Oil & Gas Industry Brief

U.S. TRANSPORTATION SECURITY ADMINISTRATION PIPELINE SECURITY DIRECTIVES

LESSONS LEARNED & CYBERSECURITY REQUIREMENTS FOR PIPELINE AND FACILITY OWNERS & OPERATORS

November 2022

Dragos, Inc.

info@dragos.com

@DragosInc

@Dragos, Inc.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Creation of effective regulations to reduce the cyber risk to critical pipeline infrastructure is a difficult endeavor. The scale and complexity of the business, the immense potential impact of a successful attack, the known and unknown adversaries, and techniques. Sorting through those complexities is challenging, it's a process involving the business and the government entities charged with protecting us. The good news is that there is a shared vision of an outcome – resilient, continuously operating pipelines secure from cyber disruption. The U.S. Transportation Security Administration (TSA) Security Directive Pipeline-2021-02C (Pipeline-2021-02C) is a good result of that sometimes difficult process.

Summary of Timelines

1. Create and submit draft of a Cybersecurity Implementation Plan to TSA by October 25, 2022.
2. Develop a Cybersecurity Assessment Program and submit to TSA 60 days after the Implementation Plan is approved.
3. Test Incident Response plan annually.
4. Conduct at least one Architecture Review every two years.

Summary of Requirements

- Identification of Critical Cyber Systems
- Cybersecurity Implementation Plan:
  - Network Segmentation
  - Access Control Measures
  - Continuous Monitoring
  - Patch Management Program
- Cybersecurity Assessment Program:
  - IT/OT Interdependencies
  - External Connections to OT
  - Zone Boundaries
- Incident Response Plan:
  - Responsible Roles
  - Device Containment and Segregation
  - IT/OT Systems Isolation

BACKGROUND

This brief discusses the U.S. Transportation Security Administration (TSA) security directives that established mandatory cybersecurity requirements for owners and operators of hazardous liquid and natural gas pipelines or liquified natural gas facilities deemed critical. Dragos appreciates and recognizes the continued collaboration efforts of federal partners such as TSA, the Cybersecurity and Infrastructure Security Agency (CISA), U.S. Coast Guard, and the Department of Energy on continuing to move forward the topic of cybersecurity. It is a point the industry asset owners and operators take very seriously and the TSA's attention here is undoubtedly a step towards a great partnership.

Security Directive Pipeline-2021-02C aligns with multiple standards, such as the NIST Cybersecurity Framework (CSF), API 1164, and the ISA/IEC 62443 series. By bringing the security directive in line with a variety of operational technology (OT) standards, owners and operators can pull from a broader set of guidance, experience, and solutions to meet the updated security directive requirements. This brief includes a review of the updated requirements prescribed in Pipeline-2021-02C and lessons learned and recommendations from Validated Architecture Design Reviews (VADRs) conducted by Dragos for customers in accordance with the TSA Security Directive Pipeline-2021-02B.

INTRODUCTION

The largest source of energy in the United States is petroleum, including oil and natural gas. According to the United States Energy Information Administration, oil furnishes 40 percent of our energy and natural gas furnishes 25 percent, with the remaining sources being coal, nuclear, and renewables.[1]

It would be difficult to identify products used in our daily lives that are not derived from oil. These products have a direct impact on our quality of life and are absolute necessities. One example is vehicle transportation fuels for cars, buses, trains, airplanes, etc. Another example is the chemicals made from oil that are used to make a wide range of products including, but not limited to, modern plastics, pharmaceuticals, clothing, rubbers, etc. Oil is also used as a source of energy to heat our homes and power the factories and plants that manufacture these products and/or produce the products required to make them.

Natural gas is our second-largest source of energy and supplies 25 percent of all the energy the U.S. consumes. It is another product that is relied on for numerous uses. For example, power companies use natural gas to generate electricity and other industries may use it as a source to generate heat for their processes. Additionally, liquid propane gas and compressed natural gas, which are both produced from natural gas, provide convenient fuel to locations where pipeline distribution may not be available.

1 https://www.phmsa.dot.gov/faqs/general-pipeline-faqs#QA_0

There are more than 2.6 million miles of pipelines in the U.S. that safely deliver trillions of cubic feet of natural gas and hundreds of billions of tons/miles of liquid petroleum products each year. These pipelines are operated and maintained by thousands of different-sized organizations and millions of consumers are dependent on their output. Although pipelines are indeed the safest means to move these products, they are not exempt from being identified as targets in cyberattacks, as recent events indicate.

The TSA's priorities are civil aviation security and security responsibilities over surface modes of transportation. This includes pipelines that are used for the transportation of oil and natural gas.

HOW WE GOT HERE

COLONIAL PIPELINE

On May 7th, 2021, public reporting emerged that Colonial Pipeline operations were impacted by a ransomware incident in their informational technology (IT) environment. As a precaution, Colonial Pipeline operators temporarily halted OT operations for six days. The direct impact of the shutdown was limited, but the resulting panic buying of gasoline and diesel lead to shortages at many filling stations along the Eastern Seaboard. In response to this event, the TSA announced a series of security directives that would enable the Administration to better identify, protect against, and respond to threats to critical infrastructure companies in the pipeline sector. The security directives apply to TSA-designated critical pipeline systems (about 100).

SECURITY DIRECTIVES

MAY 2021

TSA announced the first security directive for pipeline owners and operators on May 27, 2021, Pipeline-2021-01. These initial guidelines were seen as a good first step without being overly burdensome.

JULY 2021

On July 20, 2021, TSA announced a second security directive, Pipeline-2021-02 effective on 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 of the TSA-designated critical pipeline systems were able to obtain copies; however, there were restrictions regarding sharing the document with contractors, vendors, and non-TSA government entities. Second, the requirements within the directive were seen as overly prescriptive with arbitrary timelines, and often included many technical requirements that could not be easily implemented as they were developed for IT systems with no consideration taken for the complexity of OT systems. As an example, owners and operators were required to implement and complete mandatory password resets on all equipment within OT systems within 120 days of issuance of the security directive. This is an IT-centric practice that many OT assets are unable to support or can result in significant disruptions and safety issues.

JULY 2022

Over the last year, TSA worked with pipeline owners and operators to understand how they could revise the security directive to better meet the goal of improving the overall cybersecurity resilience of pipeline organizations. By aligning the directive requirements with multiple standards, such as the NIST CSF, API 1164 version 3, and the ISA/IEC 62443 series, TSA allows owners and operators the flexibility to meet requirements in a variety of ways. TSA incorporated feedback from industry groups and other federal partners, as well as input gained by evaluating pipeline owner's and operator's submissions against Pipeline-2021-02B (a slightly revised version of the original Pipeline-2021-02) into the new version of the directive known as Pipeline-2021-02C.

