DRAGOS

DATASHEET

OIL AND GAS PIPELINES

Align With TSA Pipeline Requirements While Safeguarding Operations

Dragos maps to TSA Security Directive Pipeline-2021-02G and supports API Standard 1164, so pipeline operators can see their environment, detect threats, and produce evidence on TSA's annual cycle.

The Challenge Pipeline Operators Face

Pipelines once ran on isolated control networks. Today, control centers, compressor and pump stations, meter stations, LNG facilities, and vendor connections are linked across hundreds or thousands of miles. Every link creates a path between enterprise IT and the systems that move product.

Since the 2021 Colonial Pipeline ransomware attack, TSA has required owners and operators of designated critical natural gas and hazardous liquid pipelines and LNG facilities to meet mandatory cybersecurity requirements. Those requirements cover both IT and OT, and they are renewed every year.

Requirements Are Performance-Based

- **TSA sets the outcomes.** Each operator writes, implements, and maintains a TSA-approved Cybersecurity Implementation Plan for its Critical Cyber Systems.
- **OT must keep running if IT is compromised.** Segmentation is designed to achieve that outcome. Access control, continuous monitoring, and risk-based patching reinforce it.
- **Evidence runs on a fixed clock.** Annual assessments, annual incident response exercises, and periodic architecture design reviews require current proof, not point-in-time reconstructions.

Visibility, Detection, and Evidence From One Place

Dragos shows pipeline operators what assets exist, how they communicate, which access paths configurations permit, which vulnerabilities matter now, and where adversary behavior is showing up. The same data becomes the audit-ready evidence TSA expects.

SUPPORTING PROOF POINTS

70%

of OT incidents originate in IT. [1]

THE RISK

On a pipeline, an IT compromise can halt product movement even when control systems are untouched. Weak IT/OT separation turns a business-network incident into an operational one.

REQUIREMENTS

- **TSA SD Pipeline-2021-02G**
- **TSA SD Pipeline-2021-01G**
- **PI Std 1164, 3rd Edition**
- **NIST Cybersecurity Framework**
- **ISA/IEC 62443**

[1] Dragos Year In Review 2024

 | © 2026 Dragos, Inc. All Rights Reserved.

Built for How Pipelines Operate

Pipeline OT is distributed, long-lived, and connected over telecom links that span entire regions. Dragos covers each part of that footprint with a passive-first approach that does not put operations at risk.

01
Control centers and backup control centers

Platform sensors perform deep packet inspection across 600+ industrial protocols to baseline SCADA servers, HMIs, historians, and the IT/OT boundary where most incidents begin. Detections are mapped to MITRE ATT&CK for ICS and linked to response playbooks.

02
Compressor, pump, and meter stations

Station traffic is often sparse and equipment can be decades old. Where passive monitoring cannot see enough, the Dragos Agent collects firmware, OS, and patch-level detail, and data import adds context from engineering project files.

03
Remote sites and telecom paths

Dragos Segmentation reads firewall, router, and switch configurations offline, with no agents, no scans, and no traffic on the OT network. Teams can assess remote, sensitive, or air-gapped sites and see every access path their configurations permit, including paths that have never carried traffic.

04
Vendor and third-party remote access

Path analysis shows which remote access routes into OT the configurations actually allow. Platform detections surface remote access sessions and unexpected communications, giving teams evidence that access controls work as designed.

05
LNG facilities and process control

The same capabilities apply to liquefaction and storage facilities covered by the directive. Detections built from Dragos analysis of ICS malware, including PIPEDREAM, ship to the Platform through Knowledge Packs.

06
Acquisitions, laterals, and expansions

New assets and acquired systems arrive with unknown inventories and inherited configurations. Asset discovery and segmentation validation bring them into the Implementation Plan before they become a gap in the next assessment.

THE TSA CLOCK

What SD Pipeline-2021-02G asks operators to prove, and how often.[3]

- **Directive renewal:** Every 12 months
- **Assessment Plan resubmitted:** Every 12 months
- **Annual assessment report:** Every 12 months
- **Incident response exercise testing at least two plan objectives:** At least once a year
- **Architecture design review:** Every 24 months
- **100% of the Implementation Plan assessed:** Every 36 months

SUPPORTING PROOF POINTS

3-6%

of OT vulnerabilities require immediate action.[2]

73%

of Dragos incident response cases involve compromised VPN or jumphost credentials.[2]

42 days

average OT dwell time.[2]

[2] Dragos OT/ICS Cybersecurity Year in Review, 2026

[3] TSA Security Directive Pipeline-2021-02G, Sections III.F and III.G

 | © 2026 Dragos, Inc. All Rights Reserved.

