E-BOOK

Pipeline Protection Priorities

TSA Compliance and Beyond: Investing in a Security Solution that Supports Safety and Availability

Table of Contents

Executive Summary

The 2021 Annual Threat Assessment of the U.S. Intelligence Community and the 2020 Homeland Threat Assessment, among others, note that certain nations and criminal groups pose the greatest cyberattack threats to U.S. critical infrastructure. Industrial control systems — typically network-based systems that monitor and control sensitive processes and physical functions, including those needed to operate pipelines — are increasingly connected in modern energy systems. While this form of digital transformation provides real-time data for better business decisions, it also opens the door for cyberattacks that often originate in business IT systems to migrate to industrial control systems.

This led the federal government, under the authority of the TSA, to create a set of stringent security guidelines for pipelines, which are considered part of the nation's critical infrastructure. With the implementation deadline already passed and fines looming, compliance with the new TSA directives for cybersecurity resilience was understandably a significant item on many organizations' priority lists this year.

With the implementation deadline already passed and fines looming, compliance with the new TSA directives for cybersecurity resilience was understandably a significant item on many organizations' priority lists this year.

Fortinet offers specific solutions to comply with the Pipeline Security Directive — and beyond. Equally important, we realize that there is much more value to be realized by organizations who invest in their future by going beyond meeting minimum compliance. With a portfolio the provides broad, integrated and automated cybersecurity that is unmatched in the industry, Fortinet's ability to help our customers navigate these uncertain waters is second to none. We invite you to speak with our industrial cybersecurity experts or visit us online at www.fortinet.com/OT.

Introduction: The TSA Pipeline Cybersecurity Directive

The fallout and impact of the May 2021 pipeline ransomware attack[1] — enabled by a single leaked password[2] — attracted intense congressional and national agency scrutiny. The resulting federal report identified four significant federal cybersecurity challenges. The solution to one of those challenges, protecting critical infrastructure, was to strengthen the federal role in the cybersecurity of critical infrastructure, such as pipelines.

The United States TSA, under the auspices of the Department of Homeland Security, developed and issued a comprehensive security directive mandating that critical pipeline owners and operators implement several urgently needed cybersecurity resilience measures. In the time period following this attack, the threat posed to this sector has evolved and intensified. Reducing this national security risk requires public and private collaboration.

The new cybersecurity resilience requirements apply to all U.S. locations of owners and operators of a hazardous liquid and natural gas pipeline or a liquefied natural gas facility who have been notified by TSA that their pipeline system or facility is critical. Additionally, they apply to operational pipeline systems that transport materials categorized as toxic inhalation hazards (TIH). **The deadline** to submit a Cybersecurity Implementation Plan for TSA approval **was October 25, 2022**. If you are reading this ebook, you may have either achieved some level of compliance — or are facing the possibility of fines for not doing so. You may also be working through feedback from the TSA on areas of improvement based upon the plan that you submitted.

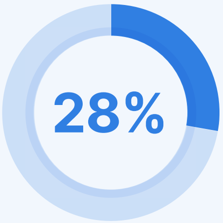
Global cybersecurity spending in industrial critical infrastructure sectors such as energy, transport, and water and waste water management is projected to reach **$36.67 billion** by 2027.[3]

Recognizing Risks and Impacts

The convergence of IT and OT networks has greatly expanded the attack surface of industrial and critical infrastructure environments. The long-standing protection by isolation “air gap” and “security by obscurity” is all but gone, and a false sense of confidence remains for many who operate OT networks’ cybersecurity resilience with a legacy mindset.

Threats to critical infrastructure typically stem from two main sources: nation-states and criminal groups.

Nations of concern: China, Russia, Iran, and North Korea have the ability to launch cyberattacks that could disrupt or damage critical infrastructure, according to the Office of the Director of National Intelligence Annual Threat Assessment.



28% of breaches amongst critical infrastructure were ransomware or destructive attacks.[4]

Criminal groups: In addition, according to the 2020 Homeland Threat Assessment, cybercriminals will increasingly target critical infrastructure to generate profit. These cybercriminals will use ransomware to exploit gaps in the cybersecurity of critical infrastructure entities.