INITIAL CHALLENGES WITH PIPELINE-2021-02B

No regulation or security directive from the government comes without challenges. This is especially true for those that have strict due dates for compliance. When TSA released Pipeline-2021-02, they received several comments from industry related to the challenges discussed in this section. Pipeline-2021-02C is an attempt to address some of these challenges.[2]

As mentioned earlier, there are thousands of companies that operate and maintain the millions of miles of pipelines containing the products relied upon by millions. The operations of these pipelines must follow three main tenets: reliability, efficiency, and most importantly, safety. When combining both security directives and the timeline requirements, there were several items that directly conflicted with those tenets that posed risks, including: OT assets are unable to support or can result in significant disruptions and safety issues.

- Organization Scale and Availability: Pipeline and facility owner and operator organizations can range from Fortune 500 companies with thousands of employees, to smaller municipalities that only have a dozen or fewer employees. Smaller organizations may struggle to meet tight deadlines as they are resource constrained, while larger organizations may also struggle with tight deadlines due to the sheer number of devices and systems they are required to manage. Pipeline-2021-02B contained many requirements with tight deadlines which added unnecessary stress and uncertainty to teams that were likely already challenged by the constantly evolving cyber threats. Pipeline-2021-02C has since removed the prescriptive timelines for individual requirements and instead requires owners and operators to create a Cybersecurity Implementation Plan – containing how cyber measures will be achieved – to be approved by TSA.

- Operational Validation and Downtime: Pipeline systems and facilities go through rigorous in-depth testing and commissioning processes to protect the health and safety of personnel and the public, prevent damage to the environment, and ensure reliable and efficient operations of the facilities. These aspects must be considered, and potential impacts understood, when introducing changes to the systems, whether required

2 https://www.dragos.com/blog/industry-news/how-to-implement-the-revised-tsa-pipeline-security-directive/

by regulations or business processes. Organizations will often need to work with vendors, integrators, contractors, and third parties to determine how changes can be applied to reduce their impact. Furthermore, changes are often completed during either a maintenance window or when operations are shut down for safety reasons. The strict deadlines that existed in Pipeline-2021-02B presented challenges for owners and operators since maintenance windows or operation shut down timeframes only occur at predetermined times. Pipeline-2021-02C has accounted for these operationalconsiderations by allowing owners and operators to make risk-based decisions on when they can implement cybersecurity changes to their systems.

- Interconnected Systems:
  As with many OT organizations, pipeline systems and facility owners and operators have greater interconnectedness between their IT and OT systems. It is becoming increasingly difficult to completely delineate and separate operations from the business. In the Colonial Pipeline ransomware incident, Colonial made the conscious decision to halt operations out of an abundance of caution. While this might have been the safest option, it was not without significant business and national impacts. The definition of Critical Cyber System used in the directives is somewhat vague. This has led to some confusion for owners and operators on which of their systems are covered and which are not. It is understandable TSA needed to provide some flexibility for owners and operators, given the breadth of organizations that are covered by the directives. But it does mean that owners and operators should be challenged with understanding the scope of the requirements. An additional complexity is that some owners and operators may fall under multiple regulations at a single facility, such as the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) Reliability Standards. This means they may have competing and/or conflicting requirements to manage.

- Supply Chain Issues:
  Many organizations will need to implement additional technology to be identified as compliant with these security directives. Procuring additional technology in today's economic environment is considerably challenging given the supply chain issues that exist across many different industries. Additionally, procuring electronics with trusted cyber integrity adds more challenges. This can cause a delay in implementing the required technology or solution(s) by the directive deadlines, which has the potential to lead to fines. The scale of the deployments along the millions of miles of pipelines and multiple facilities can lead to difficulties in acquiring all the newer hardware necessary. These acquisition delays can extend already existing testing and commissioning delays that are part of the validation steps before deployment. There may also be maintenance blackout windows, such as the middle of winter when many homes, schools, and buildings need heat or the middle of summer when electric generation plants are needed to power air conditioning.

HIGH-LEVEL OVERVIEW OF PIPELINE-2021-02C

GOAL OF PIPELINE-2021-02C

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

CYBERSECURITY IMPLEMENTATION PLAN

Owners and operators must submit a Cybersecurity Implementation Plan 90 days from the effective date of the directive for TSA review and approval. The implementation plan should describe 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 as shown in *Appendix A*. The tables found in Appendix A provide an in-depth review of requirements along with Dragos recommendations for implementation.

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

- Identify critical cyber systems,
- Implement network segmentation controls,
- Implement access control measures,
- Implement continuous monitoring and detection,
- Apply patches and updates consistent with their risk-based methodology.

The directive revision reflects industry feedback to move away from prescriptive requirements and instead to performance-based requirements. Owners and operators have the flexibility to leverage various industry standards allowing them to develop actionable implementation plans around their unique environments utilizing a broader set of guidance, experience, and solutions. Most importantly, identifying the flexibility to structure implementation plans for their OT environments given their specific risk profiles.

The revised directive addresses key findings Dragos identified in the 2021 ICS/OT Cybersecurity Year in Review report. Throughout the numerous VADRs performed by Dragos, the most common findings identified in 2021 can be avoided if owners and operators implement the five cybersecurity measures outlined above. These measures, along with the other

requirements, align with the five critical controls for world-class OT cybersecurity established by Dragos to increase organizational resilience and reduce risks.

CYBERSECURITY INCIDENT RESPONSE PLAN

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

- Contain the infected device(s),
- 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, and
- 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., Pipeline-2021-02C 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, while, Pipeline-2021-02C specifies *"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. 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 establishing a process to conduct triage and establishing severity criteria to use during an event. This helps to reduce confusion and stress during an incident by providing known processes for how to begin the response effort.

CYBERSECURITY ASSESSMENT PROGRAM

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 between 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 VADRs. While the name has become more generic, the elements of the program have not. VADRs continue to be performed, focusing on evaluating the owner's and operator's existing OT cybersecurity program.

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 their cybersecurity assessment program will meet the directive requirements of Pipeline-2021-02C, but more importantly, it will ensure owners and operators are implementing measures that best protect their critical systems.

DOCUMENTATION TO ESTABLISH COMPLIANCE

Included in Pipeline-2021-02C is a list of documentation that owners and operators must make available to TSA upon request for inspection or copying. This list was not originally provided in Pipeline-2021-02B. Instead of asking what evidence they would need to provide to auditors, owners and operators can focus on developing and maintaining documentation that will ensure they are meeting the security directive requirements. The list, while not exhaustive, is like what would be asked of an owner or operator during a VADR, including documentation on asset inventory, network infrastructure equipment configurations, network and architecture diagrams, policies and procedures, network and device logs, and network packet captures at various important points.

