IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

# PIPELINE CYBERSECURITY


The U.S. pipeline infrastructure is critical to the functioning of the Nation's economy. Composed of more than 2.7 million miles of pipeline, this vast network is responsible for transporting natural gas, liquid fuels, and other commodities for use in homes and businesses such as airports, power plants, farms, and refineries. As automation drives pipeline owners and operators to rely on an increasingly complex web of interconnected devices to run their business and operational systems (e.g., industrial control systems), they must also implement security measures to protect their pipeline operations from evolving and emerging cyber risks.

The **Cybersecurity and Infrastructure Security Agency (CISA)**, through the **National Risk Management Center (NRMC)**, is working with government and industry partners to identify cybersecurity risks and develop strategies to strengthen the security and resilience of the Nation's pipeline infrastructure.

## PIPELINE CYBERSECURITY INITIATIVE OVERVIEW

Pipelines are an efficient and safe means of transporting materials—many of which are flammable or toxic. To increase efficiency and reliability and to reduce costs, pipeline owners and operators leverage information technology (IT) and operational technology (OT) extensively in their day-to-day operations. In today's evolving threat environment, the inherent vulnerabilities in these IT and OT systems can present high-consequence opportunities for foreign adversaries, hackers, and other malicious actors to exploit.

In October 2018, the U.S. Department of Homeland Security created the **Pipeline Cybersecurity Initiative (PCI)** and charged CISA and the Transportation Security Administration (TSA) with assessing cybersecurity risks to the Nation's pipeline infrastructure—with a focus on oil and natural gas (ONG) pipelines. This effort aligns CISA's cybersecurity resources, the TSA's pipeline security relationships and authorities, and the Department of Energy's (DOE) energy sector expertise with industry knowledge and experience to identify cybersecurity risks and develop risk strategies to prepare for, respond to, and mitigate significant cyber events.

Three primary functions of the PCI are:

**Assessing the cybersecurity posture and preparedness** of pipeline companies to identify significant vulnerabilities that increase risk to key systems and reliable operations.

**Analyzing assessment findings** to develop risk mitigation strategies and informational tools that companies may use to address the identified risks.

**Engaging with partners and industry stakeholders** to share information, raise awareness of critical issues, and inform pipeline cybersecurity activities.

## PIPELINE CYBERSECURITY RISKS

Pipeline infrastructure is critical to national security both because of the materials transported and because pipeline operations rely on, and impact, many critical infrastructure sectors including energy, water and wastewater systems, chemical, and transportation systems. Additionally, as one of the 55 **National Critical Functions (NCFs)**; the operational disruption, corruption, or dysfunction of pipelines would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. To learn more about NCFs, visit, cisa.gov/national-critical-functions.

A cyberattack on a pipeline system could result in explosions and spills; equipment sabotage, malfunction, and unanticipated shutdowns; theft of intellectual property; and supply chain disruptions to midstream and downstream operations to other NCFs. The consequences of an attack could impact fuel, natural gas, and certain chemical supplies; cause power shortages; damage the environment; and hinder manufacturing across sectors.

## ENHANCING PIPELINE CYBERSECURITY

To build a better understanding of the pipeline OT and IT cybersecurity environment, CISA and TSA are working with pipeline owners and operators to conduct voluntary, non-regulatory cyber assessments. These in-depth reviews provide CISA technical experts an opportunity to review network architecture design, system configuration and logs, and network traffic and provide recommendations on how owners and operators can improve their cybersecurity. They also contribute to an understanding of the overall risk to the critical function.

Additionally, the NRMC's National Infrastructure Simulation and Analysis Center (NISAC) supports programs intended to gain an in-depth understanding of critical pipeline components and conduct modeling and simulations to:

- Analyze pipeline OT infrastructure to identify vulnerabilities with the highest risk
- Determine the cascading impacts of a successful attack within and across sectors
- Engineer solutions to reduce the likelihood of a successful attack
- Develop a roadmap for improving pipeline cyber resilience

To learn more about the cyber assessments, visit: www.us-cert.gov/resources/ncats.
To learn more about NISAC, visit: www.dhs.gov/about-national-infrastructure-simulation-and-analysis-center.

## BUILDING LONG-TERM RESILIENCY

Protecting the Nation's pipeline ecosystem depends on a unified effort. CISA is also engaging with the private industry through the ONG Subsector Coordinating Council (SCC)—composed of pipeline owners, operators, and other key stakeholders—to share timely information and ensure that actionable risk mitigation strategies are also informed by stakeholders' self-identified needs. This holistic collaboration builds a national culture of pipeline security and resilience and strengthens economic and national well-being.

To learn more about the ONG SCC, visit: www.ongsubsector.com.

## PCI RESOURCES

- Pipeline Cybersecurity: cisa.gov/pipeline-cybersecurity-initiative
- Pipeline Cyber Risk Mitigation Infographic: cisa.gov/publication/pci-cyber-risk-infographic
- NRMC Resources: cisa.gov/nrmc-resources

For questions or to seek additional help, contact us at NRMC@hq.dhs.gov.