Congressional Research Service
Informing the legislative debate since 1914

TESTIMONY

Statement of

Paul W. Parfomak
Specialist in Energy and Infrastructure Policy

Before

Committee on Homeland Security
Subcommittee on Transportation Security
U.S. House of Representatives

Hearing on

"Pipelines: Securing the Veins of the American Economy"

April 19, 2016

Congressional Research Service
7-5700
www.crs.gov
<Product Code>

CRS TESTIMONY
Prepared for Congress

Good morning Chairman Katko, Ranking Member Rice, and members of the subcommittee. My name is Paul Parfomak, Specialist in Energy and Infrastructure Policy at the Congressional Research Service (CRS). CRS appreciates the opportunity to testify here today about the evolution of and current federal role in pipeline security. Please note that, in accordance with our enabling statutes, CRS does not advocate policy or take a position on any related legislation.

Introduction

Nearly three million miles of pipeline transporting natural gas, oil, and other hazardous liquids crisscross the United States. While an efficient and comparatively safe means of transport, these pipelines carry materials with the potential to cause public injury, destruction of property, and environmental damage. The nation's pipeline network is also widespread, running alternately through remote and densely populated regions. Pipelines are operated by increasingly sophisticated computer systems which manage their product flows and provide continuous information on their status. Due to their scale, physical exposure, and reliance on computer controls, pipelines are vulnerable to accidents, operating errors, and malicious attacks.

Congress has had long-standing concern about the security of the nation's pipeline network. Beginning with the Aviation and Transportation Security Act of 2001 (P.L. 107-71), which established the Transportation Security Administration, and continuing through the PIPES Act of 2006 (P.L. 109-468) and the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53), Congress has enacted specific statutory provisions to help secure pipelines. Likewise, successive presidential administrations have promulgated executive orders establishing a federal framework for the security of pipelines, among other critical infrastructure. The 114th Congress is overseeing the implementation of the federal pipeline security program and considering new legislation related to the nation's pipeline systems. In particular, the SAFE PIPES Act (S. 2776), which reauthorizes the federal pipeline *safety* program, would also mandate a report to Congress on the staffing, resource allocation, oversight strategy, and management of the federal pipeline security program (§20).

Physical Threats to Pipeline Security

Pipelines are vulnerable to intentional attacks using firearms, explosives, or other physical means. Oil and gas pipelines, globally, have been a favored target of terrorists, militant groups, and organized crime. For example, in 1996, London police foiled a plot by the Irish Republican Army to bomb gas pipelines and other utilities across the city.[1] In Colombia, rebels have bombed the Caño Limón oil pipeline and other pipelines hundreds of times since 1993, most recently last March.[2] Likewise, militants in Nigeria have repeatedly attacked oil pipelines, including coordinated bombings of three pipelines in 2007 and the sophisticated bombing of an underwater pipeline in 2016.[3] A rebel group detonated bombs along Mexican oil and natural gas pipelines in July and September 2007.[4] Natural gas pipelines in British Columbia, Canada, were bombed six times between October 2008 and July 2009 by unknown perpetrators in acts

[1] President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures*, Washington, DC, October 1997.

[2] Luis Jaime Acosta, "Colombia's Caño Limón Pipeline Suspended After Rebel Attacks," *Reuters*, March 14, 2016; Government Accountability Office (GAO), *Security Assistance: Efforts to Secure Colombia's Caño Limón-Coveñas Oil Pipeline Have Reduced Attacks, but Challenges Remain*, GAO-05-971, September 2005.

[3] Maggie Fick and Anjil Raval, "Bombed Pipeline to Hit Nigeria Oil Output," *Financial Times*, March 8, 2016; Katherine Houreld, "Militants Say 3 Nigeria Pipelines Bombed," *Associated Press*, May 8, 2007.

[4] Reed Johnson, "Six Pipelines Blown Up in Mexico," *Los Angeles Times*, September 11, 2007. p. A-3.

classified by authorities as environmentally motivated "domestic terrorism."[5] In 2009, the *Washington Post* reported that over $1 billion of crude oil had been stolen directly from Mexican pipelines by organized criminals and drug cartels.[6]

Pipelines in the United States have also been targeted by terrorists and other malicious individuals. In 1999, Vancouver police arrested a man planning to bomb the Trans Alaska Pipeline System (TAPS) for personal profit in oil futures.[7] In 2005 a U.S. citizen sought to conspire with Al Qaeda to attack TAPS and a major natural gas pipeline in the eastern United States.[8] In 2006 federal authorities acknowledged the discovery of a detailed posting on a website purportedly linked to Al Qaeda that reportedly encouraged attacks on U.S. pipelines, especially TAPS, using weapons or hidden explosives.[9] In 2007, the U.S. Department of Justice arrested members of a terrorist group planning to attack jet fuel pipelines and storage tanks at the John F. Kennedy International Airport.[10] In 2011, a man planted a bomb, which did not detonate, along a natural gas pipeline in Oklahoma.[11] In 2012, a man who reportedly had been corresponding with "Unabomber" Ted Kaczynski unsuccessfully bombed a natural gas pipeline in Plano, Texas.[12] To date, there have been no successful bombings of U.S. pipelines, but the threat of physical attacks remains credible.