LESSONS LEARNED FROM VADRS

NOTABLE OBSERVATIONS AND FINDINGS

It is evident in the VADRs completed by Dragos, that while there was a willingness and effort put forth to improve the security of their systems as well as meet the requirements of the directive, owners and operators struggled with the prescriptive controls and strict timelines. Pipeline-2021-02B required owners and operators to schedule a third-party evaluation of their OT system design and architecture. In response to this requirement, organizations tasked Dragos to complete VADRs. Throughout the VADRs, the Dragos Services team identified numerous environment misconfigurations, some of which were identified as actionable findings, while others were noted as recommendations. Unique findings were observed during each assessment, but a handful of them were observed across most of the assessments, including, but not limited to:

- **Limited Network Visibility:**
  The ability to monitor and log communication flow within the OT environment in real-time is paramount to building a secure system. Dragos identified that numerous environments assessed had limited to no network visibility over their OT network.

- **Permissive Firewall Configurations:**
  Isolating OT environments from external threats requires a defense-in-depth strategy. Network firewalls are a key element to this solution as they can be used to logically segment IT networks from the OT networks. Firewalls are only as secure as the configuration they are built with, and common misconfigurations could lead to an unwanted breach. While conducting the VADR assessments, Dragos identified multiple environments using network firewalls configured with permissive access control entries (ACEs). ACEs are designed to permit or deny traffic from one network, or security zone, to another. Having permissive ACEs allows more traffic than required to complete an action to flow across a network boundary and can be a gateway for adversaries to gain initial access, laterally move, or pivot throughout an environment. A key takeaway here is to configure each ACE with a specific source and destination, all communicating over only needed ports.

- **Account and Credentials Management:**
  Dragos identified a lack of local, domain, and service account management throughout the VADR assessments. Local administrator accounts were observed with common credentials across multiple assets. This configuration allows an adversary to laterally move to and from each asset with the common credentials. Some of the assessed environments were documented with domain account misconfigurations, including interactive service accounts, kerberoastable accounts, and a substantial number of domain administrators.

- **Default Credentials:**
  Along with overall account and credential management, default credentials were also identified by Dragos during the VADR assessments. These credentials are often predefined by a vendor and are easily identified through documentation or a quick internet search. Gaining access to an asset or application that is configured with default credentials is not a sophisticated technique. Adversaries will often take the path of least resistance and this configuration offers none.

- **Insecure Protocols Detected Within the Environment:**
  Identifying insecure protocols within an environment are key areas of focus for adversaries as they often communicate over cleartext and contain potentially sensitive information, including credentials. Common insecure protocols detected during the VADR assessments include Server Message Block (SMB) version 1, Telnet, Cisco Discovery Protocol (CDP), Hypertext Transfer Protocol (HTTP), among others. SMBv1 is a particularly vulnerable protocol with exploits that have been demonstrated in multiple high-profile cybersecurity incidents. While it may be a convenient way to share files between Windows computers, there are more secure protocols that should be used. Since Telnet is a cleartext protocol, it is also notably problematic since it was often used to manage devices remotely and the administrator credentials were passed across the network unprotected.

SELECT RECOMMENDATIONS

VISIBILITY AND MONITORING

By a large margin, the most common finding identified during the VADRs is limited or no visibility into the OT environment. This has been identified for many years in a row in the Dragos Year in Review reports as being a problem that owners and operators struggle with in their OT environments. Visibility and monitoring are also number three in the five critical controls for world-class OT cybersecurity.

Establishing visibility into the systems and networks is important to understanding what information is being collected, monitored, and retained to ensure systems are operating as expected. To address this, the directive requirements can help owners and operators improve their security posture by maintaining an up-to-date OT asset inventory, mapping vulnerabilities to those assets, and implementing a detection and monitoring solution to oversee network traffic for potential threats. In doing this, owners and operators will not only meet the requirements outlined in the directive, but they will also be able to actively detect, triage, and respond to cybersecurity threats.

Owners and operators will benefit from implementing detection and monitoring measures, as it will provide them greater visibility and understanding of network communications crossing zone boundaries, such as those between IT and OT. With modern OT networks, there are often interdependencies between IT and OT, and these need to be understood and limited where possible. These interdependencies can introduce unnecessary process risks if they are not considered.

Lastly, established continuous monitoring practices will ensure owners and operators are able to understand when new vulnerabilities are detected, identify older vulnerabilities that have not been mitigated, determine how the vendor has responded to the vulnerability by developing appropriate patches, and evaluate the potential consequences to either applying or not applying the patch. All these criteria go along with requirements in the revised directive.

INCIDENT RESPONSE PLANNING

Number one in the five critical controls for world-class OT cybersecurity recommends that owners and operators develop an OT-specific incident response plan. Unfortunately, cyber-security related incidents are becoming more, not less, frequent. Therefore, it is important to have a comprehensive, OT-specific incident response plan to ensure the effectiveness and efficiency of response activities. Consistent with the other sections of Pipeline-2021-02C, the revised directive is less prescriptive and allows organizations to create OT-specific cybersecurity incident response plans that account for the risks in their environments.

In the 2021 ICS/OT Cybersecurity Year in Review report, Dragos identified multiple findings after conducting incident response tabletop exercises (TTX) across several industry verticals. A TTX is comprised of pre-designed scenarios to identify a client's concept of operations to detect and respond to attacks. The TTX is designed to challenge and evaluate a client's existing response plans, practices, and capabilities. While multiple findings were reported, the

most significant finding was the lack of detection. Throughout the TTXs, Dragos found that organizations rely on enterprise-wide incident response plans that are built around IT environments, not OT. While an OT-specific incident response plan has many of the same actions as a plan for IT, particular care needs to be taken due to the nature of OT assets. OT involves different device types, communication protocols, and types of tactics, techniques, and procedures (TTPs) specific to industrial threats. Safety and reliability are paramount in OT, and common forensic tools and practices, such as information gathering, can cause further damage and disruption in an OT environment. For this reason, owners and operators are an integral part of incident response and building an OT-specific incident response plan.

FIVE CRITICAL CONTROLS FOR WORLD CLASS OT CYBERSECURITY

In addition to aligning with many industry standards, Security Directive Pipeline-2021-02C also aligns well with the Dragos five critical controls for world-class OT cybersecurity. Dragos analyzed years of data from services engagements to identify the key security controls that can put OT organizations, including oil and natural gas owners and operators, on a path to a more safe and reliable industrial process. Dragos recommends that organizations review these five controls, as opposed to spreading the focus across too many possibilities. As mentioned previously, there are many IT security controls that have a significantly reduced value when applied to OT or can introduce risk to the OT environment. Taking this into consideration, below is a discussion of how the five critical controls for world-class OT cybersecurity relate to Pipeline-2021-02C and how they can provide the best value in assisting owners and operators in meeting the revised directive.

