Forensics, Inc. All rights reserved.

instrument is recorded beside it. For New York work use the Clause matrix and questions Q01 to Q10 in the New York set. Current instruments and local facts that are still being gathered carry the Unresolved status, which clears when someone retrieves the text or establishes the fact.

Source Access and Revision History

The Sources sheet lists each source with the date it was reviewed. Request the current text of each source as you come to it, and keep the duty on the register while the text arrives. Use the Edition record to track your own revisions and reviews, and keep the previous version when you adopt a new one.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03)

Using this planning pack

Use this pack mode by mode, naming each mode's operating owner first. Choose evidence and methods once those owners have agreed what may be examined.

First use

Read the sector applicability pages, then the State and local applicability companion. Create one record for each legal entity, facility and regulatory program, and one for each mode where an operator runs more than one. The workbook's state and sector rows form a client research checklist, with a separate register of fifty state starting sources; a row becomes a facility determination when the operator records the instrument and the decision. Appoint a sponsor, an operating owner, a technical lead, a compliance owner and a project manager. Complete the site worksheet. Resolve the mandatory instruments and the operating permissions first, then schedule any intrusive work, and use the field authorization sheet for each approved activity.

Reading the evidence

The pack separates binding law or an incorporated instrument, agency guidance, standards and proposed assessment procedures. A citation identifies the source for a regulatory statement. A procedure description explains how the assessment team can collect evidence, and the legal obligations themselves come from the cited instruments. A rule can be effective while a particular requirement has a later compliance date, and an approved standard can reach enforcement at a later date. Record both dates and the applicable version, and take each deadline from the instrument's effective date.

Signing an assessment conclusion

The reviewer signs against the actual facility facts, the current instruments, the examined evidence, the test permissions and the open questions recorded with them. Preparing this pack readies the facility, and the assessment itself is the examination that follows. A named technical reviewer reviews the completed work, and the organization then adopts or publishes its conclusions.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03)

Working across more than one mode? The OT assessment planning library holds the other sector packs and the shared workbook, so each operator's record starts from the same structure.

Decisions before mobilization

Split the engagement by mode and by regulatory boundary as the first step, ahead of any checklist. Surface rail, urban transit, roads, maritime facilities, vessels, airports, aircraft and pipelines each require their own applicability and evidence decisions, and a separate approval for each mode is the record a regulator or an insurer expects to see.

Define the work product

Decide in writing whether the engagement is an engineering risk assessment, a gap assessment against named requirements, independent assurance, or a combination with the responsibilities separated. The decision changes the evidence standard, the sampling and the words the report may use. Name the intended recipients and who may receive the technical appendices. If the assessment team or its firm designed, installed or operates any of the controls in scope, disclose that relationship at the outset, so any description of the work as independent sits beside a recorded disclosure.

Record the facility boundary

Identify rail signaling interfaces, traction power SCADA, tunnel systems, traffic controllers, terminal cranes, access systems, airport operational support, pipeline SCADA and remote control sites. Include the identity, DNS, time, virtualization, telecommunications and backup dependencies whose failure could affect the process, because the record follows the process past the controller to the services that can actually take it down. Identify shared corporate services and third party interfaces explicitly, and record test permission for each as its own decision, so the scope names them and the permit governs them. For each legal entity record the physical address, owner, operator, sector, production or service function, permits, regulators, contracts, insurer conditions and public body status. For distributed assets list every other state, local authority and control center involved.

Record each exclusion and its effect

Document every excluded safety system, vendor appliance outside reach, firmware past vendor support, protocol outside the approval and record held elsewhere, and state in one sentence how each exclusion shapes the conclusion. An excluded critical dependency stays in the report as a visible item the sponsor accepted. Fixing the asset count at the start keeps the scope matched to the process rather than to convenience.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Release decision

The sponsor approves purpose and resources. The operating owner approves the process boundary. The compliance owner signs the applicability register. The technical lead signs the method. The project manager records the dependencies and the open items. Each signature is dated and kept with the scope record, and approval is that signed, dated entry itself.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03)

Roles and decision authority

Assign people and alternates before work starts, and record them where the field team can find them during an outage. Small organizations may combine roles, and three authorities stay explicit at every team size: who authorizes operating activity, who reviews evidence, and who accepts residual risk.

Role	Decision or work owned
Sponsor or CISO	Approves the business objective, the resources and the reporting audience. Accepts residual business risk within delegated authority and records that acceptance in writing.
Operating owner and engineering authority	Approve process boundaries, safe state and production methods. The dispatcher, control room supervisor, port or terminal authority, airport operations lead or pipeline controller retains operating authority.
Compliance and legal owners	Resolve the applicable instruments, disclosure restrictions and incident reporting duties. Identify the responsible filing official and an alternate who acts in the official's absence.
Technical lead and field technician	Design the permitted method and collect traceable evidence. A technician works to the permitted target list and tool settings, and an active test goes ahead on the written authorization of the people named in the permit.
Project manager	Sequences work, tracks evidence and approvals, protects operating windows, manages changes and closes acceptance records. Owns the open items register.
Evidence custodian and quality reviewer	Control evidence access, integrity, retention and the independent review of facts and conclusions. Record conflicts of interest and review exceptions.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03)

© 2026 Global Digital Forensics, Inc. All rights reserved.

Project stages and acceptance

Plan by completed decisions and evidence rather than by a fixed number of days. Populate durations and staffing once site access, document availability and maintenance windows are known, and treat each stage's exit evidence as the gate for the next one.

Stage	Required exit evidence
1 Applicability and scope	Signed facility register, controlling instruments, exclusions and reporting scope. Every open legal question has an owner and a stated effect on the engagement.
2 Readiness	Approved evidence request, interview schedule, collection method, secure workspace, current backup evidence and operating contacts with alternates.
3 Examination	Asset and process records, reconciled diagrams, sampled control evidence and a dated account of what was examined and what was held outside the examination.
4 Authorized validation	Activity permits, baseline observations, test log, stop and recovery record and post work operating acceptance. The record states whether validation was authorized and the reason for that decision.
5 Reporting and decisions	Reviewed findings, requirement mappings, stated boundaries, corrective owners, funding decisions and a residual risk record signed by the person entitled to accept it.
6 Verification and handover	Retest evidence, recurring review schedule, retained records, lessons and a signed handover. A recommendation closes when it is verified or formally dispositioned.

