Fact Sheet on DHS Actions to Secure the U.S. Pipeline Sector

Under the leadership of Secretary Mayorkas, the Transportation Security Administration (TSA) at the U.S. Department of Homeland Security (DHS), with support from the Department's Cybersecurity and Infrastructure Security Agency (CISA), has taken decisive action to strengthen the cybersecurity and resilience of the U.S. pipeline sector.

The disruptive ransomware attack on Colonial Pipeline in May 2021 revealed a continuing significant national security risk with critical vulnerabilities in the pipeline sector that previous voluntary efforts did not sufficiently mitigate. Following the incident, TSA issued two Security Directives mandating that pipeline owners and operators implement several critically important and urgently needed cybersecurity measures.

TSA developed these Directives in close consultation with federal partners, including CISA, the Pipeline Hazardous Materials and Safety Administration (PHMSA), and the Department of Energy (DOE). TSA is working closely with the pipeline industry to ensure the successful implementation of the measures required by the Directives. As a result of these actions, our nation's oil and gas supply is significantly more resilient in today's evolving threat landscape.

Overview of Threat Landscape

- The 2019 Annual Threat Assessment from the Office of the Director of National Intelligence (ODNI) found that "China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the United States."
- The May 2021 ransomware attack that hit Colonial Pipeline paralyzed the business networks of the company and resulted in gas shortages, partly as a result of panic buying. The incident highlighted the national security risk posed by malicious cyber actors and demonstrated to the American public that an incident in cyberspace can have real world consequences and disrupt their daily lives.
- In July 2021, CISA and the FBI released Alert AA21-201A: Chinese Gas Pipeline Intrusion Campaign, 2011-2013, highlighting a spear-phishing and intrusion campaign conducted by state-sponsored Chinese actors that targeted U.S. oil and natural gas pipeline companies.
- In a March 2022 statement, President Biden emphasized that the Russian Government is exploring options for potential cyberattacks on critical infrastructure in the United States.

TSA Security Directives for the Pipeline Sector

- In 2021, TSA issued two critically important Security Directives intended to strengthen the cybersecurity and resilience of the pipeline sector.
- In May 2021, TSA issued the first Security Directive. This Directive requires owners and operators of critical pipelines to (i) report confirmed and potential cybersecurity incidents to CISA; (ii) designate a Cybersecurity Coordinator to be available 24 hours a day, seven days a week; (iii) review current cybersecurity practices; and (iv) identify any gaps and related remediation measures to address cyber-related risk and report the results to TSA and CISA within 30 days.
- In July 2021, TSA issued the second Security Directive. This Directive requires owners and operators of critical pipelines to (i) implement a series of mitigation measures to

reduce vulnerabilities and increase the resilience of both information technology (IT) and operational technology (OT) systems; (ii) develop and implement Contingency/Recovery plans; and (iii) test the effectiveness of cybersecurity practices annually through a cybersecurity architecture design review conducted by a third party.

- TSA developed these Security Directives in close collaboration with technical experts – including industrial control systems experts – from CISA. The Security Directives build on the voluntary Pipeline Cybersecurity Initiative, which was launched by TSA and CISA in 2018, and were informed by the associated Validated Architecture Design Review (VADR) assessments conducted on over 60 pipeline companies. The Directives also integrated the lessons learned from the Colonial Pipeline ransomware attack.

Alternative Measures Requests

- As part of its standard practice for Security Directives, TSA allows pipeline owners and operators to seek alternative measures if they believe that they may have an alternate methodology or process for achieving the requirements of the Directives.
- Alternative measures are granted if TSA determines that an alternative measure proposal is both in the public interest and in the interest of safety (i.e., resulting in equivalent or better security outcomes than required in the Directive).
- Following the issuance of the second Security Directive, TSA received an unprecedented number – more than 380 –of alternative measure requests. TSA carefully evaluates each alternative measure request and works collaboratively with industry partners. For example, 41 requests were addressed and closed by revising the Security Directive to extend the cycle time for certain actions from 7 days to 15 days.

Risk of Operational Disruption or Safety Risk

- Due to the complexities of the nation's pipeline sector, the TSA Security Directives were purposefully designed to allow for flexibility.
- In addition to allowing the implementation of alternative measures, these Security Directives enable owners and operators to alert TSA if requirements may jeopardize safe operations or cause operational disruption. When notified, TSA will evaluate the claim, coordinate with PHMSA, and, if appropriate, create a plan with the operator to address the issue.
- To date, TSA has not received any notification that an operational disruption has occurred as a result of a specific requirement. In addition, TSA has received fewer than 10 notifications indicating concern about a potential future disruption.
- When an owner or operator raises a potential concern, TSA works directly with the operator to evaluate and address the claims of the pipeline operator. None of these claims have been determined by PHMSA to present risk of an operational disruption.

TSA Staffing

- TSA currently has more than twenty specialists who focus on pipeline cybersecurity and operations with 13 new positions funded in the FY 2022 budget adopted in March 2022.
- Recognizing the need for expedited processing of these alternative measures requests, TSA established a surge team of cyber experts, policy writers, and attorneys dedicated to reviewing and processing the requests for alternative measures.