Cyber Threats to Pipelines

Although physical attacks on pipelines have been a focus in North America and elsewhere, the sophisticated computer systems used to operate pipeline systems are also vulnerable to cyber attacks. Cyber infiltration of supervisory control and data acquisition (SCADA) systems could allow "hackers" to disrupt pipeline service and cause spills, explosions, or fires—all from remote locations via the Internet or other communication pathways. Such an approach reportedly was used to cause the 2008 explosion of the Baku-Tbilisi-Ceyhan oil pipeline in Turkey.[13]

In March 2012, the Industrial Control Systems Cyber Emergency Response Team housed within the Department of Homeland Security identified an ongoing series of cyber intrusions among U.S. natural gas pipeline operators dating back to December 2011. According to the agency, various pipeline companies described targeted spear-phishing[14] attempts and intrusions into multiple natural gas pipeline sector

[5] Ben Gelinas, "New Letter Threatens Resumption of 'Action' against B.C. Pipelines," *Calgary Herald*, April 15, 2010.

[6] Steve Fainaru and William Booth, "Mexico's Drug Cartels Siphon Liquid Gold," *Washington Post*, December 13, 2009.

[7] David S. Cloud, "A Former Green Beret's Plot to Make Millions Through Terrorism," *Ottawa Citizen*, December 24, 1999, p. E15.

[8] U.S. Attorney's Office, Middle District of Pennsylvania, "Man Convicted of Attempting to Provide Material Support to Al-Qaeda Sentenced to 30 Years' Imprisonment," Press release, November 6, 2007; A. Lubrano and J. Shiffman, "Pa. Man Accused of Terrorist Plot," *Philadelphia Inquirer*, February 12, 2006, p. A1.

[9] Wesley Loy, "Web Post Urges Jihadists to Attack Alaska Pipeline," *Anchorage Daily News*, January 19, 2006.

[10] U.S. Department of Justice, "Four Individuals Charged in Plot to Bomb John F. Kennedy International Airport," press release, June 2, 2007.

[11] U.S. Attorney's Office, "Konawa Man Sentenced for Attempting to Destroy or Damage Property Using an Explosive," press release, December 5, 2012.

[12] Valerie Wigglesworth, "Plano Blast Suspect Corresponded with Unabomber," *Dallas Morning News*, June 29, 2014; U.S. Attorney's Office, "Plano Man Guilty in Pipeline Bombing Incident," press release, June 3, 2013.

[13] Jordan Robertson and Michael Riley, "Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar," *Bloomberg*, December 10, 2014

[14] "Spear-phishing" involves sending official-looking e-mails to specific individuals to insert harmful software programs (malware) into protected computer systems; to gain unauthorized access to proprietary business information; or to access confidential data such as passwords, social security numbers, and private account numbers.

organizations "positively identified … as related to a single campaign."[15] In 2011, computer security company McAfee reported similar "coordinated covert and targeted" cyber attacks originating primarily in China against global energy companies. The attacks began in 2009 and involved spear-phishing, exploitation of Microsoft software vulnerabilities, and the use of remote administration tools to collect sensitive competitive information about oil and gas fields.[16] In 2010, the Stuxnet computer worm was first identified as a threat to industrial control systems. Although the Stuxnet software initially spreads indiscriminately, the software includes a highly specialized industrial process component targeting specific industrial SCADA systems built by the Siemens company.[17] The increased vulnerability of pipeline SCADA systems due to their modernization, taken together with the emergence of SCADA-specific malicious software and the recent cyber attacks, suggests that cybersecurity threats to pipelines have been increasing.

Potential Consequences of Pipeline Releases

Although there have been no intentional releases from U.S. pipelines due to bombing or cyber attacks, accidental releases may illustrate the potential consequences of a successful attack. Pipeline accidents in the United States, on the whole, cause few fatalities compared to other product transportation modes, but such accidents have been catastrophic in several cases. For example, a 1999 gasoline pipeline accident in Bellingham, WA, killed three people and caused $45 million in damage to a city water plant and other property.[18] In 2000, a natural gas pipeline accident near Carlsbad, NM, killed 12 campers.[19] A 2010 natural gas pipeline explosion in San Bruno, CA, killed 8 people, injured 60 others, and destroyed 37 homes.[20] A 2010 pipeline spill released 819,000 gallons of crude oil into a tributary of the Kalamazoo River near Marshall, MI.[21] A 2014 natural gas distribution pipeline explosion in New York City killed eight people, injured 50 others, destroyed two five-story buildings, and caused the temporary closure of a transit line due to debris.[22] Such accidents demonstrate the potential risk to human life, property, and the environment. Disruption of service from these pipelines also caused economic and operational impacts among the pipelines' customers. Such accidents have generated substantial scrutiny of pipeline regulation and increased state and community activity related to pipeline safety and security.[23]

---

[15] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), "Gas Pipeline Cyber Intrusion Campaign," *ICS-CERT Monthly Monitor*, April 2012, p.1, http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Apr2012.pdf.

[16] McAfee Foundstone Professional Services and McAfee Labs, *Global Energy Cyberattacks: "Night Dragon,"* white paper, February 10, 2011, p. 3, http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf.

[17] Tobias Walk, "Cyber-attack Protection for Pipeline SCADA Systems," *Pipelines International Digest*, January 2012, p. 7.

[18] National Transportation Safety Board, *Pipeline Rupture and Subsequent Fire in Bellingham, Washington June 10, 1999*, NTSB/PAR-02/02, October 8, 2002.

[19] National Transportation Safety Board, *Natural Gas Pipeline Rupture and Fire Near Carlsbad, New Mexico August 19, 2000*, NTSB/PAR-03-01, February 11, 2003.

[20] National Transportation Safety Board, *Pacific Gas and Electric Company Natural Gas Transmission Pipeline Rupture and Fire, San Bruno, California*, September 9, 2010, NTSB/PAR-11/01, August 30, 2011.

