GAO Highlights

Highlights of GAO-19-48, a report to congressional requesters

December 2018

CRITICAL INFRASTRUCTURE PROTECTION

Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management

Why GAO Did This Study

More than 2.7 million miles of pipeline transport and distribute oil, natural gas, and other hazardous products throughout the United States. Interstate pipelines run through remote areas and highly populated urban areas, and are vulnerable to accidents, operating errors, and malicious physical and cyber-based attack or intrusion. The energy sector accounted for 35 percent of the 796 critical infrastructure cyber incidents reported to DHS from 2013 to 2015. Several federal and private entities have roles in pipeline security. TSA is primarily responsible for the oversight of pipeline physical security and cybersecurity.

GAO was asked to review TSA's efforts to assess and enhance pipeline security and cybersecurity. This report examines, among other objectives: (1) the guidance pipeline operators reported using to address security risks and the extent that TSA ensures its guidelines reflect the current threat environment; (2) the extent that TSA has assessed pipeline systems' security risks; and (3) the extent TSA has assessed its effectiveness in reducing pipeline security risks.

GAO analyzed TSA documents, such as its *Pipeline Security Guidelines*; evaluated TSA pipeline risk assessment efforts; and interviewed TSA officials, 10 U.S. pipeline operators—selected based on volume, geography, and material transported—and representatives from five industry associations.

What GAO Recommends

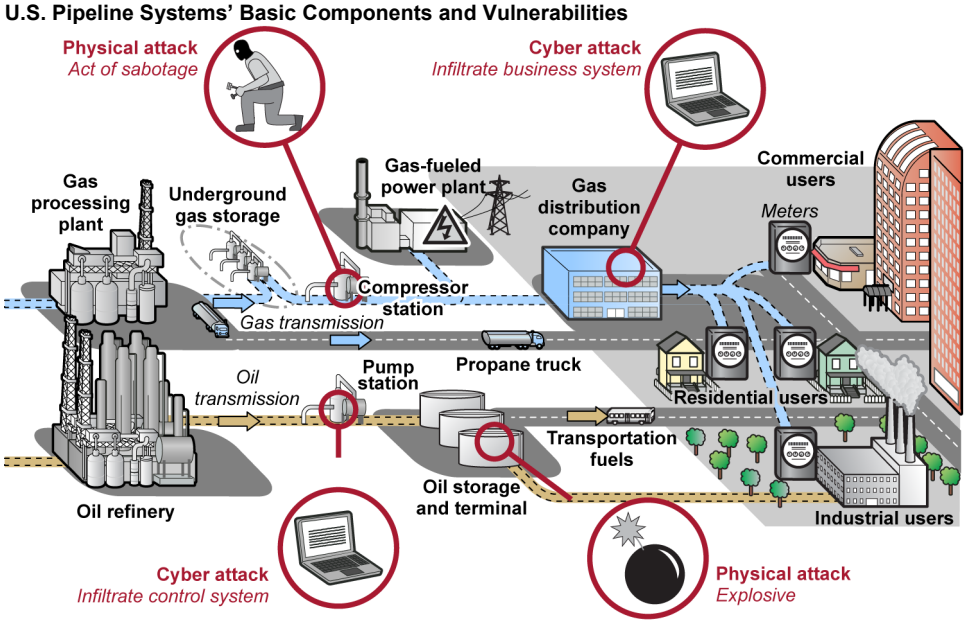
GAO makes 10 recommendations to TSA to improve its pipeline security program management (many are listed on the next page), and DHS concurred.

View GAO-19-48. For more information, contact Chris Currie at (404) 679-1875 or curriec@gao.gov and Nick Marinos at (202) 512-9342 or marinosn@gao.gov.

What GAO Found

Pipeline operators reported using a range of guidelines and standards to address physical and cybersecurity risks, including the Department of Homeland Security's (DHS) Transportation Security Administration's (TSA) *Pipeline Security Guidelines*, initially issued in 2011. TSA issued revised guidelines in March 2018 to reflect changes in the threat environment and incorporate most of the principles and practices from the National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity*. However, TSA's revisions do not include all elements of the current framework and TSA does not have a documented process for reviewing and revising its guidelines on a regular basis. Without such a documented process, TSA cannot ensure that its guidelines reflect the latest known standards and best practices for physical security and cybersecurity, or address the dynamic security threat environment that pipelines face. Further, GAO found that the guidelines lack clear definitions to ensure that pipeline operators identify their critical facilities. GAO's analysis showed that operators of at least 34 of the nation's top 100 critical pipeline systems (determined by volume of product transported) deemed highest risk had identified no critical facilities. This may be due, in part, to the guidelines not clearly defining the criteria to determine facilities' criticality.

