Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

Pipeline Security: Homeland Security Issues in the 116th Congress

March 1, 2019

Ongoing threats against the nation's natural gas, oil, and refined product pipelines have heightened concerns about the security risks to these pipelines, their linkage to the electric power sector, and federal programs to protect them. In a December 2018 study, the Government Accountability Office (GAO) stated that, since the terrorist attacks of September 11, 2001, "new threats to the nation's pipeline systems have evolved to include sabotage by environmental activists and cyber attack or intrusion by nations." In a 2018 *Federal Register* notice, the Transportation Security Administration stated that it expects pipeline companies will report approximately 32 "security incidents" annually—both physical and cyber. The Pipeline and LNG Facility Cybersecurity Preparedness Act (H.R. 370, S. 300) would require the Secretary of Energy to enhance coordination among government agencies and the energy sector in pipeline security; coordinate incident response and recovery; support the development of pipeline cybersecurity applications, technologies, demonstration projects, and training curricula; and provide technical tools for pipeline security.

Pipeline Physical Security

Congress and federal agencies have raised concerns since at least 2010 about the physical security of energy pipelines, especially cross-border oil pipelines. These security concerns were heightened in 2016 after environmentalists in the United States disrupted five pipelines transporting oil from Canada. In 2018, the Transportation Security Administration's Surface Security Plan identified improvised explosive devices as key risks to energy pipelines, which "are vulnerable to terrorist attacks largely due to their stationary nature, the volatility of transported products, and [their] dispersed nature." Among these risks, according to some analysts, are the possibility of multiple, coordinated attacks with explosives on the natural gas pipeline system, which potentially could "create unprecedented challenges for restoring gas flows."

Congressional Research Service
https://crsreports.congress.gov
IN11060

Pipeline Cybersecurity

As with any internet-enabled technology, the computer systems used to operate much of the pipeline system are vulnerable to outside manipulation. An attacker can exploit a pipeline control system in a number of ways to disrupt or damage pipelines. Such cybersecurity risks came to the fore in 2012 after reports of a series of cyber intrusions among U.S. natural gas pipeline operators. In April 2018, new cyberattacks reportedly caused the shutdown of the customer communications systems (separate from operation systems) at four of the nation's largest natural gas pipeline companies. Most recently, in January 2019, congressional testimony by the Director of National Intelligence singled out gas pipelines as critical infrastructure vulnerable to cyberattacks which could cause disruption "for days to weeks."

Pipeline and Electric Power Interdependency

Pipeline cybersecurity concerns are exacerbated by growing interdependency between the pipeline and electric power sectors. A 2017 Department of Energy (DOE) staff report highlighted the electric power sector's growing reliance upon natural gas-fired generation and, as a result, security vulnerabilities associated with pipeline gas supplies. These concerns were echoed in a June 2018 op-ed by two commissioners on the Federal Energy Regulatory Commission (FERC) who wrote, "as … natural gas has become a major part of the fuel mix, the cybersecurity threats to that supply have taken on new urgency." A November 2018 report by the PJM regional transmission organization concluded that "while there is no imminent threat," the security of generation fuel supplies, especially natural gas and fuel oil, "has become an increasing area of focus." In a February 2019 congressional hearing on electric grid security, the head of the North American Electric Reliability Corporation (NERC) testified that pipeline and electric grid interdependency "is fundamental" to security.

The Federal Pipeline Security Program

The Transportation Security Administration (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, authorized 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)). However, to date, TSA has not issued such regulations, relying instead upon industry compliance with voluntary guidelines for pipeline physical and cybersecurity. The pipeline industry maintains that regulations are unnecessary because pipeline operators have voluntarily implemented effective physical and cybersecurity programs. The 2018 GAO study identified a number of weaknesses in the TSA program, including inadequate staffing, outdated risk assessments, and uncertainty about the content and effectiveness of its security standards.

In fulfilling its responsibilities, TSA cooperates with the Department of Transportation's (DOT) Pipeline and Hazardous Materials Safety Administration (PHMSA)—the federal regulator of pipeline safety—under the terms of a 2004 memorandum of understanding (MOU) and a 2006 annex to facilitate transportation security collaboration. TSA also cooperates with DOE's recently established Office of Cybersecurity, Energy Security, and Emergency Response (CESER), whose mission includes "emergency preparedness and coordinated response to disruptions to the energy sector, including physical and cyber-attacks." TSA also collaborates with the Office of Energy Infrastructure Security at the Federal Energy Regulatory Commission—the agency which regulates the reliability and security of the bulk power electric grid.

Issues for Congress

Over the last few years, most debate about the federal pipeline security program has revolved around four principal issues. Some in Congress have suggested that TSA's current pipeline security authority and voluntary standards approach may be appropriate, but that the agency may require greater resources to more effectively carry out its mission. Others stakeholders have debated whether security standards in the pipeline sector should be mandatory—as they are in the electric power sector—especially given their growing interdependency. Still others have questioned whether any of TSA's regulatory authority over pipeline security should move to another agency, such as the DOE, DOT, or FERC, which they believe could be better positioned to execute it. Concern about the quality, specificity, and sharing of information about pipeline threats also has been an issue.

Author Information

Paul W. Parfomak
Specialist in Energy and Infrastructure Policy

Disclaimer