Originally appeared in Pipeline & Gas Journal DECEMBER 2022 issue, pg 43-45. Posted with permission.

Understanding, Implementing New TSA Pipeline Directive

By **Jim Gilsinn,** Technical Leader, **Dragos Professional Services**

The U.S. Transportation Security Administration (TSA) made a significant change to its security directive for owners and operators of hazardous liquid and natural gas pipeline and liquified natural gas facilities, with the goal "to reduce the risk that cybersecurity threats pose to critical pipeline systems."

Security Directive Pipeline-2021-02C, which supersedes and replaces Pipeline-2021-02B, went into effect just five days later, on July 27 and reflects lessons learned by the TSA after working with industry stakeholders and other federal agencies for the past year.

Directive's Timeline

Let's take a look at the history around the development and release of TSA's pipeline security directives.

May 2021: Security Directive Pipeline-2021-01 – Colonial Pipeline became the victim of a ransomware attack in their information technology (IT) environment. As a precaution, Colonial Pipeline operators temporarily halted operational technology (OT) operations. The lines of cars at gas pumps when drivers along the East Coast panicked over possible shortages triggered real shortages.

Airlines ran out of jet fuel, while companies dependent on fleets of delivery trucks and vans had to curtail their operations until the panic subsided, and fuel deliveries resumed.

In response to this event, TSA announced a series of Security Directives to enable the agency to better identify, protect against, and respond to threats to critical companies in the pipeline sector.

The first Security Directive for pipeline owners and operators, Pipeline-2021-01, was issued on May 27, 2021. These initial guidelines were seen as a good first step without being overly burdensome.

July 2021: Security Directive Pipeline-2021-02 – Just two months later, on July 20, 2021, TSA announced a second Security Directive, Pipeline-2021-02, effective July 26, 2021. Pipeline owners and operators found the second directive to be more difficult to implement as part of their cybersecurity program.

First, the document was categorized as Security Sensitive Information (SSI), which meant that pipeline owners and operators were able to obtain copies, but there were restrictions on sharing the document with contractors and vendors.

Second, the requirements within the directive were seen as overly prescriptive, and often included many aspects that could not easily be met with much of the embedded OT equipment, like multi-factor authentication (MFA).

July 2022: Security Directive Pipeline-2021-02C – Over the past year, TSA worked with pipeline owners and operators to understand how the Security Directive could be revised to better meet TSA's goal of improving the overall cybersecurity resilience of organizations, while allowing them the flexibility to meet requirements in a variety of ways.

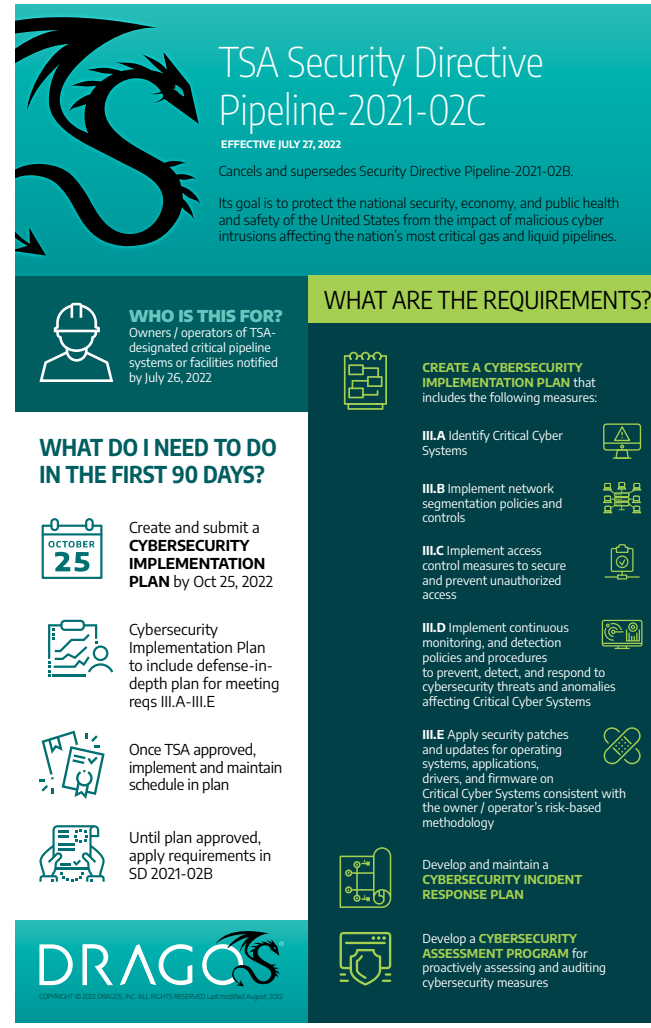

Figure 1: Implementation directive (Image: Dragos)

TSA incorporated feedback from industry groups and other federal partners, as well as input gained by evaluating pipeline owners' and operators' submissions against Pipeline-2021-02 into the new version of the directive.