Sources: NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03)

Applicability and obligation records

Use one row per obligation. A single facility can carry several reporting clocks, several evidence packages and several responsible officials for the same event, and one row per obligation keeps every deadline in view.

Make a defensible decision

For each candidate instrument record the issuing authority, the legal citation, the adopted version, the effective date, the compliance date, the regulated entity, the covered system, the trigger and the exceptions. Link the controlled copy of the source and the evidence that establishes the facility facts the decision turns on. Mark the site decision Applicable, Not applicable with reason, or Unresolved.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Separate obligation types

Federal requirements, state utility orders, public agency standards, local permits and contracts overlap on the same equipment. Use the fifty state companion to select additional checks, and confirm municipal, county, tribal or territorial authority where it is relevant. Municipal ownership can change utility jurisdiction and public entity duties, and a federal obligation that independently applies stays on the register alongside them.

Preserve the reasoning

The compliance owner signs the decision date and the next review trigger. Save the instrument and its source URL in controlled records and name the person who will watch for amendments. For an incident clock record the trigger event, the start timestamp with its time zone, the deadline rule, the recipient, the permitted channel, the responsible official and the receipt. The auditor's first question about any applicability decision is why it was made and by whom, and this record is where that answer lives.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), CIRCIA public rulemaking notice (F05), Cybersecurity Resource Center (F09)

Transportation mode and operator boundaries

Separate each mode, each operator and each approved security or safety program first, then apply the assessment checklist. The table names the authority question that has to be answered for each mode and the record that answers it.

Mode	Authority and decision needed
Freight and passenger rail	Determine the carrier and whether a current TSA directive or security program applies. Obtain the issued instrument, the applicability notice, the approved implementation plan and the assessment program from the designated security official.
Urban transit	Determine FTA assistance, rail transit status, State Safety Oversight and applicable TSA coverage. FTA identifies a cybersecurity planning certification under 49 U.S.C. 5323(v) for covered rail transit operators; obtain the actual certification and award conditions.
Roads tunnels and traffic management	Identify state or local ownership, public agency cyber policies, contracts, tunnel safety programs and operator procedures. The cyber assessment cycle for traffic controllers is set by the agency's own program and funding conditions, so the record takes it from those documents.
Maritime facilities vessels and OCS	Determine whether the owner or operator is required to have a security plan under 33 CFR Parts 104, 105 or 106. Apply the relevant Part 101 Subpart F provisions and the current approval or waiver conditions.
Airports and aircraft operators	Obtain the current TSA approved security program with its amendments and the relevant FAA and airport operating constraints. The issued program supplies the clause level basis for the cybersecurity assessment, and public summaries serve for orientation.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Mode	Authority and decision needed
Hazardous liquid natural gas and LNG	Determine current TSA notification or directive coverage, PHMSA SCADA control room rules and state pipeline authority. Record the overlapping operator and system boundaries.

Sources: Cybersecurity in the Marine Transportation System (T01), Pipeline Cybersecurity Mitigation Actions Contingency Planning and Testing (T03), Rail Cybersecurity Mitigation Actions and Testing (T04), Pipeline control room management (T05), Cybersecurity Resources for Transit Agencies (T06), FY2026 Certifications and Assurances (T07), Public Transportation Agency Safety Plans (T08), TSA cybersecurity resource route and operator issued aviation security programs (T09)

Maritime obligations and milestones

33 CFR Part 101 Subpart F applies to the owners and operators required to have security plans under 33 CFR Parts 104, 105 and 106.

Compliance timing

The final rule became effective July 16 2025. Coast Guard implementation information identifies January 12 2026 for the initial general training milestone and its annual recurrence. July 16 2027 is the principal milestone for designation of the Cybersecurity Officer, completion of the Cybersecurity Assessment and submission of the Cybersecurity Plan for approval. Sign the calendar after checking later amendments, waivers and operator specific conditions.

Assessment and plan evidence

Establish the vessel or facility scope, the IT and OT inventory, the critical functions, the vulnerabilities, the existing safeguards and the remedial measures, and keep each as a dated record the CySO controls. The annual assessment and the plan maintenance program link to a designated CySO and to controlled records. The required operational scope reaches the crane, mooring and terminal operating systems, so the assessment gathers that evidence directly rather than relying on a generic IT questionnaire.

Testing and exercises

The final rule provides for penetration testing in conjunction with Cybersecurity Plan renewal under 101.650(e)(2), at least two drills each calendar year, and an exercise each calendar year with no more than 18 months between exercises. Schedule each one from the precise applicable clauses, the compliance schedule and the approved alternatives. A penetration testing obligation is met with a safe method: agree on the targets, the method, the operator safeguards and any regulatory treatment of constraints at the outset, and keep the drill, exercise, assessment, audit and penetration test records as five distinct files.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Handling

Determine SSI handling and the approval channels for the actual records. Keep security plans and detailed vulnerabilities within authorized systems and recipients. The Coast Guard approval or receipt is a separate event from the assessor's report delivery, and the calendar records both.

Sources: Cybersecurity in the Marine Transportation System (T01), Maritime cybersecurity implementation timeline (T02)

Maritime recurring work register

The CySO assigns owners and retains evidence for each separate obligation. Populate the actual completion dates and apply the relevant compliance schedule, approval conditions and exceptions; the dates and receipts behind each row are what make the register defensible.

Workstream	Calendar and acceptance record
Assessment and plan audit	After the initial assessment, assess annually and sooner on ownership changes under 101.650(e)(1). The CySO also ensures annual and triggered plan audits under 101.630(f), with qualified independent auditors and required amendment follow up. Retain scope, results and corrective decisions.
Personnel training	General and key personnel training recur annually, with the initial milestone January 12 2026. New personnel train within five days of system access and no later than 30 days after hiring. Record the relevant OT topics and any authorized monitored access arrangement.
Drills and exercises	Track at least two drills each calendar year and one exercise each calendar year, with at most 18 months between exercises. Keep participants, scenario, findings and correction records.
Penetration testing	Link the required test to Cybersecurity Plan renewal under 101.650(e)(2). Retain approved targets, safe method, constraints, results and correction evidence.
Records and amendments	Section 101.640 routes records to 104.235, 105.225 or 106.230. Verify the applicable retention and secure access. Preserve required approvals and plan amendments separately from the assessment report.