1. OT INCIDENT RESPONSE PLAN (IRP)

TSA is requiring organizations to establish an up-to-date Cybersecurity IRP to reduce the risk of operational disruption or other significant impacts. This incident response plan must include aspects to:

- Segregate and/or isolate systems to respond to an incident,
- Preserve forensic evidence,
- Secure system backups,
- Conduct exercises to determine the effectiveness of the plan, and
- Identify roles and responsibilities for implementing the plan.

2. DEFENSIBLE ARCHITECTURE

Multiple aspects of Pipeline-2021-02C work together to form the basis for a defensible architecture. The first is understanding what exists in the systems as part of an asset inventory and identifying critical assets. Another major aspect to a defensible architecture is network segmentation. With modern OT networks, there are often interdependencies between IT and OT. These need to be understood and limited where possible. TSA also requires owners and operators to limit communications between zones.

3. VISIBILITY AND MONITORING

Owners and operators are required to implement continuous monitoring and detection to prevent, detect, and respond to cybersecurity threats and anomalies. These could be to detect and respond to malicious activity and software in real-time, but they can also be the logging necessary to support an incident response investigation or the detections that are necessary for the defensible architecture to respond to an incident.

4. MULTI-FACTOR AUTHENTICATION (MFA)

To utilize MFA properly, whether remotely or internally, an owner and/or operator must have previously incorporated several access control policies and procedures, including things such as credential management, least privileges, and individual accounts. Realizing that MFA is a difficult requirement to meet for many OT systems, TSA expects compensating controls and/or alternate methods to meet the requirements around access controls.

5. KEY VULNERABILITY MANAGEMENT

An important aspect of vulnerability management for OT systems is patch management. It is vital for owners and operators to understand when new vulnerabilities are detected, identify older vulnerabilities that have not been mitigated, determine how the vendor has responded to the vulnerability by developing appropriate patches, and evaluate the potential consequences of either applying or not applying the patch. Owners and operators need to make these risk-based decisions, understanding that TSA requires them to, at a minimum, acknowledge and document their approach to prioritizing different patches.

CONCLUSION

Shortly after Colonial Pipeline operations were impacted by a ransomware incident, TSA released a series of security directives developed to strengthen OT environments in an attempt to greatly reduce the number of cyberattacks that can impact critical pipeline 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 understanding that the OT environment has 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.

For more information on how Dragos can help your organization to understand and align with the latest TSA directives or to request a Dragos Validated Architecture Design Review, connect with us at sales@dragos.com, reach out to your current account executive at Dragos, or use our contact us form.

1 https://www.phmsa.dot.gov/faqs/general-pipeline-faqs#QA_0

2 https://www.dragos.com/blog/industry-news/how-to-implement-the-revised-tsa-pipeline-security-directive/

APPENDIX A: A COMPARISON OF TSA PIPELINE SECURITY DIRECTIVES 2021-02B & 2021-02C MEASURES

Pipeline-2021-02B Measures To Be Maintained Until Plan Approval

The table below compiles a list of measures contained in Pipeline-2021-02B, that have been revised for Pipeline-2021-2C, that owners and operators are still expected to follow until a new Cybersecurity Implementation Plan is approved. The table identifies the section in Pipeline-2021-02C that owners and operators can refer to as they may already be meeting the directive measures that can be included in the proposed implementation plan. In addition to the measures, Dragos has provided some comments to help owners and operators understand the changes between the versions and how they may affect their cybersecurity programs.

2021-02B SECTION	PIPELINE-2021-02B REVISIONS TO FOLLOW UNTIL IMPLEMENTATION PLAN APPROVED	2021-02C SECTION	PIPELINE-2021-02C REQUIREMENT	DRAGOS COMMENTS
II.B.1.a. II.B.1.b. II.B.1.c.	Implement and complete a mandatory password reset of all passwords within information technology systems (such as corporate remote access, and Virtual Private Networks). Implement and complete a mandatory password reset(s) of all equipment within operational technology systems, to include Programmable Logic Controllers. The Owner/Operator must continue to comply with any TSA-approved alternative measures previously approved for systems where implementing a mandatory password reset is not technically feasible. For equipment within information and operational technology systems that do not permit password resets, update or develop a plan that identifies the equipment and provides a timeline for replacing the designated equipment. This plan must be approved by TSA.	III.C.1.	Implement access control measures, including for local and remote access, to secure and prevent unauthorized access to Critical Cyber Systems. These measures must incorporate the following policies, procedures, and controls: 1. Identification and authentication policies and procedures designed to prevent unauthorized access to Critical Cyber Systems that include: a. A schedule for memorized secret authenticator resets; and b. Documented and defined mitigation measures for components of Critical Cyber Systems that will not have passwords reset in accordance with the schedule required by the preceding subparagraph (III.C. l .a.) and a timeframe to complete these mitigations.	Dragos recommends focusing on password resets for devices on the perimeter due to the basic functions of those components inside that can't be configured as securely as those on their perimeter. Develop a password reset procedure for all new devices before adding them to the operational technology (OT) system. Create a plan to reset passwords on existing devices during the next scheduled downtime, or when a device is replaced.

2021-02B SECTION	PIPELINE-2021-02B REVISIONS TO FOLLOW UNTIL IMPLEMENTATION PLAN APPROVED	2021-02C SECTION	PIPELINE-2021-02C REQUIREMENT	DRAGOS COMMENTS
II.B.1.d. II.B.1.e.	Require supervisors of individuals with elevated privilege accounts/permission to verbally confirm and document with users of all such accounts their account ownership and continued need for access to information and operational technology systems. Implement a schedule for verification of continued need at least every 90 days after the verbal confirmation required by B.1.d. and maintain documentation establishing the date of last verification.	III.C.3	Policies and procedures to manage access rights based on the principles of least privilege and separation of duties. Where not technically feasible to apply these principles, the policies and procedures must describe the compensating controls that the Owner/Operator will apply. Schedule for review of existing domain trust relationships to ensure their necessity and policies to manage domain trusts.	Slight change in verbiage – development of policies and procedures based on the principle of least privilege.
II.B.1.f.	No longer a requirement within 2021-2C		No longer a requirement within 2021-2C	
II.B.2.a.	Apply multi-factor authentication for non-service accounts accessing information and operational technology systems in a manner compliant with the most current version of NIST Special Publication 800-63B, Digital Identify Guidelines, Authentication and Lifecycle Management standards for use of multifactor cryptographic device authenticators.	III.C.2	Multi-factor authentication, or other logical and physical security controls that supplement password authentication to provide risk mitigation commensurate to multi-factor authentication. If an Owner/Operator does not apply multi-factor authentication for access to industrial control workstations in control rooms regulated under 49 CFR parts 192 or 195, the Owner/Operator shall specify what compensating controls are used to manage access.	Change in verbiage: • Still addresses multi-factor authentication or other logical and physical security controls • Removes NIST SP 800-63B reference • Must specify compensating controls if not using multi-factor authentication