Understanding the Change

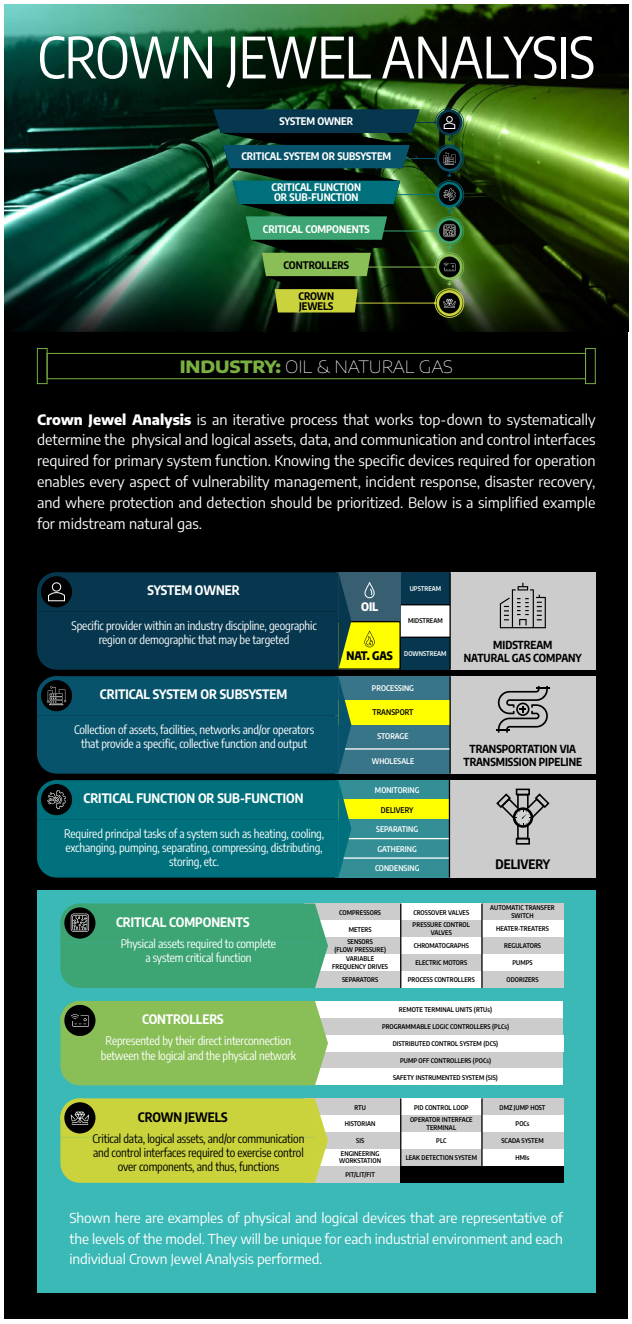

Figure 2: Crown Jewel Analysis for pipelines (Image: Dragos)

The shift from a prescriptive, compliance-based standard to a functional, performance-based standard is a major improvement in Security Directive Pipeline-2021-02C. The requirements now describe "what" should be accomplished and "why" without specifying "how" to meet the requirement.

This allows pipeline owners and operators the flexibility to determine the correct risk-based solutions to meet the cybersecurity requirements in the standard. The new focus on performance-based, rather than prescriptive, measures to achieve strategic cybersecurity outcomes and to accommodate differences in systems and operations will help support the distinct needs and challenges of the sector and of individual companies.

In addition, the TSA will partner and work with owners and operators to set dates and other decisions, making it a conversation rather than a command, and help to refine tactical execution.

Further, the focus on continuous monitoring and auditing to assess the achievement of outcomes, as well as the approval to use compensating controls, represents a major improvement for all pipeline owners and operators.

The main elements of Security Directive Pipeline-2021-02C require the development of a Cybersecurity Implementation Plan, Cybersecurity Incident Response Plan and Cybersecurity Assessment Program **(Figure 1)**.

Implementation Plan

Owners and operators must establish and implement a TSA-approved Cybersecurity Implementation Plan 90 days from the effective date of the directive.

The implementation plan describes the specific cybersecurity measures employed and the schedule for achieving the outcomes described in the directive. Until the implementation plan is approved, owners and operators must continue to implement measures from Pipeline-2021-02B.