[21] National Transportation Safety Board, *Enbridge, Inc. Hazardous Liquid Pipeline Rupture*, Board meeting summary, July 25, 2010, http://www.ntsb.gov/news/events/2012/marshall_mi/index.html.

[22] National Transportation Safety Board, *Natural Gas-Fueled Building Explosion and Resulting Fire New York City, New York March 12, 2014*, NTSB/PAR-15/01, June 9, 2015.

[23] See, for example: Jim Lynch and Jonathan Oosting, "Opposition Grows to Straits of Mackinac Oil Lines," *Detroit News*, April 13, 2016; Bellingham Herald Editorial Board, "Citizens Need Panel To Monitor Pipeline Safety," *Bellingham Herald* (WA), Januray 24, 2010; Janet Zink, "Fueling the Resistance," *St. Petersburg Times*, December 16, 2007; J. Nesmith and R. K. M. Haurwitz, "Pipelines: The Invisible Danger," *Austin American-Statesman*, July 22, 2001.

The Federal Role in Pipeline Security

Federal pipeline security efforts originated in the pipeline safety program. The Natural Gas Pipeline Safety Act of 1968 (P.L. 90-481) and the Hazardous Liquid Pipeline Act of 1979 (P.L. 96-129) are two of the principal early acts establishing the federal role in pipeline safety. Under both statutes, the Transportation Secretary is given primary authority to regulate key aspects of interstate pipeline safety: design, construction, operation and maintenance, and spill response planning. At the end of FY2015, the Department of Transportation (DOT) employed 234 pipeline safety staff in its Pipeline and Hazardous Materials Safety Administration (PHMSA).[24] In addition to its own staff, PHMSA's enabling legislation allows the agency to delegate authority to *intra*state pipeline safety offices, and allows state offices to act as "agents" administering *inter*state pipeline safety programs (excluding enforcement) for those sections of *inter*state pipelines within their boundaries.[25] There were approximately 330 full-time equivalent state pipeline safety inspectors in 2015.[26]

Presidential Decision Directive 63, issued by the Clinton administration in 1998, assigned to the DOT lead responsibility for pipeline *security* as well as safety.[27] Under this authority, after the terrorist attacks of September 11, 2001, the DOT conducted a vulnerability assessment to identify critical pipeline facilities and worked with industry groups and state pipeline safety organizations to assess the industry's readiness to prepare for, withstand, and respond to a terrorist attack.[28] Together with the Department of Energy and state pipeline agencies, the DOT promoted the development of consensus standards for security measures[29] tiered to correspond with the five levels of threat warnings issued by the Office of Homeland Security.[30] The DOT also developed protocols for inspections of critical facilities to ensure that operators implemented appropriate security practices. To convey emergency information and warnings, the DOT established a variety of communication links to key staff at the most critical pipeline facilities throughout the country. The DOT also began identifying near-term technology to enhance deterrence, detection, response, and recovery, and began seeking to advance public and private sector planning for response and recovery.[31]

In September 2002, the DOT circulated formal guidance developed in cooperation with the pipeline industry associations defining the agency's security program recommendations and implementation expectations. This guidance recommended that operators identify critical facilities, develop security plans consistent with prior trade association security guidance, implement these plans, and review them annually.[32] While the guidance was voluntary, the DOT expected compliance and informed operators of

[24] Artealia Gilliard, PHMSA, personal communication, September 18, 2015. Employees as of September 18, 2015.

[25] 49 U.S.C. 60107.

[26] Artealia Gilliard, September 9, 2015.

[27] Presidential Decision Directive 63, *Protecting the Nation's Critical Infrastructures*, May 22, 1998.

[28] Research and Special Programs Administration (RSPA), *RSPA Pipeline Security Preparedness*, December 2001.

[29] See: American Petroleum Institute and National Petrochemical and Refiners Association, *Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries*, March 2002; Interstate Natural Gas Association of America (INGAA) and American Gas Association (AGA), *Security Guidelines for the Natural Gas Industry*, September 2002.

[30] Ellen Engleman, Administrator, Research and Special Programs Administration (RSPA), statement before the Subcommittee on Energy and Air Quality, House Energy and Commerce Committee, March 19, 2002.

[31] Ellen Engleman, Administrator, Research and Special Programs Administration (RSPA), statement before the Subcommittee on Highways and Transit, House Transportation and Infrastructure Committee, February 13, 2002.

[32] James K. O'Steen, Research and Special Programs Administration (RSPA), *Implementation of RSPA Security Guidance*, presentation to the National Association of Regulatory Utility Commissioners, February 25, 2003.

its intent to begin reviewing security programs within 12 months, potentially as part of more comprehensive safety inspections.[33]

Transferring Pipeline Security to TSA

In November 2001, President Bush signed the Aviation and Transportation Security Act (P.L. 107-71) establishing the Transportation Security Administration (TSA) within the DOT. According to TSA, the act placed the DOT's pipeline security authority (under PDD-63) within TSA. The act specified for TSA a range of duties and powers related to general transportation security, such as intelligence management, threat assessment, mitigation, and security measure oversight and enforcement, among others. On November 25, 2002, President Bush signed the Homeland Security Act of 2002 (P.L. 107-296) creating the Department of Homeland Security (DHS). Among other provisions, the act transferred to DHS the Transportation Security Administration from the DOT (§403). On December 17, 2003, President Bush issued Homeland Security Presidential Directive 7 (HSPD-7), clarifying executive agency responsibilities for identifying, prioritizing, and protecting critical infrastructure.[34] HSPD-7 maintains DHS as the lead agency for pipeline security (par. 15), and instructs the DOT to "collaborate in regulating the transportation of hazardous materials by all modes (including pipelines)" (par. 22h). The order requires that DHS and other federal agencies collaborate with "appropriate private sector entities" in sharing information and protecting critical infrastructure (par. 25). TSA joined both the Energy Government Coordinating Council and the Transportation Government Coordinating Council under provisions in HSPD-7. The missions of the councils are to work with their industry counterparts to coordinate critical infrastructure protection programs in the energy and transportation sectors, respectively, and to facilitate the sharing of security information.