Malicious actors have a number of tactics, techniques, and procedures at their disposal to compromise the cybersecurity of critical infrastructure, such as pipelines. Some of the methods of attack and the possible impacts include:

METHODS
• **Spearphishing** to obtain initial access to the organization’s information technology (IT) network before pivoting to the OT network
• Deployment of **commodity ransomware** to encrypt data for impact on both networks
• Connecting to **internet accessible PLCs** requiring no authentication for initial access
• Utilizing **commonly used ports and standard application layer protocols**, to communicate with controllers and download modified control logic
• Use of vendor **engineering software and program downloads**
• Modifying **control logic and parameters** on PLCs

IMPACT
• Impacting a loss of **availability** on the OT network
• Partial loss of **view** for human operators
• Resulting in loss of **productivity and revenue**
• Adversary **manipulation of control** and disruption to physical processes

Beyond the Directive: The Need for Agile Security

Just as threats and technology evolve, it is worth noting that governmental regulations tend to evolve and expand in scope over time. Fortinet recommends an approach that goes beyond compliance. This helps to future-proof your current efforts and make for easier, more cost-effective adjustments should these directives grow in complexity or scale.

There are several good reasons why the TSA directives should be considered table stakes – or a starting point – for energy companies when it comes to cyber resilience. Compliance is the perfect opportunity to improve your OT security posture. A close consideration of assets, users, and access can enable organizations to define their current risks and proactively ensure they have the right security processes and architecture in place.

The 2022 State of Operational Technology and Cybersecurity Report released by Fortinet reveals that organizations are still moving too slowly toward full protection of their operational technology (OT) assets. With 93% of OT organizations experiencing an intrusion in the past year and 78% of them experiencing more than three intrusions, it's more imperative than ever that CISOs and business leaders improve their OT security and implement best practices outlined in Fortinet's report.[5]

This report highlights why OT security strategy should be a top-level concern that goes far beyond mandated compliance. Items of concern to businesses include:

Business and financial impacts
Attacks on OT can significantly impact an organization's productivity and, therefore, its finances.

Security Gaps with Point Products
The vast majority of organizations use between two and eight different security vendors for securing their industrial devices, with a complex combination of 100 to 10,000 devices in operation.

Lack of Centralized Visibility
Without the centralized visibility of OT activities, the network and entire organization lacks focus and becomes much more vulnerable.

Clarity on Responsibilities
Only 15% of those surveyed say that their CISO is responsible for OT security at their organization — but safety dictates there must be a designated, highly qualified security individual protecting your OT networks.

Organizations that take the TSA mandates beyond meeting minimum compliance will earn greater credibility and have an opportunity to build trust with regulators, legislators, and surrounding communities. In addition to the goodwill at stake, energy providers and infrastructure owners are obligated to consider the potentially fatal outcomes of a cyberattack on their operations.