Sources: Cybersecurity in the Marine Transportation System (T01), Maritime cybersecurity current codified provisions (T10)

© 2026 Global Digital Forensics, Inc. All rights reserved.

Rail and transit assessment planning

Separate the current issued TSA obligations, the grant related duties and the operational safety programs. Each produces its own evidence, and each auditor reads the record written for that program.

Obtain current instruments

TSA Security Directive 1580/82-2022-01E, effective May 3, 2026 through May 2, 2027, replaced 1580/82-2022-01D, and the reporting directives 1580-21-01E for freight rail and 1582-21-01E for passenger rail and transit were issued January 15, 2026. Obtain the operator's current directive and applicability notice through the designated security official and protect SSI where it applies. The rail applicability row carries the Unresolved status while that instrument is obtained, and it closes against the issued text.

Build the evidence boundary

Map the operator's approved cybersecurity implementation and assessment arrangements to the actual systems. Include dispatch, traction power, wayside interfaces, tunnel ventilation, access systems and the supporting communications when they are within scope, and identify third party and shared facility responsibilities for each. The boundary record names the operator who owns every interface on the drawing.

FTA and state safety oversight

FTA identifies cybersecurity planning certification as a condition of assistance for covered rail transit operators under 49 U.S.C. 5323(v). Obtain the FY2026 certifications and the actual award conditions. Separately identify the 49 CFR Part 673 safety plan and State Safety Oversight responsibilities. A safety plan certification and the test of a cyber control are filed as separate evidence, each read for what it records.

Field method

Use the approved drawings, configuration records, access samples and event records first. Movement authority, signaling, traction power and emergency ventilation tests require the proper operating and engineering authorities. The permit names the system, the window and the person who can stop it.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), Rail Cybersecurity Mitigation Actions and Testing (T04), Cybersecurity Resources for Transit Agencies (T06), FY2026 Certifications and Assurances (T07), Public Transportation Agency Safety Plans (T08)

Pipeline and energy transport planning

TSA cybersecurity instruments and PHMSA control room safety rules can apply to the same operator for different purposes, and the assessment keeps two registers rather than merging them into one.

© 2026 Global Digital Forensics, Inc. All rights reserved.

TSA applicability

Obtain the current directive, the notice and the approved operator plans. Security Directive Pipeline-2021-02G, effective May 3, 2026 through May 2, 2027, replaced Pipeline-2021-02F, and Pipeline-2021-01G, issued January 15, 2026, carries the reporting requirements. Confirm with the operator which directive versions and approved alternatives apply, and test against those.

PHMSA control room boundary

Identify whether controllers in a control room monitor and control pipeline facilities through SCADA within 49 CFR 192.631 or 195.446 scope. Review the applicable control room procedures, alarm management, point to point information validation, change management, training and operating records using the current rule and the operator's program. The alarm management records and the point to point verification files are the artifacts a PHMSA inspector will know by name.

Evidence and field work

Trace control and telemetry, communications, leak detection interfaces, engineering access and vendor dependencies. Review the authoritative configuration and alarm records with the control room supervisor present.

Overlap and reports

Record the federal pipeline safety, TSA, state pipeline, environmental and contractual notification criteria separately, and capture the actual event facts and awareness timestamps for each. A cyber report and a release or safety report are each filed in their own right, and safe plant response takes precedence over evidence collection every time.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), Pipeline Cybersecurity Mitigation Actions Contingency Planning and Testing (T03), Pipeline control room management (T05), Emergency Release Notifications under EPCRA (F07)

Aviation ports and roadway field boundaries

These environments share technologies and have different operating authorities. Divide the work by authority rather than running one approval across the campus or the transport network.

Aviation

Distinguish airport enterprise IT, baggage, fuel and building systems, airfield operational systems, air traffic systems and aircraft. Obtain the operator's current security program and the applicable amendments.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Ports and terminal interfaces

Determine the facility and vessel responsibilities, the tenant connections, the crane controls, the cargo systems, the reefer monitoring, the access systems, the shore services and the third party remote support. Link the boundary to the MTSA plan and the current CySO. Tenant or lease obligations can supplement federal scope while the federal applicability test stays as written, and work on tenant equipment proceeds with the tenant's own approval.

Road traffic and tunnels

Record state or local ownership, DOT or municipal contracts, communications providers, traffic control, tunnel ventilation, emergency power and recovery dependencies. Identify the public agency incident rules and the local operating plans. Take the cyber audit interval for each traffic controller group from the owning agency's rules and plans.

Deliverable Review and Acceptance Criteria

Each responsible operator signs the boundary and the permitted method. Each affected activity proceeds once ownership and operational authority are resolved in writing.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), Cybersecurity in the Marine Transportation System (T01), Public Transportation Agency Safety Plans (T08), TSA cybersecurity resource route and operator issued aviation security programs (T09)

Transportation exercise and handover

Use one scenario per mode and a separate coordination scenario for the shared dependencies. The following scenario is fictional, and it is built around the shared service that transportation operators map least often.

Scenario

Remote vendor access is suspected of compromise at a shared communications service. One operator reports loss of visibility while another still appears normal. Which interfaces share an identity or a management path is the open question.

Operational decisions

Ask each operator to establish its safe response, its service restrictions and its decision authority. Ask the technical lead to identify the shared dependency and the reach of the evidence. Ask the project manager to account for tenants, contractors and cross state assets within the existing test permission.

Reporting decisions

Have the responsible officials evaluate the current TSA instruments, Coast Guard reporting, FTA and State Safety Oversight, PHMSA, state and local public entity duties and contract duties as each applies. Where a controlled directive is still being obtained, record the instrument and the escalation, and take the deadline from

© 2026 Global Digital Forensics, Inc. All rights reserved.

the issued text once it arrives.

Closure

Record the tested communications, the identified delays, the records to locate, the actions, the owners and the review dates. Reconcile any mode specific safety acceptance, security plan amendment or regulator receipt needed for return to service.