HSPD-7 also required DHS to develop a national plan for critical infrastructure and key resources protection (par. 27), which the agency issued in 2006 as the *National Infrastructure Protection Plan* (NIPP). The NIPP, in turn, required each critical infrastructure sector to develop a Sector Specific Plan (SSP) that describes strategies to protect its critical infrastructure, outlines a coordinated approach to strengthen its security efforts, and determines appropriate funding for these activities. Executive Order 13416 further required the transportation sector SSP to prepare annexes for each mode of surface transportation.[35] In accordance with the above requirements the TSA issued its *Transportation Systems Sector Specific Plan* and *Pipeline Modal Annex* in 2007 with an update on 2010.

TSA's Pipeline Security Activities

Although the TSA has regulatory authority for pipeline security under P.L. 107-71 and P.L. 110-53, its activities to date have relied upon voluntary industry compliance with the agency's security guidance and best practice recommendations.[36] TSA has administered a multifaceted program to facilitate these efforts. In 2003, TSA initiated its ongoing Corporate Security Review (CSR) program, wherein the agency visits the largest pipeline and natural gas distribution operators to review their security plans and inspect their facilities. During the reviews, TSA evaluates whether each company is following the intent of the DOT's voluntary security guidance, as updated by TSA, and seeks to maintain the list of assets each company has identified meeting the criteria established for critical facilities. In 2008, the TSA initiated its Critical

[33] James K. O'Steen, Office of Pipeline Safety (OPS), personal communication, June 10, 2003.

[34] HSPD-7 supersedes PDD-63 (par. 37).

[35] Executive Order 13416, "Strengthening Surface Transportation Security," December 5, 2006.

[36] Transportation Security Administration, *Pipeline Security Guidelines*, April 2011, and *Pipeline Security Smart Practice Observations*, September 19, 2011.

Facility Inspection Program (CFI), under which the agency conducted in-depth inspections of all the critical facilities of the 125 largest pipeline systems in the United States. The agency estimated that these 125 pipeline systems collectively included approximately 600 distinct critical facilities.[37] TSA concluded the initial round of CFI inspections in 2011, having completed a total of 347 site visits throughout the United States.[38]

Over the last decade, TSA has engaged in a number of additional pipeline security initiatives, including:

- Developing a statistical tool used for relative risk ranking and prioritization,
- Completing a security incident and recovery protocol plan mandated under P.L. 110-53,
- Initiating a program to address risks from pipeline transportation of hazardous materials other than oil and natural gas,
- Assessing U.S. and Canadian security and planning for critical cross-border pipelines,
- Convening international pipeline security forums for U.S. and Canadian governments and pipeline industry officials,
- Facilitating pipeline security drills and exercises including those under the Intermodal Security Training Exercise Program (I-STEP),
- Developing pipeline security awareness training materials,
- Convening periodic information-sharing conference calls between key pipeline security stakeholders, and
- Participating in Sector Coordinating Councils and Joint Sector Committees.[39]

In addition to these activities, TSA has also conducted regional supply studies for key natural gas markets, has conducted training on cyber security awareness, has participated in pipeline blast mitigation studies, and has joined in "G-8" multinational security assessment and planning.[40]

Pipeline Cyber Security Initiatives

Pipeline cyber security is an element of several federal initiatives within DHS.[41] For example, TSA has included a number of general cybersecurity provisions in its industry security guidance[42] and has encouraged industry compliance with the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*.[43] TSA has also employed the

[37] Department of Homeland Security, "Extension of Agency Information Collection Activity Under OMB Review: Critical Facility Information of the Top 100 Most Critical Pipelines," 76 *Federal Register* 62818, October 11, 2011.

[38] Jack Fox, General Manager, Pipeline Security Division, Transportation Security Administration, personal communication, February 24, 2012.

[39] Jack Fox, Pipeline Industry Engagement Manager, TSA, *Pipeline Security: An Overview of TSA Programs*, slide presentation, May 5, 2014; Transportation Security Administration, *Transportation Systems Sector-Specific Plan*, 2010, p. 326.

[40] Transportation Security Administration, *Pipeline Modal Annex*, June 2007, pp. 10-11. G8 = Group of Eight (the United States, the United Kingdom, Canada, France, Germany, Italy, Japan, and Russia).

[41] The Interstate Natural Gas Association of America (INGAA), a trade association for gas pipeline companies, maintains its own extensive cyber security guidelines for natural gas pipeline control systems: INGAA, *Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry*, Washington, DC, January 31, 2011. Likewise, the American Petroleum Institute (API), a trade association within the oil industry, maintains a standard for oil pipeline control system security: API, *Pipeline SCADA Security*, Second Edition, API Std. 1164, Washington, DC, June 2009.

[42] For example, TSA's guidance advises operators to "conduct a risk assessment to weigh the benefits of implementing wireless networking against the potential risks for exploitation." TSA, April 2011, p. 18.

[43] Jack Fox, Pipeline Industry Engagement Manager, TSA, personal communication, October 29, 2015. See: National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, February 12, 2014, (continued...)