Mapping Dragos to TSA Security Directive Pipeline-2021-02G

TSA organizes the directive around three operator-owned plans. Each required area maps to the Dragos capabilities that support it. Section references follow SD Pipeline-2021-02G.

TSA REQUIREMENT	WHAT TSA EXPECTS	HOW DRAGOS SUPPORTS IT
IMPLEMENTATION PLAN SECTION III.A **Critical Cyber Systems**	Identify the IT and OT systems and data that, if compromised, could disrupt pipeline operations, and keep that list current.	**Asset Visibility and Inventory.** Multi-detection engine monitoring across 600+ industrial protocols builds a continuously updated inventory. The Dragos Agent and data import fill gaps in segmented or low-traffic segments. **OT Cybersecurity Assessment.** Through documentation reviews, staff interviews, and network data collection, Dragos experts run a crown jewel analysis that identifies the systems whose compromise would cause the greatest operational, safety, or financial impact, with prioritized recommendations to protect them. **Dragos EmberAI.** As assets are added or changed, the Crown Jewel Analysis Skill guides analysts through identifying and tagging critical assets in the Platform, keeping the Critical Cyber Systems list current. The practitioner approves every change.
SECTION III.B **Network Segmentation**	Segment IT and OT so neither can disrupt the other if compromised. Document IT/OT interdependencies, all external connections to OT, and zone boundaries, and prevent unauthorized communication between zones.	**Dragos Segmentation**. Reveals every access path firewall, router, and switch configurations permit, including external connections into OT. Policy Manager flags risky rules and traces each finding to the exact line in the exact config file. More than 25 supported vendors. **Network Monitoring.** Sensors baseline communications at the IT/OT boundary and within OT zones. Together with Segmentation, teams verify that network-based compensating controls hold.
SECTION III.C **Access Control**	Secure local and remote access to Critical Cyber Systems with multi-factor authentication or equivalent controls, apply least privilege, limit shared accounts, and review domain trust relationships.	**Threat Detection.** Surfaces remote access sessions, new or unauthorized communications, credential misuse, and assets using default or insecure credentials across monitored zones, with response playbooks. Dragos does not enforce access policy; it provides evidence that access controls work. **Dragos Segmentation.** Path analysis shows which remote access routes into OT configurations permit.
SECTION III.D **Continuous Monitoring and Detection**	Continuously collect and analyze data for intrusions and anomalous behavior. Block known or suspected malicious IP addresses, domains, and command-and-control connections. Audit OT communications with external systems that deviate from the established baseline and be able to isolate control systems when an IT incident puts OT at risk.	**Threat Detection.** Continuously monitors traffic to and between Critical Cyber Systems, within OT and across the IT/OT boundary, to catch intrusions that have already bypassed perimeter defenses. Baselines of expected asset and network behavior surface anomalous activity. Modeling, configuration, indicator, and threat behavior detections mapped to MITRE ATT&CK for ICS. Composite Detections correlate related alerts across time and data sources into a single, higher-order alert that shows a coordinated campaign. Weekly Knowledge Pack updates add new detections, IOCs, and playbooks from Dragos threat intelligence as adversaries change their tactics. **Neighborhood Keeper.** Threat activity validated in one participating OT environment is shared, anonymized, with other participants as Trusted Insight Alerts, so operators can detect it earlier in their own environment. Opt-in, at no additional cost for Dragos Platform customers. **OT Watch and OT Watch Complete.** Expert-led threat hunting, and with OT Watch Complete, 24/7 monitoring and SLA-based alert triage. **Integrations.** Dragos xOT Threat Intelligence IOCs and Platform detections flow to existing SIEM, SOAR, and firewall tools.

© 2026 Dragos, Inc. All Rights Reserved.