Sources: NIST SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management (F04), Cybersecurity in the Marine Transportation System (T01), Pipeline Cybersecurity Mitigation Actions Contingency Planning and Testing (T03), Rail Cybersecurity Mitigation Actions and Testing (T04), Pipeline control room management (T05), Cybersecurity Resources for Transit Agencies (T06), Public Transportation Agency Safety Plans (T08), TSA cybersecurity resource route and operator issued aviation security programs (T09)

Document requests and interviews

Request existing records first, ahead of any proposal for a live connection. Most of what a competent OT assessment needs already exists in engineering, maintenance and identity systems, and asking for it first tells you how well the operator knows its own process before a single packet is observed.

Initial evidence request

Request the asset inventory, the approved network and process drawings, the process description, current configuration exports, the remote access arrangements, the account owner list, maintenance records, the backup inventory and the most recent restoration evidence. Include rail signaling interfaces, traction power SCADA, tunnel systems, traffic controllers, terminal cranes, access systems, airport operational support, pipeline SCADA and remote control sites. Ask for the applicable regulatory assessments, prior findings and the change history for the period in scope. Give each request an identifier, a purpose, an expected owner, a time period, a format and a due date, and allow a supervised on site review for any record that stays at the facility. Record each item still outstanding together with its effect on the conclusion.

Interviews that test the record

Ask operations what happens when visibility, remote control, communications or a critical vendor service is lost, and listen for whether the answer names a procedure or a person. Ask engineering which installed details differ from the drawing; there usually are some, and the honest list is the most useful document the assessment will receive. Ask the identity owner how vendor access is approved and revoked and request the last revocation as evidence. Ask the recovery owner for the record of the last actual restore rather than a description of the backup product.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Sampling

Define the control population and the sampling rationale before selecting items. Include the material differences in site function, equipment family, criticality, remote access and support arrangements so the sample represents the estate rather than the nearest site. A sample drawn across the remote stations speaks for the remote stations, and the report states both the sample and the population outside it in plain terms.

Readiness evidence

Retain the request register, the interview notes with participants and dates, the source versions received, the missing item log and the agreed question list for the field visit. Before the visit the technical lead reads the notes once more to confirm that every interview statement is recorded as a statement and every tested fact as a tested fact.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03)

Safe work and stop authority

The dispatcher, control room supervisor, port or terminal authority, airport operations lead or pipeline controller retains operating authority. That sentence is the operating rule for the entire engagement, and every member of the assessment team can repeat it from memory before the first site day.

Before connecting anything

Attend the operator's safety briefing and follow the site access, electrical, hazardous energy, confined space and other controls that the operator says apply. The operator determines which safety program governs, and electrical switching, confined space entry and plant permits stay with the qualified plant staff who hold those programs. Verify the asset owner, the permitted access point, the device approval, its malware screening, the cable path and the isolation design, and then attach the collection device. A mirror port or passive tap design can affect traffic handling, data exposure and network load, so its installation and its removal are both approved steps.

Define measurable stop conditions

Operations defines the baseline process indicators and limits appropriate to rail and transit movement, road traffic management, port and terminal operations, aviation support and pipeline control. Record the conditions that require stopping in the operator's own terms: unexpected alarms, impaired communications, controller health changes, operator concern or any departure from the approved method. The number that matters is the one the operator watches. Name who can stop work and who can authorize resumption. Any technician may call a safety stop. The operating owner directs the plant response, and isolation, device resets and process restarts all happen at that owner's direction.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Record the stop and recovery

Log the time, the activity, the observed symptoms, the notifications made, the actions directed by operations and the restoration evidence. Preserve the available records alongside the safety response, which always comes first. Hold the activity permit while operations and the technical lead review the cause, then reauthorize the changed method and the remaining targets. A stop that is logged and reviewed is a mark of a controlled assessment, and the log is the record a later reviewer reads to confirm the assessment was run that way.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03), State Plans (F06)

Inventory and process dependencies

Build an inventory that explains how each asset supports rail and transit movement, road traffic management, port and terminal operations, aviation support and pipeline control. An inventory ties each address to its function, and a passive discovery export joins it once it has been reconciled against the drawings.

Use existing evidence first

Reconcile the engineering inventories, configuration exports, approved drawings, maintenance records and supervised physical observation into one record. For each asset capture the identifier, function, location, owner, manufacturer, model, firmware or software version, support status, protocols, zone and recovery dependency. Mark each value as observed, taken from a configuration export, or supplied by a vendor or operator, because the three carry different weight and a reviewer will ask which one applies.

Trace the consequence

For each critical process trace the route from the operator interface and the control logic through communications to field equipment and the supporting services. Identify how an asset failure could contribute to unsafe movement, loss of dispatch or signaling visibility, terminal interruption, loss of emergency ventilation, flight support disruption or pipeline release. Ask engineering to validate the consequence and the available protection or manual alternative, then write down what they said and who said it. Record protective functions separately from normal process control and document the dependencies on identity, time sources, licensing, cloud support, third party communications and engineering tools. A safety function is recorded as independent when engineering has shown how it is isolated, whatever layer of the drawing it sits in.

Resolve discrepancies

Mark unidentified devices, duplicated identifiers, outdated drawings and vendor assets awaiting verification, and give each discrepancy to its owner to resolve. A system past vendor support gets its own control and recovery decision, and patching, scanning or replacing it during the assessment is an operating decision that operations approves. Expect the first reconciliation to surface undocumented engineering laptops, dual homed workstations and vendor modems; those are findings, and the inventory is where they belong.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Deliverable Review and Acceptance Criteria

The asset owner signs the scoped inventory and the dependency map. The report states the sources used, the collection date, the coverage achieved and every high consequence dependency still open. Sensitive addressing and configuration detail belong in the controlled technical appendix, and the management report carries the summary.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), A survey of cyber security management in industrial control systems (R01), Threat modeling of industrial control systems: A systematic literature review (R02)

Network paths and remote access

Review every path by which a person, a service or an external system can reach the scoped process. A firewall diagram is a hypothesis that the examiner tests against the rule base, the routing and the actual sessions, and that test is where a segmentation claim is confirmed or corrected.

Examine the intended boundary

Use dated configuration exports, rule bases, drawings and approved architecture records to identify the zones, conduits, remote entry points, jump services and management interfaces. For each material path record the source, the destination, the permitted service, the business purpose, the approver and the review date. Separate corporate identity, vendor support, telemetry, cloud management and emergency access into their own path records. Check whether access can be limited to named users and required assets, and whether it is reviewed, recorded and revoked. Examine an actual approval and an actual revocation from the period rather than the policy that describes them.