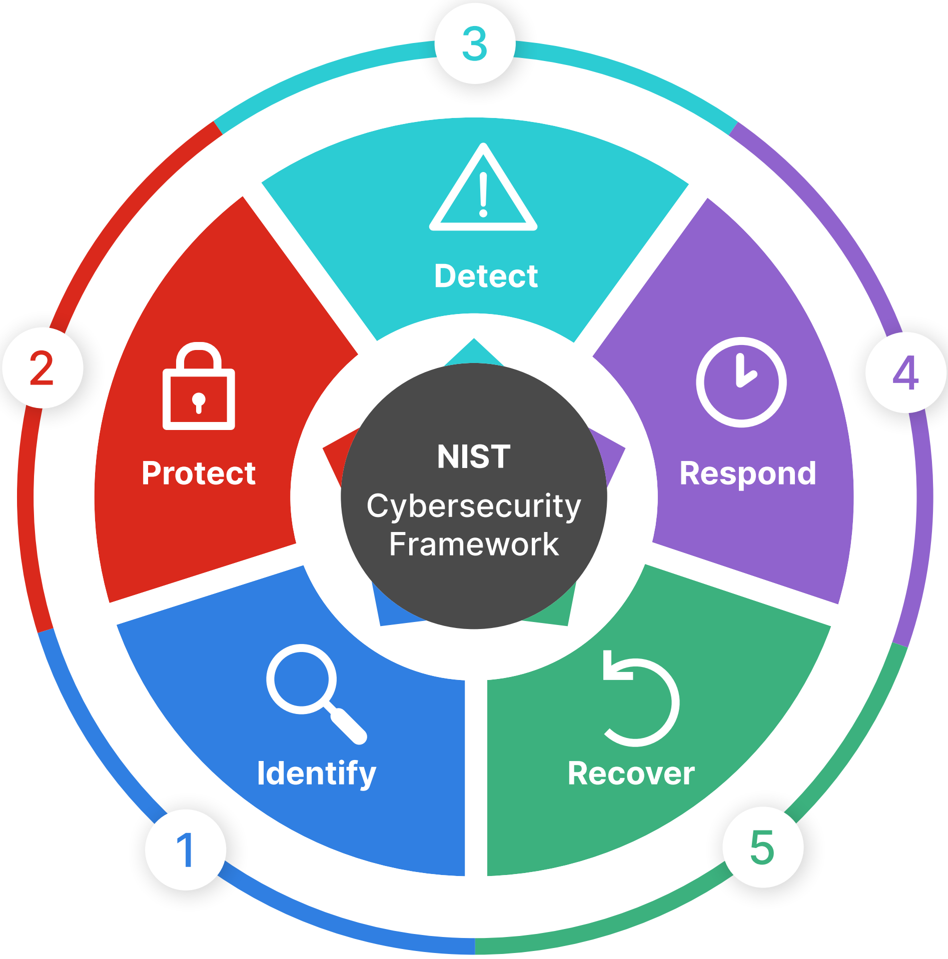
The number one concern of senior cyber leaders globally is infrastructure breakdown due to a cyberattack.[6]

A Framework for Maturing Your Cyber Plan and Security Technology

Understanding the nuances of the TSA requirements, as well as the growing sophistication of hackers and the impact that IT/OT network convergence has had on the vulnerability of critical infrastructure, can save both time and money when it comes to achieving compliance. Going beyond compliance, however, sets up your organization for better protection and leaves you in a better position as the TSA directives expand.

A recommended approach to developing and implementing measures for pipeline cybersecurity that also paves the path to cybersecurity maturity leverages the NIST (National Institute of Standards and Technology) Cybersecurity Framework.[7] The NIST Framework provides a common language for understanding, managing, and expressing cybersecurity risk both internally and externally. It can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk. It can be used to manage cybersecurity risk across entire organizations or it can be focused on the delivery of critical services within an organization. Different types of entities – including sector coordinating structures, associations, and organizations – can use the framework for different purposes.

The framework covers five specific pillars: functional areas that, when addressed together, lead to increased cybersecurity maturity, compliance, and resilience.



NIST Pillar 1: IDENTIFY

Key points: asset inventory | cybersecurity governance | risk management

The foundations of the cybersecurity maturity journey begin here, by identifying the data and systems that need to be protected. A company must employ mechanisms to maintain an accurate inventory of assets and to detect unauthorized components.

Look for solutions that are capable of:

- Reviewing network connections periodically
- Developing a detailed inventory for every endpoint
- Reviewing and assessing pipeline cyber asset classification as critical or non-critical at least every 12 months

Part of the Identify function includes monitoring the business environment. Your chosen solution must ensure that any change that adds control operations to a non-critical pipeline cyber asset results in the system being recognized as a critical pipeline cyber asset and enhanced security measures being applied.

Governance plays a key role in this step. Cybersecurity policies, plans, processes, and supporting procedures must be reviewed and assessed regularly, not to exceed 36 months, or when there is a significant organizational or technological change.

Your risk management strategy is also part of this phase. Your business must develop an operational framework to ensure coordination, communication, and accountability for information security on and between the control systems and enterprise networks.

It's impossible to develop a robust risk management strategy, however, without first performing a thorough risk assessment.