TSA REQUIREMENT	WHAT TSA EXPECTS	HOW DRAGOS SUPPORTS IT
SECTION III.E **Patch Management**	Reduce exploitation risk of unpatched systems with a risk-based methodology, prioritizing vulnerabilities in CISA's Known Exploited Vulnerabilities Catalog, with documented mitigations and timelines where patching would degrade operations.	**Vulnerability Management.** OT-corrected scoring and "Now, Next, Never" prioritization identify the 3-6% of OT vulnerabilities that require immediate action. **Alternative mitigations.** OT-specific compensating controls, configuration changes, and detection signatures reduce risk until the next maintenance window. **Vulnerability Dispositions.** Each decision is recorded where the vulnerability data lives: Risk Accepted, Compensating Control, Deferred, or Third-Party Controlled, with rationale and review. New evidence can reopen a resolved finding.
SECTION III.F **Incident Response**	Maintain a Cybersecurity Incident Response Plan covering containment, segregation, backup integrity, and IT/OT isolation. Exercise at least two plan objectives each year with the named responders participating.	**Investigation and Response.** Insights Hub, case management, timeline views, and Response Playbooks authored by Dragos OT experts. **Tabletop Exercises.** Scenarios built on real adversary TTPs test the plan with documented results. An After-Action Report rates performance and prioritizes recommendations for improving the Incident Response Plan. **Rapid Response Retainer.** 24/7 access to Dragos OT incident responders, with SLA-backed first contact within one hour for Platform customers.
SECTION III.G **Cybersecurity Assessment**	Assess at least one-third of the Implementation Plan each year and all of it over any three-year period. Complete an architecture design review at least every two years, including network traffic validation and system log review, plus penetration testing and red or purple team exercises.	**Cybersecurity Architecture Design Review.** Evaluates controls against frameworks including TSA pipeline requirements, NIST, and ISO. **Red Team Services.** Vulnerability assessment, penetration testing, and purple team exercises validate that controls hold.
SECTION IV **Records and Inspection**	Make records available to TSA, including asset inventories, firewall rules, network diagrams, switch and router configurations, VLANs, log files, and up to 24 hours of network traffic capture covering East-West and North-South traffic.	**Dragos Platform.** Exportable asset inventory and network topology provide audit-ready evidence. Teams can search captured packets or start a new capture on demand, then download the PCAP files, with an auditable record of every capture job. **Dragos Segmentation.** Firewall, router, and switch configurations, topology, and the three most recent configuration versions with visual diffs show how configurations changed. Segmentation and Best Practice reports provide a durable audit record.
SD PIPELINE-2021-01G **Reporting and Coordination**	Designate a primary and alternate Cybersecurity Coordinator, reachable 24/7, and report cybersecurity incidents to CISA no later than 72 hours after identification.	**Investigation and Response.** Packages forensic artifacts, analyst notes, and timelines to support regulator reporting. **Rapid Response Retainer.** Supports communications to executives, regulators, and stakeholders during an incident.

© 2026 Dragos, Inc. All Rights Reserved.

The Current Regulatory Landscape

TSA SD Pipeline-2021-02G	In force May 3, 2026 through May 2, 2027. Implementation, incident response, and assessment plans for Critical Cyber Systems. Renewal of 02F with no substantive changes.
TSA SD Pipeline-2021-01G	In force January 16, 2026 through January 15, 2027. 24/7 Cybersecurity Coordinator, incident reporting to CISA within 72 hours, and a vulnerability assessment. Adds vetting requirements for non-U.S. citizen coordinators.
API Std 1164, 3rd Edition	Published August 2021. Risk-based management system for pipeline control systems cybersecurity, extending scope beyond SCADA to the full industrial automation and control environment.
TSA proposed rule	"Enhancing Surface Cyber Risk Management," proposed November 7, 2024 and not final as of this datasheet. Would replace the directives with permanent regulation.

Aligned to API Standard 1164

API Std 1164 sets a risk-based management system for pipeline control systems cybersecurity. The Dragos Platform supports its core expectations: an accurate inventory of control system assets, network visibility and monitoring, risk-based vulnerability management, detection of adversary behavior, and documented incident response. Dragos services support program review and governance through assessments, tabletop exercises, and incident response retainers.

Why Pipeline Operators Choose Dragos

- **Built for OT.** Purpose-built for OT cybersecurity, with a passive-first approach that does not put operations at risk.
- **Intelligence that tracks the adversaries.** Research from the Dragos Intelligence Fabric ships to the Platform as detections, playbooks, and vulnerability guidance.
- **Prioritized action, not noise.** "Now, Next, Never" shows which vulnerabilities to act on first.
- **Frontline experience.** Over a decade of OT-specific incident response informs every playbook, assessment, and exercise.

This datasheet reflects Dragos' understanding of TSA Security Directives Pipeline-2021-01G and Pipeline-2021-02G as of November 2026. It is not legal advice. Owners and operators remain responsible for compliance with their TSA-approved plans; consult the directive text and TSA for authoritative requirements.

RECOGNITION

Named a Leader in the 2026 Gartner® Magic Quadrant™ for CPS Protection Platforms.

INTELLIGENCE

26+

OT threat groups tracked by name.[2]

COMMUNITY

600+

customers globally.[4]

[2] Dragos OT/ICS Cybersecurity Year in Review, 2026

[4] Dragos, 2026

Talk to an OT Security Specialist.

See how Dragos supports pipeline operators at dragos.com

Connect With an Expert

 | © 2026 Dragos, Inc. All Rights Reserved.