2021-02B SECTION	PIPELINE-2021-02B REVISIONS TO FOLLOW UNTIL IMPLEMENTATION PLAN APPROVED	2021-02C SECTION	PIPELINE-2021-02C REQUIREMENT	DRAGOS COMMENTS
II.B.2.b.	Require supervisors of individuals with elevated privilege accounts/permission to verbally confirm and document with users of all such accounts their account ownership and continued need for access to information and operational technology systems. Implement a schedule for verification of continued need at least every 90 days after the verbal confirmation required by B.1.d. and maintain documentation establishing the date of last verification.	III.B.	Implement network segmentation policies and controls designed to prevent operational disruption to the operational technology system if the information technology system is compromised or vice versa. As applied to Critical Cyber Systems, these policies and controls must include:	
II.B.2.b.i.	Identifying information and operational technology network inter-dependencies.	III.B.1.a.	A list and description of: a. information and operational technology system interdependencies	
II.B.2.b.ii.	Implementing and maintaining capability for network physical and logical segmentation between Information and the operational technology systems sufficient to ensure the operational technology system can continue to operate even if the information technology system is taken offline because it has been compromised.	III.D.4.	Mitigation measures or manual controls to ensure industrial controlsystems can be isolated when a cybersecurity incident in the information technology system creates risk to the safety and reliability of the operational technology system.	
II.B.2.b.iii.	Defining a demilitarized zone and using firewall rules, physical separation, and other tools to eliminate unrestricted communication between the information and operational technology systems.	III.B.2.a.	An identification and description of measures for securing and defending zone boundaries, that includes security controls: a. To prevent unauthorized communications between zones; and	

2021-02B SECTION	PIPELINE-2021-02B REVISIONS TO FOLLOW UNTIL IMPLEMENTATION PLAN APPROVED	2021-02C SECTION	PIPELINE-2021-02C REQUIREMENT	DRAGOS COMMENTS
II.B.2.b.iv.	Organizing operational technology systems assets into logical zones, such as isolating unrelated sub-processes, by taking into account criticality, consequence, and operational necessity.	III.B.1.c.	Zone boundaries, including a description of how information and operational technology systems are defined and organized into logical zones based on criticality, consequence, and operational necessity.	
II.B.2.b.v.	Monitoring and filtering traffic between networks of different trust levels, such as between the information technology and the operational technology system, by defining appropriate communication conduits between the logical zones and deploying security controls to monitor and filter network traffic and communications between logical zones.	III.B.2.a.	An identification and description of measures for securing and defending zone boundaries, that includes security controls: a. To prevent unauthorized communications between zones.	
II.B.2.b.vi.	Prohibiting operational technology system protocols from traversing the information technology system unless expressly through an encrypted point-to-point tunnel.	III.B.2.b.	An identification and description of measures for securing and defending zone boundaries, that includes security controls: b. To prohibit operational technology system services from traversing the information technology system, unless the content of the operational technology system is encrypted while in transit.	Verbiage change but still requires encryption of data in transit when traversing information technology.

2021-02B SECTION	PIPELINE-2021-02B REVISIONS TO FOLLOW UNTIL IMPLEMENTATION PLAN APPROVED	2021-02C SECTION	PIPELINE-2021-02C REQUIREMENT	DRAGOS COMMENTS
II.B.2.b.vii.	Developing workarounds or manual controls to ensure industrial control system networks can be physically isolated when the information technology system creates risk to the safe and reliable operational technology system processes.	III.D.4.	Mitigation measures or manual controls to ensure industrial control systems can be isolated when a cybersecurity incident in the information technology system creates risk to the safety and reliability of the operational technology system.	
II.B.2.c.	Review and update (or develop, if necessary) log retention policies to ensure that they include policies and procedures consistent with NIST standards for- 1. Log management; ii. Secure log management infrastructure; and iii. How long log data must be maintained.	III.D.3.	Logging policies that a. Require continuous collection and analyzing of data for potential intrusions and anomalous behavior; and b. Ensure data is maintained for sufficient periods to allow for effective investigation of cybersecurity incidents	
II.B.2.d.	Employ filters sufficient to:	III.B.2.b.	Implement continuous monitoring and detection policies and procedures that are designed to prevent, detect, and respond to cybersecurity threats and anomalies affecting Critical Cyber Systems. These measures must include capabilities to:	
II.B.2.d.i.	Identify malicious email traffic, spam and phishing emails and inhibit them from reaching end users;	III.D.1.a.	Prevent malicious email, such as spam and phishing emails, from adversely impacting operations;	

2021-02B SECTION	PIPELINE-2021-02B REVISIONS TO FOLLOW UNTIL IMPLEMENTATION PLAN APPROVED	2021-02C SECTION	PIPELINE-2021-02C REQUIREMENT	DRAGOS COMMENTS
II.B.2.d.ii.	Prohibit ingress and egress of communications with known malicious Internet Protocol addresses for information technology systems and all operational technology with external connectivity.	III.D.1.b.	Prohibit ingress and egress communications with known or suspected malicious Internet Protocol addresses;	Slight verbiage change but intent is still the same.
II.B.2.d.iii. II.B.2.d.iv.	Prevent users and devices from accessing malicious websites by implementing Uniform Resource Locator block lists and/or allowlists; Control access from the operational technology system to external internet access using an allowlist; and	III.D.1.a. & III.D.2.a.	Control impact of known or suspected malicious web domains or web applications, such as by preventing users and devices from accessing malicious websites.	
II.B.2.d.v.	Investigate any communication between the operational technology system and an outside system that deviates from the identified baseline of communications and ensure it is necessary for operations.	III.D.2.b.	Document and audit any communications between the operational technology system and an external system that deviates from the Owner/Operator's identified baseline of communications.	
II.B.2.e.	Set antivirus/anti-malware programs to conduct weekly scans, with on- access and on-demand scans, of information and operational technology systems and other network assets using current signatures.	III.D.1.	Block and prevent unauthorized code, including macro scripts, from executing.	Less prescriptive requirements, removing specifics to weekly, on-access, and on-demand scans which allows more flexibility in configuration.