Cybersecurity Assessment and Risk Management Approach (CARMA) in collaborating with key stakeholders to identify pipeline industry value chains, critical functions, and supporting cyber infrastructure.[44] The agency has also coordinated with DHS and the Department of Energy to harmonize existing cybersecurity risk management programs. Pipelines are also included in DHS's multi-modal cybersecurity initiatives, such as its Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).[45] The TSA also has established a public/private partnership-based cybersecurity program supporting the National Infrastructure Protection Plan. Pipeline operators have participated in DHS-sponsored control systems cybersecurity training and also participate in the DHS Industrial Control Systems Joint Working Group.[46]

Outside DHS, the Department of Energy operates the National SCADA Test Bed Program, a partnership with Idaho National Laboratory, Sandia National Laboratories, and other national laboratories which addresses control system security challenges in the energy sector. Among its key functions, the program performs control systems testing, research and development; control systems requirements development; and industry outreach.[47] Sandia Laboratories also performs authorized defensive cybersecurity assessments for government, military, and commercial customers through its Information Design Assurance Red Team (IDART) program.[48]

The Relationship Between DOT and TSA

Since TSA was established, Congress has had a continuing interest in the appropriate division of pipeline security authority between the DOT and TSA.[49] Both the DOT and TSA have played important roles in the federal pipeline security program, with TSA the designated lead agency since 2002. In 2004, the DOT and DHS entered into a memorandum of understanding (MOU) concerning their respective security roles in all modes of transportation. The MOU notes that DHS has the primary responsibility for transportation security with support from the DOT, and establishes a general framework for cooperation and coordination. On August 9, 2006, the departments signed an annex "to delineate clear lines of authority and responsibility and promote communications, efficiency, and nonduplication of effort through cooperation and collaboration between the parties in the area of transportation security."[50]

In January 2007, DOT officials testified before Congress that the agency had established a joint working group with TSA "to improve interagency coordination on transportation security and safety matters, and to develop and advance plans for improving transportation security," presumably including pipeline

(...continued)

http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[44] Jack Fox, May 5, 2014.

[45] Department of Homeland Security, "Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)," web page, April 13, 2106, https://ics-cert.us-cert.gov/.

[46] Department of Homeland Security, "Industrial Control Systems Joint Working Group (ICSJWG)," web page, April 13, 2016, https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG.

[47] U.S. Department of Energy, "National SCADA Test Bed," web page, August 13, 2016, http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity/national-scada-test-bed.

[48] Sandia National Laboratories, "The Information Design Assurance Red Team (IDART)," web page, August 13, 2016, http://www.idart.sandia.gov/.

[49] For example, see Hon. William J. Pascrell, Jr., statement at the House Committee on Transportation and Infrastructure, Subcommittee on Highways, Transit and Pipelines, hearing on Pipeline Safety, March 16, 2006.

[50] Transportation Security Administration and Pipelines and Hazardous Materials Safety Administration, "Transportation Security Administration and Pipelines and Hazardous Materials Safety Administration Cooperation on Pipelines and Hazardous Materials Transportation Security," August 9, 2006.

security.[51] According to TSA, the working group developed a multi-year action plan specifically delineating roles, responsibilities, resources and actions to execute 11 program elements: identification of critical infrastructure/key resources and risk assessments; strategic planning; developing regulations and guidelines; conducting inspections and enforcement; providing technical support; sharing information during emergencies; communications; stakeholder relations; research and development; legislative matters; and budgeting.[52] Nonetheless, a DOT Inspector General (IG) assessment published May 2008 was not satisfied with this plan. The IG report stated that, although the agencies

> have taken initial steps toward formulating an action plan to implement the provisions of the pipeline security annex ... further actions need to be taken with a sense of urgency because the current situation is far from an "end state" for enhancing the security of the Nation's pipelines.[53]

The assessment recommended that the DOT and TSA finalize and execute their security annex action plan, clarify their respective roles, and jointly develop a pipeline security strategy that maximizes the effectiveness of their respective capabilities and efforts.[54] According to TSA, working with the DOT "improved drastically" after the release of the IG report; the two agencies began maintaining daily contact, sharing information in a timely manner, and collaborating on security guidelines and incident response planning.[55]

Key Policy Issues

While the federal government has been engaged in various efforts to protect the nation's oil and natural gas pipelines from deliberate attacks since September 11, 2001, questions remain regarding the structure and effectiveness of these efforts. Three specific issues, in particular, may warrant further congressional consideration: (1) TSA's pipeline security resources, (2) voluntary versus mandatory security standards, and (3) uncertainty about security risks to the nation's pipeline network.

TSA Pipeline Security Resources

Some Members of Congress have been critical in the past of TSA's level of funding of non-aviation security activities, including pipeline activities. For example, as one Member remarked in 2005, "aviation security has received 90% of TSA's funds and virtually all of its attention. There is simply not enough being done to address ... pipeline security."[56] At a congressional hearing in 2010, another Member expressed concern that TSA's pipeline division did not have sufficient staff to carry out a federal pipeline security program on a national scale.[57] With respect to pipeline security funding, little may have changed since 2005. The President's FY2017 budget request for DHS does not include a separate line item for TSA's pipeline security activities. The budget does request $110.8 million for "Surface Transportation

[51] Barrett, T.J., Administrator, Pipeline and Hazardous Materials Safety Administration (PHMSA), Testimony before the Senate Committee on Commerce, Science, and Transportation hearing on Federal Efforts for Rail and Surface Transportation Security, January 18, 2007.

[52] Transportation Security Administration, Pipeline Security Division, personal communication, July 6, 2007.

