Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

Pipeline Cybersecurity—Updated Directives

September 7, 2022

The May 2021 ransomware attack against the Colonial Pipeline caused widespread repercussions, including regional gasoline shortages and significant lines at the pump. This was not the first domestic cyberattack to disrupt physical infrastructure, but it was one of the most consequential. Before the attack, the federal government did not regulate the cybersecurity of natural gas and hazardous liquids pipelines. Following the incident, the Transportation Security Agency (TSA)—as the sector risk management agency for pipelines—issued two Security Directives imposing mandatory requirements on pipeline companies' cybersecurity practices. A year later, the TSA revised and updated the directives. This Insight reviews these actions and discusses issues for Congress.

TSA's Regulatory Authority

Pipelines are part of the surface transportation critical infrastructure sector. TSA, within the Department of Homeland Security (DHS), administers the federal program for pipeline security. The Aviation and Transportation Security Act of 2001 (P.L. 107-71), which established TSA, authorizes the agency "to issue, rescind, and revise such regulations as are necessary" to carry out its functions (§101). The Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) directs TSA to promulgate pipeline security regulations and carry out necessary inspection and enforcement if the agency determines that regulations are appropriate (§1557(d)). Prior to the Colonial Pipeline attack, TSA relied upon industry's voluntary compliance with the agency's guidelines for pipeline physical security and cybersecurity. The agency's reliance on voluntary, rather than mandatory, compliance with recommended security standards had long been questioned by industry stakeholders.

TSA's 2021 Cybersecurity Directives

On May 27, 2021, TSA announced its first Security Directive applicable to owners and operators of critical pipeline facilities (as identified by TSA). The directive required that companies designate and use a Cybersecurity Coordinator and report any cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency (CISA). The directive also required pipeline companies to conduct a cybersecurity vulnerability assessment (to determine whether their practices and systems aligned with

Congressional Research Service
https://crsreports.congress.gov
IN12006

TSA's guidelines), identify gaps, identify gap remediation measures, and establish an implementation timeline to address those gaps.

On July 20, 2021, TSA announced its second Security Directive, requiring critical pipeline companies "to implement specific mitigation measures to protect against ransomware attacks and other known threats to information technology and operational technology systems, develop and implement a cybersecurity contingency and recovery plan, and conduct a cybersecurity architecture design review." TSA's announcement did not provide specific details on those security measures because they were considered Sensitive Security Information (SSI). The TSA Administrator testified that pipeline operators could seek approval for alternatives to any specific measures, providing flexibility to achieve intended security outcomes. The Security Directives were to be effective for one year from the date of issuance, with the possibility of extension. (For more background, see CRS Report R46903, *Pipeline Cybersecurity: Federal Programs*.)

Although pipeline operators worked to comply with the directives, from the outset, major pipeline trade associations expressed concern that operators had not been adequately consulted and that the measures were too prescriptive, failing to account for the uniqueness of each company's systems, which could potentially create operational problems. Some in Congress echoed these concerns. TSA subsequently reported that, after issuing its second directive, the agency "received an unprecedented number—more than 380—of alternative measure requests," but had received no notifications of operational disruption due to a directive requirement.

2022 Cybersecurity Directives

On May 29, 2022, TSA revised its first Security Directive, extending the incident reporting deadline to 24 hours and narrowing the definition of *cybersecurity incident*, while leaving the other requirements little changed.

On July 21, 2022, TSA announced the revision and reissuance of its second security directive, with more significant changes, taking "an innovative, performance-based approach ... allowing industry to leverage new technologies and be more adaptive to changing environments." The revised directive requires that pipeline operators take certain actions to achieve a defined set of cybersecurity outcomes. The actions include:

- submitting a Cybersecurity Implementation Plan,
- implementing operational technology (OT) and information technology (IT) network segmentation policies and controls,
- implementing controls to prevent unauthorized access to critical systems,
- implementing continuous cybersecurity monitoring and detection programs,
- patching and updating systems promptly,
- developing and maintaining a Cybersecurity Incident Response Plan, and
- developing a program for proactively assessing and auditing cybersecurity measures.

The revised directive is no longer considered SSI, although cybersecurity information submitted to TSA by operators remains confidential. As with the 2021 directives, the revised directives are effective for one year, with the possibility of extension.

Issues for Congress

Issues may arise regarding harmonization between TSA's requirements for cyber incident and ransomware reporting and future reporting regulations to be promulgated by CISA as required by the Cyber Incident Reporting for Critical Infrastructure Act of 2022, enacted as part of the Consolidated Appropriations Act, 2022 (P.L. 117-103). Some in industry also have been critical of TSA issuing Security Directives under emergency authority rather than promulgating cybersecurity regulations through a traditional rulemaking process with more opportunity for industry input. Some industry analysts have questioned whether TSA has sufficient staff with enough cybersecurity and regulatory expertise to effectively administer its pipeline cybersecurity program. The quality, quantity, and timeliness of cybersecurity risk information originating with the government and being shared with the private sector also continues to be an area of focus. Congress also may choose to consider how TSA's ongoing pipeline cybersecurity oversight will fit together with the nation's overall strategy to protect critical infrastructure from cybersecurity threats.

Author Information

Chris Jaikaran
Specialist in Cybersecurity Policy

Paul W. Parfomak
Specialist in Energy Policy

Disclaimer