2021-02B SECTION	PIPELINE-2021-02B REVISIONS TO FOLLOW UNTIL IMPLEMENTATION PLAN APPROVED	2021-02C SECTION	PIPELINE-2021-02C REQUIREMENT	DRAGOS COMMENTS
II.B.2.f.	Establish passive Domain Name System capabilities that are consistent with recognized standards and, at a minimum, include the following actions:	III.D.1.c. & III.D.2.a.		Recommend owners and operators review the 2021-2C requirements as this area has changed considerably/relaxed.
II.B.2.f.i.	Implementing software analytics that allow Owner/Operators to rapidly determine which host sourced each Domain Name System- query.			
II.B.2.f.ii.	Maintaining a current list of domains that are frequently visited or searched for by legitimate users within their systems that are not already included in commercially available top one million domain lists; and			
II.B.2.f.iii.	Developing and/or updating policies and procedures requiring investigation of the reputation of the domains that are only rarely queried for and/or accessed by legitimate users within their organization, to determine if the communication with these domains carries an inappropriate level of risk to the organization.			
II.B.2.g.	Ensure, with respect to all security software updates and patches	III.E.	Reduce the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers, and firmware on Critical Cyber Systems consistent with the Owner/Operator's risk-based methodology. These measures must include:	
II.B.2.g.i.	For operating systems, applications, drivers, and firmware on information technology systems:			

2021-02B SECTION	PIPELINE-2021-02B REVISIONS TO FOLLOW UNTIL IMPLEMENTATION PLAN APPROVED	2021-02C SECTION	PIPELINE-2021-02C REQUIREMENT	DRAGOS COMMENTS
II.B.2.g.i.a.	For patches and updates that are listed on CISA's Known Exploited Vulnerabilities Catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog) and have a NIST Base Score of "Critical" (under the Common Vulnerability Scoring System) the patch/update must be installed within 15 days of its availability.	III.E.2.b.	Prioritization of all security patches and updates on CISA's Known Exploited Vulnerabilities Catalog.	As of September 2022, there are over 800 vulnerabilities on the KEVC. While owners/operators are given the flexibility to prioritize patching, this will still be a large undertaking. Owners and operators will need to determine what is impactful to their systems. Recommend reviewing vulnerabilities that impact perimeter devices.

2021-02B SECTION	PIPELINE-2021-02B REVISIONS TO FOLLOW UNTIL IMPLEMENTATION PLAN APPROVED	2021-02C SECTION	PIPELINE-2021-02C REQUIREMENT	DRAGOS COMMENTS
II.B.2.g.i.b.	If the owner/operator is unable to install the patch/update for a "Critical" vulnerability within 15 days, it must do the following:	III.E.1 - III.E.3	1. A patch management strategy that ensures all critical security patches and updates on Critical Cyber Systems are current. 2. This strategy required by paragraph III.E. l. must include: a. The risk methodology for categorizing and determining criticality of patches and updates, and an implementation timeline based on categorization and criticality; and b. Prioritization of all security patches and updates on CISA's Known Exploited Vulnerabilities Catalog. 3. If the Owner/Operator cannot apply patches and updates on specific operational technology systems without causing a severe degradation of operational capability to meet necessary capacity, the patch management strategy must include a description and timeline of additional mitigations that address the risk created by not installing the patch or update.	Recommend owners/operators review requirements as strict timelines have been removed. Dragos recommends owners and operators focus on developing a patch management strategy.
II.B.2.g.i.b.1.	Include it on a cumulative list that includes operational and other risk-based considerations to justify not meeting the 15-day deadline, and			
II.B.2.g.i.b.2.	Install the patch/update within 30 days of its listing on the Known Exploited Vulnerabilities Catalog.			
II.B.2.g.i.c. II.B.2.g.ii.	All other updates and patches must be installed within 30 days of availability. For operating systems, applications, drivers, and firmware, on Operation Technology systems, software updates and patches must be tested within 35 days of update patch availability and installed within 35 days of testing validation. Patches not installed must be included on a cumulative list that includes operational and other risk-based considerations justifying the determination not to apply the patch.			

2021-02B SECTION	PIPELINE-2021-02B REVISIONS TO FOLLOW UNTIL IMPLEMENTATION PLAN APPROVED	2021-02C SECTION	PIPELINE-2021-02C REQUIREMENT	DRAGOS COMMENTS
II.B.2.h.	Implement a “zero trust” policy that provides layers of defense to prevent unauthorized execution by taking the following actions, as applicable, to the Owner/Operator’s information and operational technology systems:			
II.B.2.h.i.	If using Microsoft Office, fully disable macro use and user- based approval across the organization for Microsoft Office products (such as Word, Excel) using Group Policy. Macros determined n ecessary for business functionality may be enabled on a case-by-case basis only after implementing additional host-based security controlsand network monitoring;	III.D.1.d.& III.D.2.c.	Block and prevent unauthorized code, including macro scripts, from executing and identify and respond to execution of unauthorized code, including macro scripts.	Recommend review of this as the requirements in 2021-2C are much less prescriptive and owners and operators may not need to implement to the level required in 2021-2B.
II.B.2.h.ii.	Apply application allowlisting to information and operational technology systems and then implement software restriction policies, or other controls providing the same security benefits, to prevent unauthorized programs from executing.	III.D.2.a.	Audit unauthorized access to internet domains and addresses.	
II.B.2.h.iii.	If not already incorporated into system-change management, update application allowlisting no less frequently than quarterly to remove applications no longer in use.			

2021-02B SECTION	PIPELINE-2021-02B REVISIONS TO FOLLOW UNTIL IMPLEMENTATION PLAN APPROVED	2021-02C SECTION	PIPELINE-2021-02C REQUIREMENT	DRAGOS COMMENTS
II.B.2.h.iv.	Monitor and/or block connections from known malicious command and control servers (such as Tor exit nodes, and other anonymization services) to Internet Protocol addresses and ports for which external connections are not expected (such as ports other than virtual private network gateways, mail ports, or web ports).	III.D.1.e.	Monitor and/or block connections from known or suspected malicious command and control servers (such as Tor exit nodes, and other anonymization services).	
II.B.2.h.v.	Implement Security, Orchestration, Automation, and Response, as applicable. If the Owner/Operator determines these capabilities are not applicable, they must document which aspects of the system do not apply the capability and their justification for excluding these operations.	III.D.2.d.	Implement capabilities (such as Security, Orchestration, Automation, and Response) to define, prioritize, and drive standardized incident response activities.	Verbiage removed allowing owners/operators to determine if capabilities are applicable and to document if they deem they are not applicable. This requirement appears more restrictive.
II.B.2.h.vi.	Require implementation of signatures to detect and/or block connection from post-exploitation tools.	III.D.1.e.	Monitor and/or block connections from known or suspected malicious command and control servers (such as Tor exit nodes, and other anonymization services).	Review as III.D.1.e does not require implementation of signatures to detect and/or block connection from post-exploitation tools.