[53] U.S. Dept. of Transportation, Office of Inspector General, *Actions Needed to Enhance Pipeline Security, Pipeline and Hazardous Materials Safety Administration*, Report No. AV-2008-053, May 21, 2008, p. 3.

[54] Ibid. pp. 5-6.

[55] Jack Fox, TSA, Pipeline Security Division, personal communication, February 2, 2010.

[56] Sen. Daniel K. Inouye, opening statement before the Senate Committee on Commerce, Science and Transportation, hearing on the President's FY2006 Budget Request for the Transportation Security Administration (TSA), February 15, 2005.

[57] Congressman Gus M. Billirakis, Remarks before the House Committee on Homeland Security, Subcommittee on Management, Investigations, and Oversight hearing on "Unclogging Pipeline Security: Are the Lines of Responsibility Clear?," Plant City, FL, April 19, 2010.

Security," which encompasses security activities in non-aviation transportation modes, including pipelines. The budget would fund 761 full-time equivalent (FTE) employees.[58] TSA's pipeline branch has traditionally received from the agency's general operational budget an allocation for routine operations, travel, and outreach. The budget historically has funded on the order of 10 to 15 FTE staff to carry out the agency's pipeline security program.[59]

At its current staffing level, TSA's pipelines branch has limited field presence for pipeline site visits, and has constrained capabilities for updating standards, interacting in the various stakeholder groups with which it collaborates, analyzing security information, and fulfilling other administrative responsibilities. In conducting a pipeline corporate security review, for example, TSA typically sends one to three staff to hold a three to four hour interview with the operator's security representatives followed by a visit to only one or two of the operator's pipeline assets.[60] There is concern by some that the agency's CSRs (as currently structured) may not allow for rigorous security plan verification nor a credible threat of enforcement, so operator compliance with security guidance is uncertain. The limited number of CSR's the agency can complete in a year has also been a concern to some, even within TSA. According to a 2009 Government Accountability Office report, "TSA's pipeline division stated that they would like more staff in order to conduct its corporate security reviews more frequently," in part because other staff responsibilities such as "analyzing secondary or indirect consequences of a terrorist attack and developing strategic risk objectives required much time and effort."[61]

TSA's handful of field inspection staff stands in contrast to the hundreds of pipeline safety inspection staff available to the DOT at the federal and state levels. Furthermore, in the face of an expanding U.S. pipeline network and evolving safety requirements, DOT's budget authority for pipeline safety has more than doubled over the last 10 years.[62] Given this disparity, it may be logical to consider whether DOT's field staff, who are charged with inspecting the same pipeline systems as TSA, could somehow be deployed to help fulfill the nation's pipeline security objectives. The question also arises whether having separate inspections of the same pipeline systems for safety and security may be inherently inefficient, or may miss an opportunity for more frequent or thorough examination of pipeline security. Presumably many of the jurisdictional, operational, or administrative issues that were considered in the drafting of the 2004 MOU between DOT and TSA remain unchanged, but new factors—such as the evolving threat environment or greater experience with pipeline company security efforts—could warrant a reconsideration of the relationship between the agencies.

Voluntary vs. Mandatory Pipeline Security Standards

Federal pipeline security activities to date have relied upon voluntary industry compliance with DOT's original security guidance, which later became TSA's security best practices. By initiating this voluntary approach in 2002, DOT sought to speed adoption of security measures by industry and avoid the publication of sensitive security information (e.g., critical asset lists) that would normally be required in

[58] U.S. Office of Management and Budget, *Budget of the United States Government, Fiscal Year 2017: Appendix*, February 2016, p.537.

[59] Jack Fox, October 29, 2015.

[60] Department of Homeland Security, "Intent to Request Approval from OMB of One New Public Collection of Information: Pipeline Corporate Security Review," 74 *Federal Register* 42086, August 20, 2009.

[61] U.S. Government Accountability Office, *Transportation Security: Comprehensive Risk Assessments and Stronger Internal Controls Needed to Help Inform TSA Resource Allocation*, GAO-09-492, March 2009, p. 30, http://www.gao.gov/new.items/d09492.pdf.

[62] U.S. Office of Management and Budget, *Budget of the United States Government, Appendix*, Fiscal Years 2006 through 2017, "Pipeline Safety," Line 1900 "Budget authority (total)."

public rulemaking.[63] However, a key subject of debate is the adequacy of the TSA's voluntary approach to pipeline security, generally, and cybersecurity, in particular. For example, provisions in the Pipeline Inspection, Protection, Enforcement, and Safety Act of 2006 (P.L. 109-468) required the DOT Inspector General (IG) to "address the adequacy of security standards for gas and oil pipelines" (§23(b)(4)). The 2008 IG's report stated that

> TSA's current security guidance is not mandatory and remains unenforceable unless a regulation is issued to require industry compliance.... [DOT] and TSA will need to conduct covert tests of pipeline systems' vulnerabilities to assess the current guidance as well as the operators' compliance.[64]

Although the IG report did not elaborate on this recommendation, covert testing of vulnerabilities would likely include testing of both physical security measures and cybersecurity measures. The latter would be in place to protect pipeline SCADA systems and sensitive operating information such as digital pipeline maps, system design data, and emergency response plans. Consistent with the IG's recommendation, an April 2011 White House proposal[65] and the Cybersecurity Act of 2012 (S. 2105) both would have mandated the promulgation of cybersecurity regulations for pipelines, among other provisions, although these proposals would not necessarily have conferred upon TSA any authority it does not already have to regulate pipeline security.