Examine the actual access process

Observe a supervised, approved support session or review the retained session records. Record how the user authenticated, how authorization was granted, who owns the account, whether the session was visible to operations, what constraints apply to shared accounts and how timeout and revocation behave. Where an installed controller supports a narrower mechanism, evaluate the controls at an approved access gateway and say so in the finding. The examiner looks closely at three common points: a vendor tunnel that bypasses the jump host, a rule base with permit any entries left from commissioning, and a dual homed engineering workstation that joins two zones the drawing shows as separate.

Match each claim to its method

A configuration review identifies an allowed policy path, and a controlled connectivity check, a separate authorized activity with its own permit, tests whether the path is reachable. A proposed segmentation improvement moves from recommendation to verified as it is implemented and tested, and the report uses those three words, allowed, reachable and verified, with their distinct meanings.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Required records

Retain the approved path register, the source versions examined, the access samples, the exceptions and the method used. If ISA/IEC 62443 is contractual, a conformity statement is made against the licensed edition and the agreed assessment criteria. The publicly described zone and conduit approach is a design method, and the assessment uses it to read the architecture.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), ISA/IEC 62443 Series of Standards (F08)

Accounts, legacy systems and suppliers

Start with the access needed to operate and recover the process, then identify the controls the installed system can actually support and the protections applied around it. Legacy equipment is assessed on the compensating controls around it, measured against what the installed system can support.

Accounts and authorization

Review named users, service accounts, vendor accounts and emergency credentials through approved exports of the identity directory, the local account stores on controllers and HMIs, and the vendor access platform. Verify owners, privileges, approval, periodic review and the revocation evidence for people who have left. Review how privileged access is separated from normal user activity. Record account names and roles. For every shared or embedded account document the technical constraint, the compensating controls, who knows the credential, how its use is supervised and logged, how access is removed when people leave and what change would reduce reliance on it. A shared operator account still on its commissioning password is common, and a well run site has the compensating controls around it written down and working.

Support and vulnerability decisions

Match versions and support status to vendor advisories using approved evidence. Separate a version match, a suspected vulnerability and a validated condition, and keep them separate in the finding register. When a controller answers a scan slowly, the team pauses and reviews the scan plan. For a legacy device compare patch availability, vendor support, maintenance dependencies, network exposure, replacement lead time and restoration options. The assessment recommends a decision. Operations and engineering approve changes under their own change process.

Supplier obligations

Review the supplier contracts for remote access, notification, vulnerability handling, evidence availability, subcontracting, licensing and exit support, and compare the paper to the observed practice. Identify contract promises that practice has yet to match and dependencies awaiting a named owner. Include a supplier contact and an escalation alternate in the operating handover so the operator reaches support during an incident in one call.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), ISA/IEC 62443 Series of Standards (F08)

Monitoring, time and evidence handling

Establish whether the available records can answer who accessed what, when, through which path and with what effect. Record time offsets as found, leave production clocks as they run, and translate timestamps in the analysis.

Collect a usable record

Identify the event sources, the collection routes, the retention settings, the access restrictions and the review responsibility for each. Include the jump host, authentication, firewall, engineering workstation and system records relevant to the scoped process. Verify that a small authorized event sample actually appears at the intended collection point, because the collection point itself is where the examiner confirms what was received last month. Record the time zone, the clock source, the observed offset and the coverage periods for each source. If clocks disagree, preserve the original timestamps and document the translation used in analysis. An absent event is checked against collection coverage before it is read as inactivity, and the report records which reading the evidence supports.

Evidence integrity

Assign each item a stable evidence identifier and record its origin, custodian, collection date and method, source period, filename or record reference, integrity value where appropriate, storage location and access history. Keep originals protected and conduct analysis on controlled working copies. Log every transformation and redaction. This is the discipline that lets a finding survive challenge from a vendor, a regulator or the other side in a dispute, and it costs minutes at collection time against hours of argument later.

Sensitive information

Have the compliance owner classify customer information, engineering records and any SSI, CEII, CUI or protected public records before collection begins, and apply the handling rules that actually attach to each class.

Deliverable Review and Acceptance Criteria

The custodian verifies access, recoverability and retention against the applicable instrument or the agreed contract. Preserve incident records and any legal hold independently of the normal assessment deletion date.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03), NIST SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management (F04)

© 2026 Global Digital Forensics, Inc. All rights reserved.

Recovery and continuity evidence

Check whether the operator can restore the process after loss of rail signaling interfaces, traction power SCADA, tunnel systems, traffic controllers, terminal cranes, access systems, airport operational support, pipeline SCADA and remote control sites. A successful backup job records that a file was written, and a representative restore is where recovery is demonstrated.

Define the restoration objective

Ask operations to identify the minimum service, the safe process condition, the restoration sequence and the maximum tolerable interruption. Record the chosen recovery objectives, their owner and the evidence that supports their feasibility.

Examine recovery dependencies

Identify the controller and server configurations, engineering projects, firmware, software, licenses, keys held in controlled storage, approved hardware, spare components and vendor support that a restoration needs. Confirm where a clean engineering station and trusted installation media are kept for an incident, and whether the engineering software has a copy apart from the workstation an attacker would target. Review backup isolation, access, integrity checks and the evidence of a representative restore. A production controller upload, download or failover is a separately approved activity, and an isolated or representative system carries the work wherever operations judge production unsuitable.

Exercise and validate

Use a scenario that removes a material dependency. Record which recovery steps were discussed, which were demonstrated in a representative environment and which were performed in production under approval. Document the differences between the test environment and the installed system. A tabletop exercise demonstrates a decision process, a technical restore is demonstrated on its own, and the report keeps the two distinct.

Closure evidence

Retain the recovery procedure version, the scenario, the approvals, the result, the elapsed time where it was actually measured, the open dependencies and the corrective owner. Operations accepts the restored state. Assumptions awaiting a test stay explicit in the report and are scheduled in the recurring program.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management (F04), ICSSIM: A framework for building industrial control systems security testbeds (R03)

© 2026 Global Digital Forensics, Inc. All rights reserved.

Authorization for active validation

Active validation enters the work when a controlling requirement or the agreed scope calls for it and an acceptable method has been authorized. A contractual requirement to test is met with a safe operating method, written down by the assessor before the work runs.

