CRITICAL INFRASTRUCTURE PROTECTION

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

What GAO Found

The Department of Homeland Security’s (DHS) Transportation Security Administration (TSA) has developed and provided pipeline operators with voluntary security guidelines, and also evaluates the vulnerability of pipeline systems through security assessments. However, GAO's prior work, reported in December 2018, identified some weaknesses and made recommendations to strengthen TSA’s management of key aspects of its pipeline security program.

Pipeline security guidelines. GAO reported that TSA revised its voluntary pipeline security 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 (NIST) Framework for Improving Critical Infrastructure Cybersecurity. However, TSA’s revisions do not include all elements of the current NIST framework and TSA does not have a documented process for reviewing and revising its guidelines on a regular basis. GAO recommended that TSA implement a documented process for reviewing and revising TSA’s Pipeline Security Guidelines at defined intervals. TSA has since outlined procedures for reviewing its guidelines, which GAO is reviewing to determine if they sufficiently address the recommendation.

Workforce planning. GAO reported that the number of TSA security reviews of pipeline systems has varied considerably over time. TSA officials stated that staffing limitations within its Pipeline Security Branch have prevented TSA from conducting more reviews. Staffing levels for the branch have varied significantly, ranging from 1 full-time equivalent in 2014 to 6 from fiscal years 2015 through 2018. 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. GAO recommended that TSA develop a strategic workforce plan, which TSA plans to complete by July 2019.

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 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. GAO recommended that TSA update its risk ranking tool to include up-to-date data to ensure it reflects industry conditions and fully document the data sources, assumptions and judgments that form the basis of the tool. As of April 2019, TSA reported taking steps to address these recommendations. GAO is reviewing documentation of these steps to determine if they sufficiently address the recommendations.

Monitoring performance. GAO reported that conducting security reviews was the primary means for TSA to assess the effectiveness of its efforts to reduce pipeline security risks. However, TSA has not tracked the status of key security review recommendations for the past 5 years. GAO recommended that TSA take steps to update information on security review recommendations and monitor and record their status, which TSA plans to address by November 2019.

What GAO Recommends

GAO made 10 recommendations in its December 2018 report to strengthen TSA’s management of its pipeline security program. DHS agreed and has described planned actions or timeframes for addressing these recommendations.

View GAO-19-542T. For more information, contact William Russell at (202) 512-8777 or russellw@gao.gov.