crowell moring

CLIENT ALERT

GAO Recommends Enhancements to TSA's Cyber and Physical Security Programs

Jan.03.2019

Just as 2018 came to a close, the U.S. Government Accountability Office (GAO) released a report making recommendations to the Transportation Security Administration (TSA) intended to help TSA bolster its pipeline physical and cyber security program management. *See* GAO, "Critical Infrastructure Protection, Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management" (December 2018). GAO reports that its recommendations are based on its analysis of TSA's Pipeline Security Guidelines; evaluation of TSA pipeline risk assessment efforts; and interviews with TSA officials, selected U.S. pipeline operators, and representatives from five industry associations.

In response to the release of the GAO report, Maria Cantwell (D. Wash.), Ranking Member of the Senate Committee on Energy and Natural Resources, and Frank Pallone, Jr. (D. N.J.), Ranking Member of House Committee on Energy and Commerce, requested that the Department of Homeland Security (DHS) assess current cyber and physical security protections for U.S. natural gas, oil, and other hazardous liquid pipelines and associated infrastructure. The lawmakers also requested that DHS provide, by the end of 2019, a "specific plan of action as to how DHS will address GAO's concerns." TSA is a component of DHS and the lead security agency regulating interstate natural gas pipelines.

Among its recommendations, GAO states that TSA should further enhance its Pipeline Security Guidelines. Beginning in 2011, TSA, working cooperatively with all significant stakeholders, developed voluntary Guidelines covering onshore natural gas and hazardous liquid transmission pipelines and liquefied natural gas operators. Recognizing that physical and cyber threats evolve, the program was designed to encourage flexibility. Rather than mandating adherence to strict controls, the Guidelines identify baseline and enhanced security measures and controls which operators may use based on the characteristics of their particular facility and the assigned threat level. The most recent version of the Guidelines, published in 2018, focuses on operational technology (OT) systems and applies the suggested measures based on whether an OT system is classified as a critical or non-critical pipeline cyber asset. The 2018 Guidelines also include new incident response protocols and recommend that owners and operators consider adopting the risk-based approach included in the National Institute of Standards and Technology "Framework for Improving Critical Infrastructure Cybersecurity." TSA suggests in the 2018 Guidelines that, in addition to the NIST framework, owners and operators also consider guidance issued by other federal agencies (DHS, Department of Energy and Department of Commerce) as well as other industry standards in planning and implementing a cybersecurity program that allows them to respond to evolving threats.

TSA has conducted hundreds of security reviews over the past decade, including the pipeline systems it identified as at highest risk. TSA also conducted industry-wide meetings to communicate lessons learned and share smart practices garnered from the reviews. Recognizing that the number of reviews is impacted by staffing limitations at TSA, GAO recommends that TSA develop 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. In addition, finding data reliability issues in the information TSA has collected, GAO recommends that TSA better track the implementation of its security recommendations, including enhancing the database it currently uses to monitor and record the status of compliance by pipeline owners and operators.

We will continue to monitor developments in this area of increasing importance to the critical infrastructure, transportation and energy sectors.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Paul M. Rosen
Partner – Los Angeles, Washington, D.C.
Phone: +1 213.443.5577, +1 202.624.2500
Email: prosen@crowell.com

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1 202.624.2615
Email: ewolff@crowell.com

Maida Oringher Lerner
Senior Counsel – Washington, D.C.
Phone: +1 202.624.2596
Email: mlerner@crowell.com

Matthew B. Welling
Counsel – Washington, D.C.
Phone: +1 202.624.2588
Email: mwelling@crowell.com