Write an activity permit

Identify the exact targets, the system owner, the purpose, the tool and its version, the commands or test functions, the allowed traffic behavior, the exclusions, the operating window and the collection location. Include vendor restrictions, communications arrangements, recovery support and the evidence to retain. Approve the method for the installed firmware and configuration rather than for a similar laboratory device, because controllers of the same model and different firmware behave differently under the same probe.

Choose the least disruptive evidence

Consider configuration examination, supervised control demonstration, existing logs and validation in a representative environment before any production probe. Record which requirement each method addresses and what it shows. Peer reviewed testbed research helps explain test design.

Confirm readiness at the point of work

Operations confirms the process condition and the baseline indicators. The technical lead confirms the approved tool settings and targets. The evidence custodian confirms that recording is running. The project manager verifies that the authorization is current and that the named stop authority is reachable by a channel that has been tested that day. Each of those is a separate activity with its own method, environment and approval.

Close the permit

Record the start and end times, the targets actually reached, deviations, stops, observations and the operating owner's acceptance. Revoke temporary access and remove approved collection equipment under the agreed procedure. Keep the original permit and the test record linked to every finding that relied on them.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03), ICSSIM: A framework for building industrial control systems security testbeds (R03)

© 2026 Global Digital Forensics, Inc. All rights reserved.

Writing findings that can be audited

A finding shows the condition, its evidence, the criterion it was measured against and its significance for the process. Observed facts and possible operating consequences are kept in separate sentences, because a reviewer gives each its proper weight when the two are kept apart.

Minimum finding record

Record the finding identifier, the asset or control boundary, the evidence identifiers with dates, the requirement or agreed criterion, the observed condition, the method and what it covers. Explain the credible operating consequence and the assumptions behind it. Record the existing safeguards, the recommended action, the responsible owner and the proposed verification method.

Use precise status

Use Observed when the available evidence establishes a condition, and Suspected or Unresolved when the evidence points to a condition the examination has yet to confirm. Record recommendation, implementation and verification as three separate states. A screenshot of a changed configuration supports implementation.

Prioritize consequence and confidence

Evaluate the potential effects on rail and transit movement, road traffic management, port and terminal operations, aviation support and pipeline control, the exposure paths, the existing safeguards, the recovery capacity and the confidence in the evidence. Include unsafe movement, loss of dispatch or signaling visibility, terminal interruption, loss of emergency ventilation, flight support disruption or pipeline release where the process supports that consequence, and have engineering review the pathway before it is presented as fact. A CVSS score describes a software vulnerability, and plant risk comes from the organization's own risk method: record that method and its acceptance authority, and keep the plant score grounded in it rather than in multiplied numbers.

Resolve challenge

Give the operating owner a documented opportunity to identify asset facts to correct, safeguards to add and remediation proposals to revise for safety. Retain the challenge, the additional evidence, the reviewer's decision and the revised wording. A disagreement closes when the record shows how it was resolved, whatever the report delivery date.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), A survey of cyber security management in industrial control systems (R01), Threat modeling of industrial control systems: A systematic literature review (R02)

© 2026 Global Digital Forensics, Inc. All rights reserved.

Corrective work and management reporting

The assessment ends with decisions an owner can implement and a reviewer can verify. A corrective plan puts the vulnerabilities into an operating sequence, which is what turns a scan export into work an owner can schedule.

Plan the work

For each accepted finding identify the owner, the dependency, the required design or procurement, the change approval, the maintenance window, the recovery support, the target date and the verification evidence. Identify an interim control where the final fix takes longer, and carry the Deferred label on a postponed action through to implementation. Sequence actions by operating consequence and dependency: an access boundary may need a maintained jump host, named accounts and supplier support in place before a legacy controller can be isolated, and applying fixes in that order keeps the operator supported through the next outage. Verify that each proposed change preserves emergency operation and recovery.

Report to leadership

Provide a concise operating risk summary, the most consequential open issues, the funding or outage decisions required, the affected services and the boundaries of the assessment. Show the remaining work and who may accept the residual risk. Confidential addressing and detailed weaknesses stay in the restricted appendix.

Report to technical owners

Provide enough evidence and context to reproduce each observation using the approved method. Identify configuration versions, the affected boundary, exceptions and the exact acceptance criteria for closure.

Regulatory conclusion

State the obligations actually assessed, with their versions, the facility scope, the sample and the dates, and list in their own section the requirements outside this assessment and those awaiting demonstration.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03)

Verification closure and recurring work

Close an action against the evidence defined when the finding was written. A management assertion, a purchase order or a completed ticket is the cue to schedule verification, and the verified control result comes from that check.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Verification procedure

The reviewer checks that the implementation evidence matches the approved change. Agree a safe validation method, compare the result with the acceptance criterion and retain the evidence. Record exceptions and state whether the result establishes design, implementation or operating effectiveness, because those are three different claims.

Evidence Handover and Chain of Custody Transfer

Return the current inventory, dependency map, control and finding register, activity permits, evidence index, operating procedures, supplier contacts and training record to the designated owners. Check that authorized staff can retrieve those records during an outage, when the corporate document system may be the thing that is down. Remove temporary access under the agreed change record and confirm the removal.

Recurring triggers

Schedule reviews from the actual instruments and the operational change cycle rather than from a calendar copied from another site. Trigger a new applicability review after an ownership or service change, a new state footprint, a contract change, a revised standard, a significant architecture change or a material incident. Confirm whether a statutory update or certification is required, then set the due date.

Final acceptance

The operating owner accepts the process condition and the handover. The technical reviewer signs the evidence based conclusions. The compliance owner approves the requirement mapping and the remaining legal questions. The sponsor records the funding and residual risk decisions. The project manager closes each deliverable as it meets those acceptance criteria, and the closure record names each person and date.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03), NIST SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management (F04)

Facility and applicability worksheet

Complete one worksheet for each legal entity, facility and distinct regulatory boundary, and keep the source records in controlled storage. The worksheet is the index an auditor reads first, so every field points to a record that exists.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Evidentiary Record Fields

Facility legal entity address and operating function

Ownership operator classification permits registration and contracts

Applicable instruments exact versions and source record IDs

Applicability decisions exceptions and unresolved questions

Operating technical compliance and project owners with alternates

Decision approvers dates next review and authority record

Field activity authorization worksheet

The operating owner approves the activity before work begins. This worksheet records that permission.