You or your security partner must:

- Establish a process to identify and evaluate vulnerabilities as well as compensate for security controls
- Ensure threat and vulnerability information received from information sharing forums and sources are made available to those responsible for assessing and determining the appropriate course of action

NIST Pillar 2: PROTECT

Key points: access control | data protection | security awareness and training

This portion of the framework requires a company to employ mechanisms to maintain accurate inventory and to detect unauthorized components. This starts with access control, which means you must establish and enforce unique accounts for each individual user and administrator, establish security requirements for certain types of privileged accounts, and prohibit the sharing of these accounts.

Tools

Your team must also put security measures into place to safeguard the data. These will often involve specific tools, hardware, and software designed to address common security concerns. However, it may also involve getting stakeholders and employees on board so everyone can work together to guard sensitive data and systems.

Practices

Another important aspect of access control is to restrict user physical access to control systems and control networks through the use of appropriate controls. Employing more stringent identity and access management practices (e.g., authenticators, password-construct, access control) plays an important role.

Training

A third piece of the access control equation is awareness and training for all personnel. Companies need to provide role-based security training on recognizing and reporting potential indicators of system compromise prior to obtaining access to the critical pipeline cyber assets. Some cybersecurity experts, like Fortinet, provide training to create a cyber-aware workforce.

A good training curriculum should be:

- Easily accessible to all workers
- Varied to meet all learning needs (instructor-led, virtual instructor-led, and self-paced formats)
- Comprehensive, offering not only courses but also optional lessons, email templates, awareness tools and an administrator dashboard for easy compliance monitoring

In addition to access control, a key component of this functional area is the protection of data security and information. Cybersecurity leaders need to establish and implement policies and procedures to ensure data protection measures are in place — including identifying critical data and establishing classification of different types of data, establishing specific handling procedures, and protection and disposal.

Fulfilling the requirements to Protect also means deploying proactive technologies that can segregate and protect the pipeline cyber assets from enterprise networks and the internet using physical separation, firewalls, and other protections. The protective technology you choose must be able to regularly validate that technical controls comply with the organization’s cybersecurity policies, plans and procedures, as well as reporting results to senior management.

NIST Pillar 3: DETECT

Key points: intrusion monitoring | event detection | event classification

This functional pillar begins with the ability to detect suspicious events and anomalies. Tools and policies relevant to this phase are designed to discover an incident when it happens.

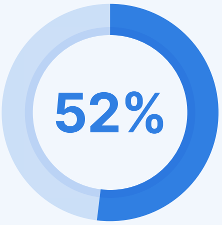
Key requirements for success include:

- Enhanced visibility into the various systems, networks, and devices used by the organization
- Implementation of processes to generate alerts and log cybersecurity events in response to anomalous activity
- Timely review of logs and response to alerts

To meet the Detect NIST Framework requirements, you must also have robust detection processes in place. This means establishing technical or procedural controls for cyber intrusion monitoring and detection.

The growing role of AI

The powerful future of breach protection technology is AI-driven. Such solutions are pre-trained via deep machine learning and designed for Security Operation Center (SOC) teams defending against various threats. An ideal choice will dynamically profile your organization's network activity and conduct file-based analysis to help you identify, classify, and respond to advanced, persistent threats — including those that are well-camouflaged.



Barely half (52%) of the surveyed organizations can track all OT activities from their security operations center (SOC).[8]

NIST Pillar 4: RESPOND

Key points: threat response | threat mitigation | the role of AI

To comply with the Respond pillar of the NIST framework, organizations must have a way to respond to and mitigate threats. This requires the establishment of technical or procedural controls for cyber intrusion monitoring, detection, and mitigation. The plan will include the different methods used to mitigate the threat, as well as which tools will be used.

