

// SECURIDIGM • BRIEFING

KNOW WHERE YOU STAND. SHOW IT.

Every requirement, deadline and document for the Coast Guard's cyber rule and TSA's cybersecurity directives. One file. Nothing leaves your computer.

For Cybersecurity Officers, Facility and Vessel Security Officers, Cybersecurity Coordinators, compliance leads, partners and investors • October 2026

HARBOR • 33 CFR 101 SUBPART F

SIGNAL • TSA CYBER DIRECTIVES

securidigm.com

// THE SHORT VERSION

THIS BRIEFING IN 60 SECONDS.

THE BURDEN

Each regime adds a yearly cycle of plans, assessments, training, drills, reports and records — all of it Sensitive Security Information.

THE CONFUSION

Coast Guard plans are due July 16, 2027, yet operators are asked not to submit full plans yet. Eight guidance releases in eleven months. Five reporting clocks.

THE MOVING TARGET

TSA renews its five cyber directives a year at a time and revises them as it goes. A permanent rule, proposed in 2024, is still not final.

THE FIX

Harbor (Coast Guard) and Signal (TSA) map every paragraph, run every deadline and draft every document from your answers, traced to the rule.

LOCAL BY DESIGN

One HTML file. No install, no account, no outside connections. AES-256 encrypted in your own folder. Your IT team can verify all of it.

// THE LANDSCAPE

THREE AGENCIES. ONE SECURITY OFFICER.

U.S. COAST GUARD

33 CFR 101, SUBPART F

Final rule. In force since July 16, 2025. Plan and assessment due July 16, 2027.

TSA

SECURITY DIRECTIVES

Five cyber directives for pipeline and rail, renewed a year at a time. A permanent rule was proposed in November 2024. Still not final.

CISA

CIRCA

Incident reporting across 16 critical infrastructure sectors. Proposed April 2024. Still not final.

“generally heading toward more fragmentation, not more harmonization.”

Harry Coker, then National Cyber Director, June 2024 · quoted in CRS R49009

// THE COAST GUARD RULE

THE RULE DOESN'T END IN 2027.

IN FORCE

JUL 16, 2025

Reportable cyber incidents go to the NRC without delay, or under 33 CFR 6.16-1.

PASSED

JAN 12, 2026

Cyber training done for everyone with IT or OT access.

NEXT

JUL 16, 2027

Cybersecurity Officer designated. Assessment complete. Cybersecurity Plan submitted.

THEN, FOREVER

EVERY YEAR

Assessment, training.
After approval: audit, two drills, an exercise.
Renewal and pen test every 5 years.

2027 is the starting line. The annual cycle runs for as long as you operate.

// WHAT THE RULE ASKS FOR

18 KEY OBLIGATIONS. ONE CySO.

CySO named in writing	Cybersecurity Assessment, every year	14-section Cybersecurity Plan	Cyber Incident Response Plan	Plan audit, every year	Training for all IT and OT staff, yearly
New hires trained within 5 days of access (30 of hire)	Plan training within 60 days of approval	Two drills every calendar year	Exercises no more than 18 months apart	Renewal and pen test every 5 years	96-hour and 30-day change notices
NRC report “without delay”	Asset inventory and network map	Approved hardware and software lists	Remote OT access justified	Third-party connections tracked	Records kept two years and protected

Most of these recur — and the assessment must cover every vessel, facility and OCS facility you operate. They land on one person, who is often also the FSO, VSO or IT manager.

// WHY IT FEELS CONVOLUTED

EIGHT GUIDANCE RELEASES IN ELEVEN MONTHS.

DATE	RELEASE	WHAT IT COVERS
Jul 22, 2025	FAQ update	Plan, reporting and other rule questions
Oct 2025	Policy Letter 01-25	Training for staff with IT or OT access
Nov 12, 2025	NVIC 02-24, Change 1	Reporting breaches and cyber incidents
Jan 9, 2026	FAQ update	Plans not yet being approved
Jan 9, 2026	Work Instruction 001	Verifying cyber training
Jun 2, 2026	Policy Letter 01-26	Assessment scoping and process
Jun 3, 2026	Work Instruction 002	Waivers and equivalency
Jun 3, 2026	Work Instruction 003	Submitting through DoD SAFE

Each release is another document to find, read and reconcile with the rule. Most of it is guidance, not regulation — the Coast Guard says use of its June 2026 guidance is not mandatory — so operators have to work out which is which.

// THE PARADOX

SUBMIT BY JULY 16, 2027. BUT DON'T SUBMIT YET.

“refrain from submitting full CSPs until further notice”

U.S. Coast Guard • June 4, 2026

“The Coast Guard is not currently approving plans for these regulations.”