Evidentiary Record Fields

Activity purpose exact targets and asset owners

Method tool version permitted functions and excluded actions

Vendor constraints approved traffic behavior and operating baseline

Operating window communications and named stop authority

Recovery support safe response and resumption authority

Operating approval technical approval date and change record

Evidence and finding worksheet

Record facts separately from possible consequences. Link the original evidence, preserve the source times and state the scope of each method, so a reviewer working from the record alone can reproduce the finding.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Evidentiary Record Fields

Evidence ID source custodian period collection method and integrity

Observed condition and method used to establish it

Applicable requirement exact version and agreed assessment criterion

Operating consequence safeguards assumptions and evidence limits

Finding ID responsible owner priority rationale and challenge

Reviewer disposition date and linked technical record

Corrective action and acceptance worksheet

Keep recommended, implemented and verified as three separate states with their own dates and evidence. Record the remaining risk and name the person authorized to accept it.

Evidentiary Record Fields

Finding ID action owner dependencies and target date

Approved implementation change record and operating window

Verification criterion authorized method result and evidence IDs

Remaining limitations interim controls and residual risk decision

Operating acceptance compliance disposition and recurring review

Technical reviewer sponsor decision date and closure record

Terms used in the planning records

Term	Meaning in this pack
OT ICS and SCADA	Operational technology; industrial control systems; supervisory control and data acquisition.
PLC RTU HMI DCS SIS	Programmable logic controller; remote terminal unit; human machine interface; distributed control system; safety instrumented system.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Term	Meaning in this pack
RRA ERP and PWSID	Risk and resilience assessment; emergency response plan; public water system identifier.
BES CIP DER and EMS DMS	Bulk Electric System; Critical Infrastructure Protection; distributed energy resources; energy/distribution management system.
SSI CEII and CUI	Sensitive Security Information; Critical Energy/Electric Infrastructure Information under the applicable authority; Controlled Unclassified Information. Determine the actual handling regime.
CySO CISO and EHS	Cybersecurity Officer; Chief Information Security Officer; environment health and safety.
PHA MOC and CMMC	Process hazard analysis; management of change; Cybersecurity Maturity Model Certification.
Applicable and Unresolved	Applicable requires facility facts and a controlling instrument. Unresolved identifies a fact or authority still being gathered, and it keeps the row open on the register, distinct from Not applicable.

Sources F01 to R03, federal guidance and peer reviewed research

F01 Guide to Operational Technology Security Revision 3

NIST. Final guidance. September 2023 final publication; chapters 4 through 6 and OT control tailoring.

F02 Guide to Operational Technology Security Revision 4

NIST. Draft guidance. September 21 2026 initial public draft. Revision 4 was released as an initial public draft on September 21, 2026, so Revision 3 remains the final baseline.

R01 A survey of cyber security management in industrial control systems

Knowles and colleagues in International Journal of Critical Infrastructure Protection. Peer reviewed research. Volume 9 June 2015 pages 52 to 80. Used for qualitative management context, with current law and effectiveness figures taken from the primary sources.

R02 Threat modeling of industrial control systems A systematic literature review

Computers and Security. Peer reviewed research. Volume 136 January 2024 article 103543. Supports structured threat modeling, which the assessment applies to the specific plant.

R03 ICSSIM A framework for building industrial control systems security testbeds

Computers in Industry. Peer reviewed research. Volume 148 June 2023 article 103906.

Sources: NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (F01), NIST SP 800-82 Rev. 4 initial public draft, Guide to Operational Technology (OT) Security (F02), A survey of cyber security management in industrial control systems (R01), Threat modeling of industrial control systems: A systematic

© 2026 Global Digital Forensics, Inc. All rights reserved.

literature review (R02), ICSSIM: A framework for building industrial control systems security testbeds (R03)

Sources F03 to T03, federal guidance and transportation instruments

F03 Technical Guide to Information Security Testing and Assessment

NIST. Final guidance. Assessment planning and rules of engagement. Apply OT operating constraints.

F05 CIRCIA public rulemaking notice

CISA and Federal Register. Rulemaking record. 2026 notice referring to the proposed rule and further town halls. The CIRCIA final rule has been under review at the Office of Management and Budget since October 1, 2026; its reporting clocks begin on the effective date the Federal Register publishes, so check the Register when setting the calendar.

F09 Cybersecurity Resource Center

New York DFS. Agency implementation source. 23 NYCRR Part 500 covered entity scope. Covered entity status is decided under the Part 500 definition, which the register checks for each New York operator apart from its location.

T01 Cybersecurity in the Marine Transportation System

US Coast Guard and Federal Register. Final rule. 90 FR 6298; 33 CFR 101 Subpart F; 101.605 and 101.630 through 101.665. Check subsequent amendments and operator specific approval, waivers and equivalents.

T03 Pipeline Cybersecurity Mitigation Actions Contingency Planning and Testing

TSA. Security directive. Security Directive Pipeline-2021-02G, effective May 3, 2026 through May 2, 2027, supersedes Pipeline-2021-02F, and Pipeline-2021-01G, issued January 15, 2026, carries the reporting requirements. Obtain the applicability notice and approved plan from the operator.

Sources: NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (F03), CIRCIA public rulemaking notice (F05), Cybersecurity Resource Center (F09), Cybersecurity in the Marine Transportation System (T01), Pipeline Cybersecurity Mitigation Actions Contingency Planning and Testing (T03)

© 2026 Global Digital Forensics, Inc. All rights reserved.

Sources T04 to T08, transportation instruments

T04 Rail Cybersecurity Mitigation Actions and Testing

TSA. Security directive. Security Directive 1580/82-2022-01E, effective May 3, 2026 through May 2, 2027, supersedes 1580/82-2022-01D, and the reporting directives 1580-21-01E and 1582-21-01E were issued January 15, 2026. Obtain the applicability notice and approved plan from the operator.

T05 Pipeline control room management

PHMSA. Agency implementation guidance. 49 CFR 192.631 and 195.446; controller and SCADA scope. These are safety requirements alongside any applicable TSA cybersecurity instrument.