There are five critical cybersecurity measures that owners and operators must incorporate into their Cybersecurity Implementation Plan:

- Identification of cyber critical systems
- Network segmentation
- Access control
- Continuous monitoring and detection
- Patch management

The revised directive reflects industry feedback to move away from prescriptive requirements to performance-based requirements. Owners and operators have the flexibility to leverage various industry standards (like the NIST Cybersecurity Framework (CSF), API 1164, and the ISA/IEC 62443 series) allowing them to develop actionable implementation plans around their environments utilizing a broader set of guidance, experience, and solutions.

Most important, the change provides flexibility to structure implementation plans for their OT environments given their specific risk profile.

Incident Response

Owners and operators must develop and maintain an OT-specific Cybersecurity Incident Response Plan to reduce risk of operational disruption, or the risk of other significant impacts. There are five critical cybersecurity measures that owners and operators must incorporate into their cybersecurity incident response plan:

- Contain the infected devices
- Segregate infected network systems/devices
- Maintain back up security and integrity
- Establish capability and governance for isolating IT and OT systems during incident response that could impact operations
- Perform annual tabletop exercises.

While Pipeline-2021-02C contains many of the same requirements as Pipeline-2021-02B, such as isolation, preservation, governance, testing, etc., it has subtle changes in language that allow owners and operators to develop effective incident response plans. As with all revised sections, greater flexibility is given in the approach, however, Pipeline-2021-02C specifies that "Owner/Operators must have an up-to-date Cybersecurity Incident Response Plan for the Critical Cyber System…"

A Crown Jewel Analysis (CJA), understanding the critical parts of a process, is an important part of building an effective incident response plan (Figure 2). Understanding which systems are critical and the threats to those systems before an incident occurs, can be a deciding factor in the success or failure of an owner and operator's incident response plan.

Another part of the incident response planning effort that is important is establishing a process to conduct triage and establishing severity criteria to use during an event. This helps to reduce confusion and stress that can be experienced during an incident by providing known processes for how to begin the response effort.

Cybersecurity Assessment

Owners and operators must establish a Cybersecurity Assessment Program to demonstrate how the owner/operator will proactively and regularly assess the effectiveness of cybersecurity measures that they intend to implement. Owners and operators must include an architectural design review at least once every two years. The program must include the following:

- A list of IT/OT interdependencies,
- All external connections to OT, and
- Zone boundaries (based on criticality, consequence, and necessity), to include measures to prevent unauthorized communication and encrypt across the IT/OT boundary.

The cybersecurity assessment program shows they are implementing and assessing the cybersecurity measures outlined within their cybersecurity implementation plan.

The ability for owners and operators to assess the effectiveness of controls in place will help identify potential threats and weaknesses in their networks, systems, processes, and procedures. The benefits of an assessment program include increasing awareness, mitigating future risk, and enhancing cybersecurity communication across the organization.

The assessment and auditing measures are analyzed during an architecture design review which is required to be performed, at a minimum, every two years. In Pipeline-2021-02B, these architecture reviews were identified as Validated Architecture Design Reviews (VADRs). While the name has become more generic, the elements of the program have not. VADRs continue to be performed, focusing on evaluating existing OT cybersecurity programs.

The Dragos method of conducting a VADR focuses on all the items mentioned above as well as conducting a network topology review and reviewing organization policies and procedures.

Incorporating these elements into cybersecurity awareness programs will meet the directive requirements of Pipeline-2021-02C, but more importantly, it will ensure owners and operators are implementing measures that have the most benefit on protecting their critical systems.

Conclusion

Shortly after Colonial Pipeline operations were impacted by a ransomware incident, TSA released a series of security directives developed to strengthen OT environments to greatly reduce the number of cyber-attacks that can impact critical infrastructure.

Both directives were intended to increase security throughout the OT environment via specific requirements. Asset owners and operators were required to implement and complete the provided security objectives within the required timeframes.

TSA has revised the security directives reflecting its recognition that the OT environment has some challenges implementing some of the more common IT cybersecurity controls. The revised security directives take this into account and have added flexibility with both timing and technical solutions to account for the different risk profiles for oil and gas pipeline owners and operators.

Author: Jim Gilsinn *is a Technical Leader for Professional Services at Dragos focused on ICS and OT cybersecurity. He previously worked at Kenexis Consulting and the NIST Engineering Lab. He is the past co-chair of the ISA99 committee developing the ISA/IEC 62443 series and an adjunct professor at George Mason University.*