2021-02B SECTION	PIPELINE-2021-02B REVISIONS TO FOLLOW UNTIL IMPLEMENTATION PLAN APPROVED	2021-02C SECTION	PIPELINE-2021-02C REQUIREMENT	DRAGOS COMMENTS
II.B.2.i.	Organize access rights based on the principles of least privilege and separation of duties, such as user and process accounts limited through account use policies, user account control, and privileged account management, compliant with the most current version of NIST Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations.	III.C.3.	Policies and procedures to manage access rights based on the principles of least privilege and separation of duties. Where not technically feasible to apply these principles, the policies and procedures must describe the compensating controls that the Owner/Operator will apply.	
II.B.2.j.	For any group accounts, establish a written process to review operational need for the account, document justification, maintain a list, ensure memorized secret authenticators are compliant with NIST SP 800-63B, maintain list of personnel who have or had access to group accounts, and dates of last password resets. Within no more than 7 days after a user of a group account leaves the Owner/Operator's employment, the Owner/Operator must rotate memorized secret authenticators for the group account.	III.C.4	Enforcement of standards that limit availability and use of shared accounts to those that are critical for operations, and then only if absolutely necessary. When the Owner/Operator uses shared accounts for operational purposes, the policies and procedures must ensure: a. Access to shared accounts is limited through account management that uses principles of least privilege and separation of duties; and b. Individuals who no longer need access do not have knowledge of the password necessary to access the shared account.	Review as timeline requirements have been removed along with verbiage changes.

2021-02B SECTION	PIPELINE-2021-02B REVISIONS TO FOLLOW UNTIL IMPLEMENTATION PLAN APPROVED	2021-02C SECTION	PIPELINE-2021-02C REQUIREMENT	DRAGOS COMMENTS
II.B.3.	Owner/Operators shall remove all trust relationships, such as identity stores between the information and operational technology systems. Separate and dedicated identity providers shall be implemented for the information and operational technology systems, if they do not already exist.	III.C.5	Schedule for review of existing domain trust relationships to ensure their necessity and policies to manage domain trusts.	
II.B.4.	N/A in 2021-2C		N/A in 2021-2C	
II.C.1.	Owner/Operators must have an up-to-date Cybersecurity Incident Response Plan for the Critical Cyber System that includes measures to reduce the risk of operational disruption, or the risk of other significant impacts on necessary capacity, should their pipeline or facility experience a cybersecurity incident.	III.F.1.	Owner/Operators must have an up-to-date Cybersecurity Incident Response Plan for the Critical Cyber System that includes measures to reduce the risk of operational disruption, or the risk of other significant impacts on necessary capacity, should their pipeline or facility experience a cybersecurity incident. The Cybersecurity Incident Response Plan must provide specific measures sufficient to ensure the following objectives, as applicable.	

Pipeline-2021-02B Measures Updated in Pipeline-20221-02C

The table below compiles a list of measures contained in Pipeline-2021-02B. While not part of the revised requirements for Pipeline-2021-2C that owners and operators are still expected to follow until a new Cybersecurity Implementation Plan is approved, they are still required as part of Pipeline-2021-2C. The table identifies the section in Pipeline-2021-02C that owners and operators can refer to as they may already be meeting the directive measures and can be included in the proposed implementation plan. In addition to the measures, Dragos has provided some comments to help owners and operators understand the changes between the versions and how they may affect their cybersecurity programs.

PIPELINE-2021-02B SECTION	PIPELINE-2021-02B REQUIREMENT	PIPELINE-2021-02C SECTION	PIPELINE-2021-02C REQUIREMENT	DRAGOS COMMENTS
II.C.1.a.	Prompt isolation of the infected system by:	III.F.1.a.	Prompt containment of the infected server or device.	
II.C.1.a.i.	Removing the infected system from all networks, and disabling the system's wireless, Bluetooth, and any other potential networking capabilities.	N/A in 2021-2C	Requirement not included in Pipeline-2021-2C.	Removal of verbiage around disabling the system's wireless, Bluetooth, and any other potential networking capabilities.
II.C.1.a.ii.	Segregation of the infected computer from other computers and devices.	III.F.1.b.	Segregation of the infected network (or devices) to ensure malicious code does not spread by, as necessary.	
II.C.1.b.	Removing the infected system from all networks, and disabling the system's wireless, Bluetooth, and any other potential networking capabilities.	N/A in 2021-2C	Requirement not included in Pipeline-2021-2C.	Removal of verbiage around disabling the system's wireless, Bluetooth, and any other potential networking capabilities.
II.C.1.b.i.	Segregating (removing from the network) the infected computer(s).	III.F.1.b.i.	Segregating (removing from the network) the infected device(s).	
II.C.1.b.ii.	Segregating any other computers or devices that shared a network with the infected computer(s).	III.F.1.b.ii.	Segregating any other devices that shared a network with the infected device(s).	

PIPELINE-2021-02B SECTION	PIPELINE-2021-02B REQUIREMENT	PIPELINE-2021-02C SECTION	PIPELINE-2021-02C REQUIREMENT	DRAGOS COMMENTS
II.C.1.b.iii.	Preserving volatile memory by collecting forensic memory image of affected device(s) before powering off or moving.	III.F.1.b.iii.	Preserving volatile memory by collecting a forensic memory image of affected device(s) before powering off or moving.	
II.C.1.b.iv.	Isolating and securing all infected and potentially infected computers and devices, making sure to clearly label any equipment that has been encrypted by malware.	III.F.1.b.iv.	Isolating and securing all infected and potentially infected devices, making sure to clearly label any equipment that has been affected by malicious code.	Verbiage changed slightly to address any system *affected* by malicious code, not just systems that were *encrypted* by malicious code.
II.C.1.c.	Security and integrity of backed-up data, including measures to secure backups, store backup data offline, and procedures requiring scanning of stored backup data with an antivirus program to check that it is free of known malware when the backup is made and when tested for restoral.	III.F.1.c.	Security and integrity of backed-up data, including measures to secure backups, store backup data separate from the system, and procedures to ensure that the backup data is free of known malicious code when the backup is made and when tested for restoral.	
II.C.1.d.	Established capability and governance for isolating the information technology and operational technology systems in the event of a cybersecurity incident that arises to the level of potential operational disruption while maintaining operational standards and limits.	III.F.1.d.	Established capability and governance for isolating the information and operational technology systems in the event of a cybersecurity incident that results or could result in operational disruption.	
II.C.1.e.	Situational exercises to test the effectiveness of procedures, and personnel responsible for implementing measures, in the Cybersecurity Contingency/Response Plan, no less than annually.	III.F.1.e.	Exercises to test the effectiveness of procedures, and personnel responsible for implementing measures, in this Cybersecurity Incident Response Plan, no less than annually.	Still an annual requirement.