U.S. Pipeline Systems' Basic Components and Vulnerabilities



Source: GAO analysis of Transportation Security Administration information. | GAO-19-48

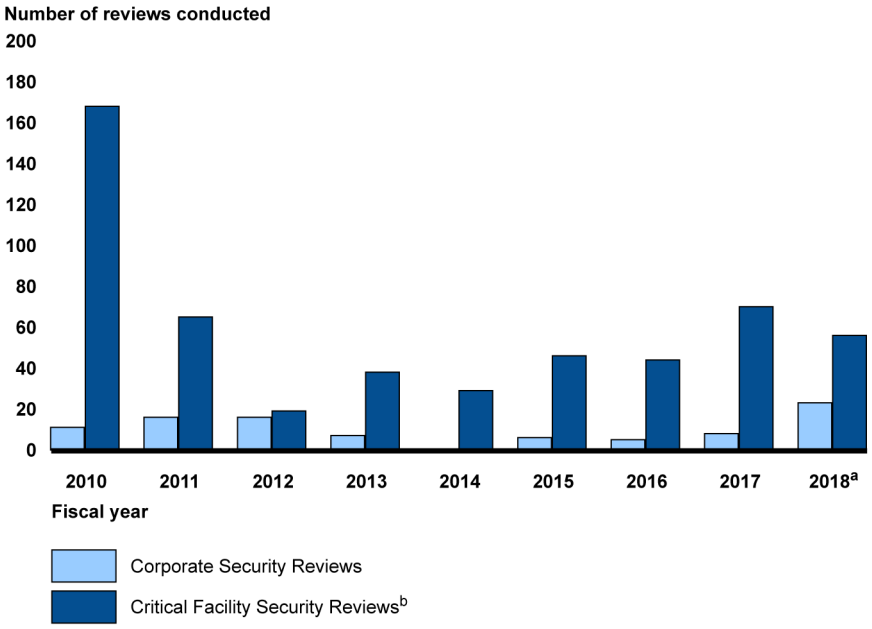
To assess pipeline security risks, TSA conducts pipeline security reviews—Corporate Security Reviews and Critical Facility Security Reviews—to assess pipeline systems' vulnerabilities. However, GAO found that the number of TSA security reviews has varied considerably over the last several years, as shown in the table on the following page.

What GAO Recommends

GAO recommends, among other things, that the TSA Administrator take the following actions:

- implement a documented process for reviewing, and if deemed necessary, for revising TSA's *Pipeline Security Guidelines* at defined intervals;
- clarify TSA's *Pipeline Security Guidelines* by defining key terms within its criteria for determining critical facilities;
- develop a strategic workforce plan for TSA's Security Policy and Industry Engagement's Surface Division;
- update TSA's pipeline risk assessment methodology to include current data to ensure it reflects industry conditions and threats;
- fully document the data sources, underlying assumptions and judgments that form the basis of TSA's pipeline risk assessment methodology;
- take steps to coordinate an independent, external peer review of TSA's pipeline risk assessment methodology;
- ensure the Security Policy and Industry Engagement's Surface Division has a suite of performance measures which exhibit key attributes of successful performance measures; and
- enter information on Corporate Security Review recommendations and monitor and record their status.

Pipeline Security Reviews Conducted, Fiscal Year 2010 through July 2018



Source: GAO analysis of Transportation Security Administration-reported figures. | GAO-19-48

[a]Fiscal year 2018 data are through July 31, 2018.
[b]Fiscal years 2010 and 2011 represent Critical Facility Inspections—the predecessor of the Critical Facility Security Review.

TSA officials stated that staffing limitations have prevented TSA from conducting more reviews. Staffing levels for TSA's Pipeline Security Branch have varied significantly since fiscal year 2010 with the number of staff ranging from 14 full-time equivalents in fiscal years 2012 and 2013 to 1 in 2014. Further, TSA does not have a strategic workforce plan to help ensure it identifies the skills and competencies—such as the required level of cybersecurity expertise—necessary to carry out its pipeline security responsibilities. By establishing a strategic workforce plan, TSA can help ensure that it has identified the necessary skills, competencies, and staffing.

GAO also identified factors that likely limit the usefulness of TSA's risk assessment methodology for prioritizing pipeline system reviews. Specifically, TSA has not updated its risk assessment methodology since 2014 to reflect current threats to the pipeline industry. Further, its sources of data and underlying assumptions and judgments regarding certain threat and vulnerability inputs are not fully documented. In addition, the risk assessment has not been peer reviewed since its inception in 2007. Taking steps to strengthen its risk assessment, and initiating an independent, external peer review would provide greater assurance that TSA ranks relative risk among pipeline systems using comprehensive and accurate data and methods.

TSA has established performance measures to monitor pipeline security review recommendations, analyze their results, and assess effectiveness in reducing risks. However, these measures do not possess key attributes—such as clarity, and having measurable targets—that GAO has found are key to successful performance measures. By taking steps to ensure that its pipeline security program performance measures exhibit these key attributes, TSA could better assess its effectiveness at reducing pipeline systems' security risks. Pipeline Security Branch officials also reported conducting security reviews as the primary means for assessing the effectiveness of TSA's efforts to reduce pipeline security risks. However, TSA has not tracked the status of Corporate Security Review recommendations for the past 5 years. Until TSA monitors and records the status of these reviews' recommendations, it will be hindered in its efforts to determine whether its recommendations are leading to significant reduction in risk.