An organization's response mechanism may include intentional redundancies designed to approach a threat from multiple angles, such as redundant firewalls or antivirus software. AI-driven technology also comes into play in responding to threats — an important consideration for organizations that are short-staffed or short-skilled in a world where vulnerabilities are exploited around the clock with increasing sophistication. These shortfalls play a large role in the expectation that the AI cybersecurity market will go from today's $8 billion to $38 billion in just 4 short years.[9]

AI-driven response offers several advantages, including:

- Speed: a strong solution can provide sub-second investigation and immediate response
- 24/7 protection: because they can automatically respond to detected threats, your organization's cybersecurity is always on, even if your people aren't
- Expert identification: solutions that use deep learning technologies not only identify different breeds of attacks, but they can also identify the right response to that type of attack

NIST Pillar 5: RECOVER

Key points: regain control | prioritize planning | incident readiness

In the event an attack penetrates the network, the final function covered by NIST includes ways of helping an organization recover as quickly as possible. This may include recovering data from backups, regaining control of workstations, or spinning up parallel devices. Recovery may also include resiliency measures and tools that ensure the company has as little downtime as possible.

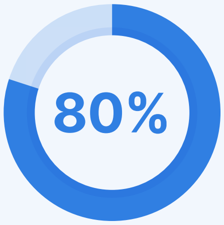
With today's fast-paced threat landscape, it is important to carve out time for planning tasks in the SOC, among all the urgent reactive tasks. A list of internal and external resources for recovery activities should be developed and kept up-to-date as part of the Recovery planning effort. Reviewing and documenting actions in the wake of an attack can also help organizations glean valuable insights that can be used to strengthen existing recovery plans and processes moving forward.

Readiness Assessments:

Conducting readiness assessments can prepare your organization for cyber incidents and shorten the time to recovery while minimizing business impact. Typically conducted by an outside partner, this kind of assessment tests your technology, people, and process effectiveness against a full flow of attacks.

Good incident response readiness assessments will help you:

- Assess your current capabilities for defending against targeted attacks
- Prioritize cybersecurity actions and investments
- Strengthen your response readiness and efficiency



Almost 80% of critical infrastructure organizations studied don't adopt zero-trust strategies, which resulted in a 25% increase in breach costs.[10]

Conclusion: The Value of Proactive Security and Compliance

TSA compliance is all about reducing risk. But the most secure, resilient path requires employing security best practices and improving an organization's security posture beyond the directive.

Building an integrated security architecture not only simplifies audit preparation but also makes an organization safer in the following ways:

- By eliminating manual reporting, threat response, and other processes, security staff can focus on strategic initiatives.
- By automating threat-intelligence analysis and threat response, organizations can catch fast-moving threats before they cause a problem.
- By building security into the foundation of industrial operations rather than adding it as an afterthought, vulnerabilities can be caught before they result in breaches.
- By effectively segmenting the network and inspecting all traffic — internal and external — organizations can ensure that access is aligned by role and responsibility.
- By deploying centralized analytical tools, organizations can bolster their security in a strategic, prioritized manner.

The above enables industrial, operational, and security leaders to transform their security and compliance postures from reactive to proactive. It moves requirements like the TSA directive from an annoying checkbox to a method of continuing to reduce risk.

If you see value in this approach and want to explore a partnership further, please email a Fortinet expert to set aside some time to talk, or visit us online at www.fortinet.com/OT.

Appendix/References

[1] https://www.tsa.gov/news/press/releases/2022/07/21/tsa-revises-and-reissues-cybersecurity-requirements-pipeline-owners

[2] https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/

[3] https://www.insurancebusinessmag.com/us/news/cyber/global-cybersecurity-spend-to-hit-23bn-in-2022--report-408361.aspx

[4] https://www.govtech.com/blogs/lohrmann-on-cybersecurity/cyber-attacks-against-critical-infrastructure-quietly-increase

[5] https://www.fortinet.com/blog/ciso-collective/new-report-underscores-why-ot-security-must-become-top-concern

[6] https://www.weforum.org/agenda/2022/05/securing-systemically-important-critical-infrastructure/

[7] https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework

[8] https://www.fortinet.com/resources-campaign/research-papers/2022-the-state-of-operational-technology-and-cybersecurity

[9] https://itchronicles.com/artificial-intelligence/the-rise-of-artificial-intelligence-in-defensive-cybersecurity/

[10] https://www.govtech.com/blogs/lohrmann-on-cybersecurity/cyber-attacks-against-critical-infrastructure-quietly-increase

FORTINET

www.fortnet.com