PIPELINE-2021-02B SECTION	PIPELINE-2021-02B REQUIREMENT	PIPELINE-2021-02C SECTION	PIPELINE-2021-02C REQUIREMENT	DRAGOS COMMENTS
II.C.2.	The Cybersecurity Contingency/Response Plan must, at a minimum, identify who (by position) is responsible for implementing the specific measures and any necessary resources needed to implement these measures.	III.F.2.	The Cybersecurity Incident Response Plan must identify who (by position) is responsible for implementing the specific measures in the Incident Response Plan and any necessary resources needed to implement the measures.	
II.C.3.	Within 7 days of completing the requirements in this section, Owner/ Operators must ensure that their Cybersecurity Coordinator or other accountable executive submits a statement to TSA at SurfOps-SD@tsa.dhs.gov certifying the Owner/Operator has met the requirement. Documentation of compliance must be provided to TSA upon request.	N/A in 2021-2C	Requirement not included in Pipeline-2021-2C	

PIPELINE-2021-02B SECTION	PIPELINE-2021-02B REQUIREMENT	PIPELINE-2021-02C SECTION	PIPELINE-2021-02C REQUIREMENT	DRAGOS COMMENTS
II.D.1.	Owner/Operators must schedule a third-party evaluation of the Owner/Operator's operational technology system design and architecture, to be conducted within 12 months from the effective date of this security directive, which includes verification and validation of network traffic and system log review and analysis to identify cybersecurity vulnerabilities related to network design, configuration, and inter-connectivity to internal and external systems. This evaluation must:	III.G. – III.G.2.c.	Develop a Cybersecurity Assessment Program for proactively assessing and auditing cybersecurity measures. 1. The Owner/Operator must develop a Cybersecurity Assessment Program for proactively assessing Critical Cyber Systems to ascertain the effectiveness of cybersecurity measures and to identify and resolve device, network, and/or system vulnerabilities. 2. The Cybersecurity Assessment Program required by Section III.G.1. must a. Assess the effectiveness of the Owner/Operator's TSA-approved Cybersecurity Implementation Plan; b. Include an architectural design review at least once every two years that includes verification and validation of network traffic and system log review and analysis to identify cybersecurity vulnerabilities related to network design, configuration, and inter-connectivity to internal and external systems; and c. Incorporate other assessment capabilities, such as penetration testing of information technology systems and the use of "red" and "purple" team (adversarial perspective) testing.	Suggest owners and operators review Cybersecurity Assessment Program requirements within 2021-2C as the requirement has changed significantly. Pipeline-2021-2B was written specifically around the requirement to conduct architecture design reviews. Pipeline-2021-2C requires a more in-depth assessment program to assess and audit all measures that are required in implementation plans. The requirements include architecture design reviews but go beyond that to include additional requirements. • No longer requires an independent third party to perform a design review • Architecture review must occur every two years • Requires a penetration test (red team / blue team) which is a new requirement
II.D.1.a	Be conducted by an independent third-party, unless otherwise approved by TSA, that has demonstrated capability to perform the cybersecurity architecture design review required by this security directive.			
II.D.1.b	Be completed annually thereafter for the duration of this security directive, as revised and renewed.			
II.D.1.c	Include a written report detailing the results of the evaluation and the acceptance or rejection of any recommendations provided by the evaluator to address vulnerabilities. This written report must be made available to TSA upon request and retained for no less than two (2) years from the date of completion.			

PIPELINE-2021-02B SECTION	PIPELINE-2021-02B REQUIREMENT	PIPELINE-2021-02C SECTION	PIPELINE-2021-02C REQUIREMENT	DRAGOS COMMENTS
II.D.2.	A Validated Architecture Design Review (VADR) conducted by the Department of Homeland Security (DHS) satisfies this requirement. If not a VADR conducted by DHS, the evaluation required by paragraph II.D.1. must be completed using a standard that, at a minimum, evaluates the extent to which the Owner/Operator's system architecture and design is compliant with the most current version of NIST Special Publication 800.82, Guide to Industrial Control Systems (ICS) Security.	N/A in 2021-2C	Requirement not included in Pipeline-2021-2C	
II.D.3.	The deadline for the testing required by paragraphs II.D.1. does not apply to Owner/Operators who have had a DHS-conducted VADR between July 26, 2020, and July 26, 2021. The anniversary date for annual testing required by this section is one year from the date of the DHS VADR report.	N/A in 2021-2C	Requirement not included in Pipeline-2021-2C	
II.D.4.	Within 7 days of completing the requirements in this section, Owner/Operators must ensure that their Cybersecurity Coordinator or other accountable executive submits a statement to TSA at SurfOps-SD@tsa.dhs.gov certifying that the Owner/Operator has met the requirement. Documentation of compliance must be provided to TSA upon request.	III.G.3.	No later than 60 days after TSA's approval of the Owner/Operator's Cybersecurity Implementation Plan, the Owner/Operator must submit the annual plan for their Cybersecurity Assessment Program to SurfOps-SD@tsa.dhs.gov. This plan must describe the Cybersecurity Assessment Program required by Section III.G.1., including the schedule for specific actions. The Owner/Operator must update thisplan on an annual basis and submit it no later than one year from the date of the previous plan's submission.	

DRAGOS

DRAGOS
SAFEGUARDING CIVILIZATION

OT security platform provides visibility into assets, network, vulnerabilities, and threats

Largest, most experienced team of industrial cybersecurity specialists

500+ employees, 300+ global customers, HQ in Hanover, MD, USA

TO LEARN MORE ABOUT DRAGOS AND OUR TECHNOLOGY, SERVICES, AND THREAT INTELLIGENCE FOR THE INDUSTRIAL COMMUNITY, PLEASE VISIT WWW.DRAGOS.COM.

CONTACT US

Dragos has a global mission: to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. The practitioners who founded Dragos were drawn to this mission through decades of government and private sector experience.

Dragos codifies the knowledge of our cybersecurity experts into an integrated software platform that provides customers critical visibility into ICS and OT networks so that threats and vulnerabilities are identified and can be addressed before they become significant events. Our solutions protect organizations across a range of industries, including power and water utilities, energy, and manufacturing, and are optimized for emerging applications like the Industrial Internet of Things (IIoT).

Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

THANK YOU