GAO@100 Highlights

Highlights of GAO-21-105263, a testimony before the Committee on Commerce, Science, and Transportation, U.S. Senate

July 27, 2021

CRITICAL INFRASTRUCTURE PROTECTION

TSA Is Taking Steps to Address Some Pipeline Security Program Weaknesses

Why GAO Did This Study

The nation's pipelines are vulnerable to cyber-based attacks due to increased reliance on computerized systems. In May 2021 malicious cyber actors deployed ransomware against Colonial Pipeline's business systems. The company subsequently disconnected certain systems that monitor and control physical pipeline functions so that they would not be compromised.

This statement discusses TSA's actions to address previous GAO findings related to weaknesses in its pipeline security program and TSA's guidance to pipeline owner/operators. It is based on prior GAO products issued in December 2018, June 2019, and March 2021, along with updates on actions TSA has taken to address GAO's recommendations as of June 2021. To conduct the prior work, GAO analyzed TSA documents; interviewed TSA officials, industry association representatives, and a sample of pipeline operators selected based on type of commodity transported and other factors; and observed TSA security reviews. GAO also reviewed TSA's May and July 2021 Pipeline Security Directives, TSA's Pipeline Security Guidelines, and three federal security alerts issued in July 2020, May 2021, and June 2021.

What GAO Recommends

In the prior reports, GAO made 15 recommendations to address pipeline security weaknesses, including clarifying its security guidelines and updating response protocols. TSA has addressed 12, and reported plans to address those remaining.

View GAO-21-105263. For more information, contact Leslie V. Gordon at (202) 512-8777 or GordonLV@gao.gov

What GAO Found

Protecting the nation's pipeline systems from security threats is a responsibility shared by both the Transportation Security Administration (TSA) and private industry stakeholders. Prior to issuing a cybersecurity directive in May 2021, TSA's efforts included issuing voluntary security guidelines and security reviews of privately owned and operated pipelines. GAO reports in 2018 and 2019 identified some weaknesses in the agency's oversight and guidance, and made 15 recommendations to address these weaknesses. TSA concurred with GAO's recommendations and has addressed most of them, such as clarifying portions of its Pipeline Security Guidelines improving its monitoring of security review performance, and assessing staffing needs.

As of June 2021, TSA had not fully addressed two pipeline cybersecurity-related weaknesses that GAO previously identified. These weaknesses correspond to three of the 15 recommendations from GAO's 2018 and 2019 reports.

- **Incomplete information for pipeline risk assessments**. GAO identified factors that likely limit the usefulness of TSA's risk assessment methodology for prioritizing pipeline security reviews. For example, TSA's risk assessment did not include information consistent with critical infrastructure risk mitigation, such as information on natural hazards and cybersecurity risks. GAO recommended that TSA develop data sources relevant to pipeline threats, vulnerabilities, and consequences of disruptions. As of June 2021, TSA had not fully addressed this recommendation.
- **Aged protocols for responding to pipeline security incidents**. GAO reported in June 2019 that TSA had not revised its 2010 Pipeline Security and Incident Recovery Protocol Plan to reflect changes in pipeline security threats, including those related to cybersecurity. GAO recommended that TSA periodically review, and update its 2010 plan. TSA has begun taking action in response to this recommendation, but has not fully addressed it, as of June 2021.

TSA's May 2021 cybersecurity directive requires that certain pipeline owner/operators assess whether their current operations are consistent with TSA's Guidelines on cybersecurity, identify any gaps and remediation measures, and report the results to TSA and others. TSA's July 2021 cybersecurity directive mandates that certain pipeline owner/operators implement cybersecurity mitigation measures; develop a Cybersecurity Contingency Response Plan in the event of an incident; and undergo an annual cybersecurity architecture design review, among other things. These recent security directives are important requirements for pipeline owner/operators because TSA's Guidelines do not include key mitigation strategies for owner/operators to reference when reviewing their cyber assets. TSA officials told GAO that a timely update to address current cyber threats is appropriate and that they anticipate updating the Guidelines over the next year.