USCG Final Rule FAQ • Jan 9, 2026

The Coast Guard is processing waiver and equivalency requests first and is still developing its plan review procedures. The July 16, 2027 date in the rule hasn't moved. For U.S.-flagged vessels, a 2–5 year delay was floated in January 2025, but any delay needs a separate rulemaking and none has been published. The safe position: be ready the day the window opens.

// WHAT OPERATORS ARE HEARING

THE INDUSTRY IS SAYING IT OUT LOUD.

“a source of genuine confusion about what is required, when, and of whom.”

Trident Group America, maritime security firm · July 2026

“The USCG cybersecurity rule for maritime facilities is now 2 rules, not 1.”

Kimberly Ramos, Upright Services · Sept 2026 · Part 105 plan cyber content plus the new plan

“This new reporting requirement creates a bureaucratic maze for regulated entities.”

Husch Blackwell cybersecurity team, Byte Back · July 2025 · on NRC vs. Part 6 reporting

“Coast Guard cannot readily access complete information on inspection results specific to cybersecurity...”

U.S. GAO, GAO-25-107244 · Feb 2025 · the regulator’s own inspection data

FIVE REPORTING CLOCKS. THREE REGIMES.

RULE	REPORT TO	CLOCK	STATUS
USCG · 33 CFR 6.16-1	FBI, CISA & COTP	“Immediately”	In force
USCG · 33 CFR 101 Subpart F	National Response Center	“Without delay”	In force
TSA security directives	CISA	72 hours (was 24)	In force
TSA proposed rule	CISA	24 hours	Proposed 2024
CISA · CIRCIA	CISA	72 h · ransom 24 h	Proposed 2024

“...likely create compliance challenges for certain companies and may lead to operational confusion.”

Congressional Research Service, R49009 · June 2026

FIVE DIRECTIVES. RENEWED A YEAR AT A TIME.

DIRECTIVE	COVERS	CURRENT
Pipeline-2021-01	Pipelines & LNG	01G · Jan 2026 – Jan 2027
Pipeline-2021-02	Pipelines & LNG	02G · May 2026 – May 2027
1580-21-01	Freight rail	01E · posted Jan 2026
1582-21-01	Passenger rail, transit	01E · posted Jan 2026
1580/82-2022-01	Freight & passenger rail	01E · posted May 2026

Each directive expires and is reissued, usually with changes. Operators have lived under emergency directives since the Colonial Pipeline attack in 2021.

20+

cybersecurity directives for pipeline and rail since 2021

TBD

Final rule date. The permanent rule was proposed Nov 7, 2024.

// WHAT THE DIRECTIVES ASK FOR

THE TSA CYCLE NEVER STOPS.

TSA-approved Implementation Plan	Amendments filed on deadline after changes	Assessment Plan updated for TSA every year	Annual report on last year's assessments
Every measure assessed within three years	Architecture design review at least every two years	Incident response plan exercised every year	Coordinator and alternate reachable 24/7
Incidents reported to CISA within 72 hours	Supplemental details within 24 hours	Critical Cyber Systems identified and current	Every record inspection-ready, marked SSI

An approved Implementation Plan isn't the finish line. The directives require the cycle above every year, and all of it is Sensitive Security Information.

// THE MOVING TARGET

EVERY REVISION MOVES THE GOALPOSTS.

“inapplicable, confusing, extremely costly, and disruptive to owners/operators”

Kimberly Denbow, American Gas Association · House Homeland Security subcommittee testimony, Nov 19, 2024 · on the new technical mandates added with each directive revision

THE CLOCK MOVED

Rail directives, October 2025: the reporting window went “from 24 to 72 hours.” TSA’s proposed rule would make it 24 again.

EVEN THE REGULATOR STRUGGLES

“TSA did not ensure all pipeline operators timely adhered to security requirements” — DHS OIG-23-57, Sept 2023

SUBPART F, START TO SUBMISSION.

A guided workbook for U.S.-flagged vessels, facilities and OCS facilities: every requirement in plain language, your evidence organized, your assessment, plan and records drafted.

172

paragraphs of Subpart F, each mapped to a step or explained

14

sections of the Cybersecurity Plan, drafted from your answers

24

documents: assessment, plan, letters, notices, records

26

ready-made forms and logs, pre-filled for you

PLAN & ASSESSMENT DUE JUL 16, 2027

APP TARGET: MAR 1, 2027

RESERVATIONS OPEN NOW

// HARBOR

WHAT HARBOR TAKES OFF YOUR DESK.

THE RULE

172 paragraphs, each mapped or listed with a reason. Each item labeled “required by regulation” or “Coast Guard guidance.”