T06 Cybersecurity Resources for Transit Agencies

FTA. Agency implementation guidance. 49 U.S.C. 5323(v) and security directives; distinction between covered operators.

T07 FY2026 Certifications and Assurances

FTA. Agency funding instrument. Current grant certifications and assurances.

T08 Public Transportation Agency Safety Plans

FTA. Agency implementation guidance. 49 CFR Part 673; applicability and safety management. Cyber audit frequency for each transit mode is read from that mode's own applicable program.

Sources: Rail Cybersecurity Mitigation Actions and Testing (T04), Pipeline control room management (T05), Cybersecurity Resources for Transit Agencies (T06), FY2026 Certifications and Assurances (T07), Public Transportation Agency Safety Plans (T08)

Sources T09 to F04, federal guidance and transportation instruments

T09 TSA cybersecurity resource route and operator issued aviation security programs

TSA. Agency routing source. Aviation security programs are issued to each operator, so obtain the current operator issued aviation security program and amendments through authorized channels.

T02 Maritime cybersecurity implementation timeline

US Coast Guard. Agency implementation notice. January 12 2026 training and July 16 2027 principal compliance milestone. Read it with the codified rule in T10.

© 2026 Global Digital Forensics, Inc. All rights reserved.

T10 Maritime cybersecurity current codified provisions

Office of the Federal Register eCFR. Current codified rule. 33 CFR 101.630(f); 101.635; 101.640; 101.650(d)-(e); implementation under 101.655. Current display reviewed October 16, 2026. Read the applicable compliance dates in 101.655 and any approved equivalent or waiver. The eCFR is authoritative but unofficial.

F07 Emergency Release Notifications under EPCRA

EPA. Agency guidance. EPCRA 304 and CERCLA release notification. Chemical thresholds, release facts and recipients are set by a separate EHS determination.

F04 Incident Response Recommendations and Considerations Revision 3

NIST. Final guidance. April 2025 final publication.

Sources: TSA cybersecurity resource route and operator issued aviation security programs (T09), Maritime cybersecurity implementation timeline (T02), Maritime cybersecurity current codified provisions (T10), Emergency Release Notifications under EPCRA (F07), NIST SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management (F04)

Sources F06 to F08, federal guidance

F06 State Plans

OSHA. Jurisdiction directory. State and federal occupational safety jurisdiction. Check public employee coverage and industry exceptions for the actual workplace.

F08 ISA/IEC 62443 Series of Standards

ISA. Standards publisher overview. Published series and applicable parts. The normative texts are licensed from ISA and IEC, and a conformity or security level claim is made against the licensed edition the organization holds.

Sources: State Plans (F06), ISA/IEC 62443 Series of Standards (F08)

© 2026 Global Digital Forensics, Inc. All rights reserved.

READY TO PLAN THE ASSESSMENT?

Scope the Assessment With Examiners Who Keep Each Mode Separate

The manual separates the modes, the authorities and the evidence each regulator will ask for. Global Digital Forensics supplies the examiners who carry that structure into the field: court tested forensic specialists who have worked for businesses since 1992, who start with existing records and passive evidence, authorize every active step with the responsible operator by name and write findings a security officer, a dispatcher or a regulator can follow. Tell us about the modes, the operators and the instruments in play, and we will scope the work with your operating and safety leads. The first consultation is free.

Web Addresses for the Sources Cited

1. NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security: https://csrc.nist.gov/pubs/sp/800/82/r3/final
2. NIST SP 800-82 Rev. 4 initial public draft, Guide to Operational Technology (OT) Security: https://csrc.nist.gov/pubs/sp/800/82/r4/ipd
3. A survey of cyber security management in industrial control systems: https://doi.org/10.1016/j.ijcip.2015.02.002
4. Threat modeling of industrial control systems: A systematic literature review: https://doi.org/10.1016/j.cose.2023.103543
5. ICSSIM: A framework for building industrial control systems security testbeds: https://doi.org/10.1016/j.compind.2023.103906
6. NIST SP 800-115, Technical Guide to Information Security Testing and Assessment: https://csrc.nist.gov/pubs/sp/800/115/final
7. CIRCIA public rulemaking notice: https://public-inspection.federalregister.gov/2026-10417.pdf
8. Cybersecurity Resource Center: https://www.dfs.ny.gov/industry_guidance/cybersecurity
9. Cybersecurity in the Marine Transportation System: https://www.federalregister.gov/documents/2025/01/17/2025-00708/cybersecurity-in-the-marine-transportation-system
10. Pipeline Cybersecurity Mitigation Actions Contingency Planning and Testing: https://www.tsa.gov/sites/default/files/signed_security_directive_pipeline-2021-02g_and_transmittal_memo_508c.pdf
11. Rail Cybersecurity Mitigation Actions and Testing: https://www.tsa.gov/sites/default/files/signed_security_directive_1580_82-2022-01e_and_transmittal_memo_508c.pdf
12. Pipeline control room management: https://www.phmsa.dot.gov/pipeline/control-room-management/control-room-management
13. Cybersecurity Resources for Transit Agencies: https://www.transit.dot.gov/regulations-and-programs/safety/cybersecurity-resources-transit-agencies
14. FY2026 Certifications and Assurances: https://www.transit.dot.gov/funding/grants/grantee-resources/certifications-and-assurances/fy2026-annual-list-certifications
15. Public Transportation Agency Safety Plans: https://www.transit.dot.gov/PTASP
16. TSA cybersecurity resource route and operator issued aviation security programs: https://www.tsa.gov/
17. Maritime cybersecurity implementation timeline: https://www.news.uscg.mil/maritime-commons/Article/4247529/final-rule-cybersecurity-in-the-marine-transportation-system-implementation-tim/
18. Maritime cybersecurity current codified provisions: https://www.ecfr.gov/current/title-33/chapter-I/subchapter-H/part-101/subpart-F
19. Emergency Release Notifications under EPCRA: https://www.epa.gov/epcra/epcra-emergency-release-notifications
20. NIST SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: https://csrc.nist.gov/pubs/sp/800/61/r3/final
21. State Plans: https://www.osha.gov/stateplans/

© 2026 Global Digital Forensics, Inc. All rights reserved.

22. ISA/IEC 62443 Series of Standards: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed November 3, 2026.

Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

Call (800) 868-8189, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

© 2026 Global Digital Forensics, Inc. All rights reserved.