In contrast to the IG's conclusions and the legislative proposals above, the pipeline industry has consistently expressed concern that security regulations could be "redundant" and "may not be necessary to increase pipeline security."[66] Echoing this sentiment, a DOT official testified in 2007 that enhancing security "does not necessarily mean that we must impose regulatory requirements."[67]

TSA officials have similarly questioned the need for new pipeline security regulations, particularly the IG's call for covert testing of pipeline operator security measures. The TSA has argued in the past that the agency is complying with the letter of P.L. 110-53 and that its pipeline operator security reviews are more than paper reviews.[68] TSA officials assert that security regulations could be counterproductive because they could establish a general standard below the level of security already in place at many pipeline companies based on their company-specific security assessments. Because the TSA believes the most critical U.S. pipeline systems generally meet or exceed industry security guidance, the agency asserts that it achieves better security with voluntary guidelines, and maintains a more cooperative and collaborative relationship with its industry partners as well.[69]

---

[63] GAO, *Pipeline Security and Safety: Improved Workforce Planning and Communication Needed*, GAO-02-785, August 2002, p. 22.

[64] U.S. Dept. of Transportation, Office of Inspector General, May 21, 2008, p. 6.

[65] The White House, "Legislative Language, Cybersecurity Regulatory Framework for Covered Critical Infrastructure," April 2011, p. 33, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/law-enforcement-provisions-related-to-computer-security-full-bill.pdf.

[66] American Gas Association (AGA), American Petroleum Institute (API), Association of Oil Pipe Lines (AOPL), and American Public Gas Association (APGA), joint letter to members of the Senate Commerce Committee providing views on S. 1052, August 22, 2005.

[67] T.J. Barrett, Administrator, Pipeline and Hazardous Materials Safety Administration, Department of Transportation, Testimony before the Senate Committee on Commerce, Science, and Transportation hearing on Federal Efforts for Rail and Surface Transportation Security, January 18, 2007.

[68] John Sammon, Transportation Security Administration, Testimony before the House Transportation and Infrastructure Committee, Railroad, Pipelines, and Hazardous Materials Subcommittee hearing on Implementation of the Pipeline Inspection, Protection, Enforcement, and Safety Act of 2006, June 24, 2008.

[69] John Pistole, Administrator, TSA, testimony before the Senate Committee on Commerce, Science, and Transportation hearing on Transportation Security Administration Oversight: Confronting America's Transportation Security Challenges, April 30, 2014; Jack Fox, General Manager, Pipeline Security Division, TSA, Remarks before the Louisiana Gas Association Pipeline Safety (continued...)

The Energy Sector Control Systems Working Group makes related assertions in its *Roadmap to Achieve Energy Delivery Systems Cybersecurity* about the effectiveness of cybersecurity standards alone:

> Although standards may elevate cybersecurity across the energy sector, they do so by requiring the implementation of minimum security measures that set a baseline for cybersecurity across an industry. These minimum security levels may not be sufficient to secure the sector against new and quickly evolving risks. Asset owners compliant with standards may still be vulnerable to cyber intrusion.[70]

Thus, in addition to cybersecurity requirements, pipeline companies may also need appropriate management practices, performance metrics, access to intelligence, and other support measures to maximize the effectiveness of their cybersecurity programs.

Although the TSA believes a voluntary approach to pipeline security is most effective, Canadian pipeline regulators have come to a different conclusion. In 2010 the National Energy Board (NEB) of Canada mandated security regulations for jurisdictional Canadian petroleum and natural gas pipelines, some of which are cross-border pipelines entering the United States. Many companies operate pipelines in both countries. In announcing these new regulations, the board stated that it had considered adopting the existing cybersecurity standards "as guidance" rather than an enforceable standard, but "taking into consideration the critical importance of energy infrastructure protection," the board decided to adopt the standard into the regulations.[71] Establishing pipeline security regulations in Canada is not completely analogous to doing so in the United States as the Canadian pipeline system is much smaller and operated by far fewer companies than the U.S. system. Nonetheless, Canada's choice to regulate pipeline security may raise questions as to why the United States has not.

The Federal Energy Regulatory Commission (FERC), which regulates the U.S. bulk electric power system, has also taken a more directive approach to infrastructure security. The Energy Policy Act of 2005 (P.L. 109-58) gave the commission authority to oversee the reliability of the bulk power system, including authority to approve mandatory security standards. FERC approved mandatory Critical Infrastructure Protection cyber security reliability standards in 2008.[72] The commission approved mandatory physical security standards in 2014[73] after a successful physical attack on a high-voltage transformer facility in California. While it differs in important ways from the pipeline system, the bulk power system faces the same threat environment and has many similar security vulnerabilities related to asset exposure and reliance on SCADA systems for network operations.

In addition to examining the regulatory motivations of the NEB and FERC, consideration of mandatory pipeline security standards within TSA would have to account for the requirements to implement such standards. Unlike maintaining voluntary standards, developing pipeline security regulations—with provisions for pipeline operations, inspection, reporting, and enforcement—would involve a complex and potentially contentious rulemaking process involving multiple stakeholders. Should Congress choose to

(...continued)

Conference, New Orleans, LA, July 25, 2012.

[70] Energy Sector Control Systems Working Group, *Roadmap to Achieve Energy Delivery Systems Cybersecurity*, September 2011, p. 15.

[71] National Energy Board of Canada, *Proposed Regulatory Change (PRC) 2010-01, Adoption of CSA Z246.1-09 Security Management for Petroleum and Natural Gas Industry Systems*, File Ad-GA-SEC-SecGen 0901, May 3, 2010, p. 1, https://www.neb-one.gc.ca/ll-eng/livelink.exe/fetch/2000/90463/409054/614444/A1S7H7_-_Proposed_Regulatory_Change_(PRC)_2010-01.pdf?nodeid=614556&vernum=0.