THE PLAN

All 14 sections drafted from your answers. Anything unaddressed is listed, not hidden.

THE CALENDAR

Every deadline with its citation: training, drills, audits, triggers. Exports to Outlook, Google, Apple.

THE ASSESSMENT

Follows Policy Letter 01-26: functions, assets, threats, priority assets, Critical IT/OT.

THE REGISTERS

Hardware, software, network map, remote OT, compensating controls, third parties.

THE SUBMISSION

Waiver or equivalency letter drafted. Each plan ends with its certification letter, with a “How to send it” checklist for DoD SAFE.

// SECURIDIGM SIGNAL • TSA CYBER DIRECTIVES

EVERY DIRECTIVE. ONE TIMELINE.

A guided workbook for pipeline, freight rail and passenger rail operators: every requirement mapped, your yearly cycle run, submissions drafted so a reviewer can check them line by line.

565

paragraphs of the
directives, each mapped or
explained

5

directives, pipeline to
passenger rail

56

requirements labeled
Required, Guidance or
Option

19

plans, notices and records
drafted

7

forms and logs; the rest
are built into the
documents

EVALUATE NOW • 14 DAYS

PURCHASE OPENS LATER

// SIGNAL

WHAT SIGNAL TAKES OFF YOUR DESK.

WHAT APPLIES

Tick the directives TSA notified you about. Only those requirements appear, each cited.

THE REVISIONS

Each release names the revision it follows and TSA's summary. Updates are designed to open your existing workspace.

THE GAPS

Plan of action: every gap gets an owner, milestones and a due date.

THE YEARLY CYCLE

Assessment Plan update and report, 3-year schedule, architecture review, IR exercise, holiday-adjusted deadlines.

THE PAPERWORK

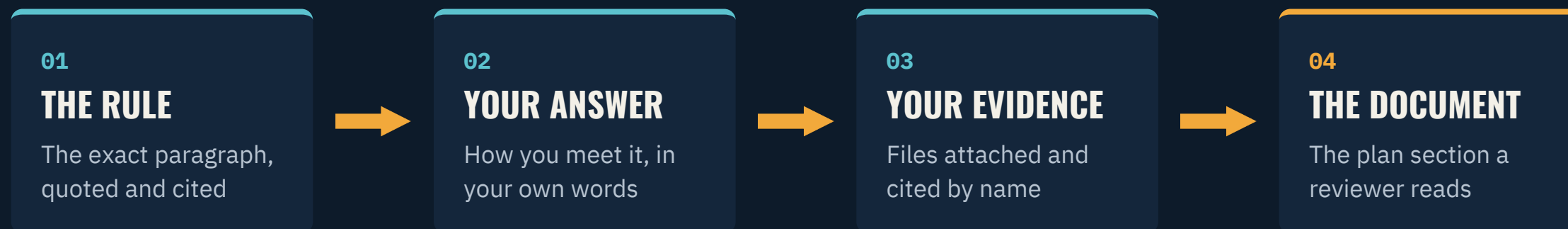
Implementation Plan, amendment requests, Coordinator notices, records package for inspection.

THE INCIDENT

72-hour CISA worksheet and call sheet, pre-filled, with the 24-hour supplement clock.

// "SHOW IT"

EVERY LINE TRACES BACK TO THE RULE.



STATUS AT A GLANCE



Missing or changed evidence is flagged. Mapped isn't met: you, your officer and the regulator decide.

Both apps show a traceability matrix on screen: paragraph → answer → evidence → plan section

// LOCAL BY DESIGN

NOTHING TO INSTALL. NOTHING TO LEAK.



ONE HTML FILE

No install, no account. Mac browsers now; Windows testing before release.



NO OUTSIDE CONNECTIONS

A security policy inside the file blocks them all.



AES-256 ENCRYPTION

Your browser's built-in cryptography. Your password.



YOUR FOLDER

Work and evidence saved, encrypted, where you choose.



SHA-256 WITH EACH RELEASE

A published fingerprint proves your copy hasn't been altered.



ONLY YOU HOLD THE KEY

We can't recover it. We can't read your data.

Your plan is SSI under 49 CFR Part 1520. It never sits on anyone's server, including ours. Printed or exported documents aren't encrypted; they carry the SSI marking.

// VERIFY IT YOURSELF

DON'T TAKE OUR WORD FOR IT. CHECK.

1

READ THE FILE

The policy that blocks outside connections is in the file. Your IT team can read it.

2

WATCH THE NETWORK

Open the browser's developer tools and use the app. Nothing goes out.

3

PULL THE PLUG

Go offline or into airplane mode. Everything still works.

4

MATCH THE HASH

Run shasum -a 256 (Mac) or Get-FileHash (Windows). Compare to the SHA-256 published with each release.

The 14-day evaluation opens from our website, so run these checks on the licensed file. Please don't enter real SSI while you evaluate.

// PLAINLY

WHAT IT IS NOT.

NOT APPROVAL

The Coast Guard and TSA decide. Mapped isn't met.

NOT LEGAL ADVICE

And we don't represent you before the Coast Guard or TSA.

NOT A CLOUD SERVICE

No account. Nothing you enter is stored on our servers.

NOT YOUR OFFICER

Your CySO or Coordinator decides how each requirement is met.

NOT A SECURITY TOOL

It doesn't scan, test or change your systems.

NOT AFFILIATED

Not affiliated with or endorsed by the Coast Guard, TSA, DHS or any agency.

// WHO BUILT IT

BUILT FROM THE INSPECTOR'S SIDE OF THE TABLE.

MICHAEL D.

FOUNDER, SECURIDIGM

M.S., Cybersecurity & Information Assurance · MBA

CISSP · CCSP · CASP+ · CySA+ · PenTest+
· SSCP · Security+ · Network+

FORMER DHS/TSA CYBER INSPECTOR

Reviewed cybersecurity programs against the NIST CSF and federal regulation. Retired June 2026.

FORMER OGA OPERATIONS OFFICER

Intelligence, counterterrorism and counterintelligence operations.

FORMER U.S. SECRET SERVICE SPECIAL AGENT

Protective details, electronic crimes, international financial-crime investigations.

DIRECTOR OF IT & SECURITY

Single-family-office portfolio of operating companies.

Independent. Built only from published regulations and public guidance: no non-public information, no SSI.

// TWO WAYS TO WORK WITH US

THE TOOL. THE PARTNER. YOUR CHOICE.

YOUR TEAM RUNS IT

SELF-MANAGED SOFTWARE

- Perpetual license for your organization (Signal: one mode)
- Guided work through every requirement
- Documents drafted from your answers
- First year of updates and email support
- Optional yearly renewal; the app keeps working if you don't

SECURIDIGM WORKS WITH YOU

MANAGED READINESS

- Facilitated interviews, running the app with you
- Document preparation and evidence organization
- Action tracking and progress reviews
- Scope agreed up front
- Quoted per engagement

// NEXT STEP

TWO WAYS TO START.

SECURIDIGM HARBOR

RESERVE YOUR LICENSE

- Letter of intent: no payment, no obligation
- Founding customers: renewal price locked while you renew (conditions apply)
- Ask to join the pilot group (by invitation)
- App target: March 1, 2027

securidigm.com/coast-guard

HARBOR & SIGNAL

EVALUATE FOR 14 DAYS

- The full app, every screen and document
- A sample company or your own workspace
- Personal link, usually within two business days
- Your workspace carries into the offline app

securidigm.com/evaluate

PLAN AND ASSESSMENT DUE JULY 16, 2027. BE READY THE DAY THE WINDOW OPENS.

// SOURCES

WHERE EVERY NUMBER AND QUOTE COMES FROM.

USCG, Cybersecurity in the Marine Transportation System, 90 FR 6298 (Jan 17, 2025); 33 CFR 101 Subpart F

USCG Maritime Commons, policy and guidance release (June 4, 2026)

USCG Final Rule FAQ, updated Jan 9, 2026; USCG fact sheet (Jan 2025)

Congressional Research Service, R49009, Cybersecurity: Considerations on Regulatory Harmonization (June 26, 2026)

GAO-25-107244 (Feb 11, 2025); GAO-25-108436 (July 30, 2025)

E. Dullea, J. Maurer & B. Nashed, Husch Blackwell, Byte Back (July 31, 2025)

Trident Group America, “The Law Has Landed” (July 26, 2026)

K. Ramos, Upright Services (upright.com), “The USCG Maritime Cyber Rules Texas Operators Keep Missing” (Sept 4, 2026)

K. Denbow, American Gas Association, testimony to the House Homeland Security transportation and maritime subcommittee (Nov 19, 2024)

DHS OIG, OIG-23-57 (Sept 27, 2023)

TSA SD 1580-21-01D memo (Oct 22, 2025); SDs Pipeline-2021-01G and -02G; tsa.gov/sd-and-ea

TSA, Enhancing Surface Cyber Risk Management, 89 FR 88488 (Nov 7, 2024); reginfo.gov RIN 1652-AA74

CISA, CIRCIA NPRM, 89 FR 23644 (Apr 4, 2024)

USCG Work Instruction 001 (Jan 9, 2026); securidigm.com and the apps (Oct 17, 2026)