[72] Federal Energy Regulatory Commission, *Mandatory Reliability Standards for Critical Infrastructure Protection*, Docket No. RM06-22-000, Order No. 706, January 18, 2008.

[73] Federal Energy Regulatory Commission, *Physical Security Reliability Standard*, Docket No. RM14-15-000, Order No. 802, Issued November 20, 2014.

mandate the promulgation of such regulations, it is not clear that TSA's pipeline security division as currently configured would be up to the task. Developing specific cybersecurity regulations may pose a particular challenge as the TSA's pipeline branch has limited existing capability to do so, although such capabilities may reside elsewhere in DHS. If mandatory standards were to be imposed, there may also be questions as to whether the agency as currently structured would have sufficient resources to implement the new security regulations, conduct rigorous security plan verification, and pose a credible threat of enforcement.

Uncertainty About Security Risks

A January 2011 federal threat assessment concluded "with high confidence that the terrorist threat to the U.S. pipeline industry is low."[74] However, subsequent events may have increased concerns about pipeline system threats, especially cyber threats. In a 2016 Federal Register notice, TSA stated that it expects pipeline companies will report approximately 30 "security incidents" annually—both physical and cyber.[75] The agency has not publicly released a more current pipeline threat assessment.

The pipeline industry's security risk assessments rely upon information about security threats provided by the federal government and by pipeline operators themselves. The quantity, quality and timeliness of this threat information is a key determinant of what pipeline companies need to be protecting against, and what security measures to take. Incomplete or ambiguous threat information—especially from the federal government—may lead to inconsistency in physical and cyber security among pipeline owners, inefficient spending of limited security resources at facilities (e.g., that may not really be under threat), or deployment of security measures against the wrong threat.

Concerns about the quality and specificity of federal threat information have long been an issue across all critical infrastructure sectors.[76] Threat information continues to be an uncertainty in the case of pipeline network security. There may be agreement among government and industry stakeholders that oil and natural gas pipelines in the United States are vulnerable to attack, and that such attacks potentially could have catastrophic consequences. But the most serious, damaging attacks could require operational information and a certain level of sophistication, especially in the cyber regime, on the part of potential attackers. Consequently, despite the technical arguments, without more specific information about potential targets and attacker capabilities, the true risk of a serious attack on the pipeline system remains an open question.

Conclusion

The nation's pipeline network is attractive to malicious actors and vulnerable to both physical and cyberattacks. Based on recent history, a strong federal pipeline security program is clearly necessary; there has been a series of unrelated terrorist plots and attempted attacks on U.S. pipelines since at least the 1990s. Real bombs have been planted, computers systems have been infiltrated, and perpetrators have been imprisoned. Such threats to the pipeline system are likely to continue.

Both government and industry have taken numerous steps to improve pipeline security since 2001. On their face, these measures have been expansive and seem to address the full range of activities and priorities Congress intended when it embarked upon a national strategy for protecting critical infrastructure. However, while TSA and industry may be engaged in appropriate pipeline security

[74] Transportation Security Administration, Office of Intelligence, *Pipeline Threat Assessment*, January 18, 2011, p. 3.

[75] 81 *Fed. Reg*. 37, February 25, 2016, p.9495.

[76] See, for example, Philip Shenon, "Threats and Responses: Domestic Security," *New York Times*, June 5, 2003, p. A15.

activities, questions remain as to their level of commitment to those activities and how effective they have been in protecting the pipeline system. TSA's pipeline staff would account for less than 2% of the agency's surface transportation security staff under the proposed FY2017 budget, and just over 2% of the staff available to DOT under its pipeline safety program. Pipeline company expenditures on security are not generally reported, so their level of financial commitment is unknown. Furthermore, while there have been no publicly reported *successful* attacks on the U.S. pipeline system since 2001, existing physical security measures did not prevent two attackers from planting the live explosive devices along two different U.S. pipelines in 2011 and 2012 discussed earlier. Their failure to detonate was fortunate.

The TSA maintains that its pipeline security program, administered as it is and relying upon voluntary standards, has been effective in protecting U.S. pipelines from physical and cyberattacks. Based on the agency's corporate security reviews, TSA believes security among major U.S. pipeline systems is good, and pipeline operators agree. However, without formal security plans and reporting requirements, it is difficult for Congress and the general public to know for certain. To a great extent, the public must therefore rely on the pipeline industry's self-interest to protect itself from malicious threats. Whether this self-interest is sufficient to generate the level of security appropriate for a critical infrastructure sector, and whether imposing mandatory standards would be a better approach, is open to debate. Faced with this uncertainty, legislators must rely upon their own best judgment to reach conclusions about the federal pipeline security program. If Congress concludes that current voluntary measures are insufficient to protect the pipeline system, it may decide to provide specific direction to the TSA to develop regulations and provide additional resources to support them, as such an effort may be beyond the TSA pipeline branch's existing capabilities.

Congress also may assess how the various elements of U.S. pipeline safety and security activity fit together in the nation's overall strategy to protect critical infrastructure. For example, diverting pipeline resources away from safety to enhance security might further reduce terror risk, but not overall pipeline risk, if safety programs become less effective as a result. Pipeline safety and security necessarily involve many groups: federal and state agencies, oil and gas pipeline associations, large and small pipeline operators, and local communities. Reviewing how these groups work together to achieve common goals could be an oversight challenge for Congress.