Pipeline Cybersecurity: Federal Policy

Paul W. Parfomak
Specialist in Energy and Infrastructure Policy

August 16, 2012

Congressional Research Service
7-5700
www.crs.gov
R42660

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

The vast U.S. network of natural gas and hazardous liquid pipelines is integral to U.S. energy supply and has vital links to other critical infrastructure. While an efficient and fundamentally safe means of transport, this network is vulnerable to cyber attacks. In particular, cyber infiltration of supervisory control and data acquisition (SCADA) systems could allow successful "hackers" to disrupt pipeline service and cause spills, explosions, or fires—all from remote locations. In March 2012, the Department of Homeland Security (DHS) reported ongoing cyber intrusions among U.S. natural gas pipeline operators. These intrusions have heightened congressional concern about cybersecurity in the U.S. pipelines sector.

The Transportation Security Administration (TSA) is authorized by federal statute to promulgate pipeline physical security and cybersecurity regulations, if necessary, but the agency has not issued such regulations. TSA officials assert that security regulations could be counterproductive because they could establish a general standard below the level of security already in place for many pipelines. An April 2011 White House proposal and the Cybersecurity Act of 2012 (S. 2105) both would mandate cybersecurity regulations for privately owned critical infrastructures sectors like pipelines. A revised version of S. 2105, S. 3414, would permit the issuance of regulations but would focus on voluntary cybersecurity measures.

While the pipelines sector has many cybersecurity issues in common with other critical infrastructure sectors, it is somewhat distinct in several ways:

- Pipelines in the United States have been the target of several confirmed terrorist plots and attempted physical attacks since September 11, 2001.
- Changes to pipeline computer networks over the past 20 years, more sophisticated hackers, and the emergence of specialized malicious software have made pipeline SCADA operations increasingly vulnerable to cyber attacks.
- There recently has been a coordinated series of cyber intrusions specifically targeting U.S. pipeline computer systems.
- TSA already has statutory authority to issue cybersecurity regulations for pipelines if the agency chooses to do so, but it may not have the resources to develop, implement, and enforce such regulations if they are mandated.

TSA maintains that voluntary standards have been effective in protecting U.S. pipelines from cyber attacks. Based on the agency's corporate security reviews, TSA believes cybersecurity among major U.S. pipeline systems is effective. However, without formal cybersecurity plans and reporting requirements, it is difficult for Congress to know for certain. Whether the self-interest of pipeline operators is sufficient to generate the level of cybersecurity appropriate for a critical infrastructure sector is open to debate. If Congress concludes that current voluntary measures are insufficient to ensure pipeline cybersecurity, 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 Security Division's existing capabilities.

Contents

Introduction 1
Pipeline Security Risks 2
General Security Threats to U.S. Pipelines 2
SCADA System Security Risks 3
Cyber Threats to U.S. Pipelines 4
U.S. Pipeline Cybersecurity Initiatives 5
Adequacy of Voluntary Pipeline Cybersecurity 7
TSA Pipeline Cybersecurity Resources 8
Conclusions 9

Contacts

Author Contact Information 10

Introduction

Over 500,000 miles of high-volume pipeline gather and transport natural gas, oil, and other hazardous liquids across the United States. In addition, nearly 900,000 miles of smaller distribution pipeline deliver natural gas to businesses and homes.[1] This vast pipeline network is integral to U.S. energy supply and has links to power plants, refineries, airports, and other critical infrastructure. While pipelines are an efficient and fundamentally safe means of transport, many carry volatile, flammable, or toxic materials with the potential to cause public injury and environmental damage. Consequently, pipeline systems have drawn attention as possible targets for terrorism or other malicious activity. 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. In particular, 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.

In March 2012, the Department of Homeland Security (DHS) reported ongoing cyber intrusions among U.S. natural gas pipeline operators.[2] The incidents drew new attention to an Al Qaeda video obtained in 2011 by the Federal Bureau of Investigation (FBI) reportedly calling for "electronic jihad" against U.S. critical infrastructure.[3] These cybersecurity events coupled with serious consequences from recent pipeline accidents have heightened congressional concern about cybersecurity measures in the U.S. pipelines sector.

The Transportation Security Administration (TSA) is authorized by federal statute to promulgate pipeline physical security and cybersecurity regulations, if necessary, but the agency has not found a need to issue such regulations to date. An April 2011 White House proposal[4] and the Cybersecurity Act of 2012 (S. 2105) both would mandate the promulgation of cybersecurity regulations for pipelines, among other privately-owned critical infrastructures sectors. A revised version of S. 2105, S. 3414, would permit the issuance of regulations but would focus on voluntary cybersecurity measures. Whether pipelines would be better protected under cybersecurity regulations or under voluntary standards is the subject of ongoing debate.

This report reviews federal programs specifically addressing pipeline cybersecurity, as well as related private sector initiatives and key policy concerns. For a more comprehensive analysis of federal cybersecurity legislative frameworks see, CRS Report R42114, *Federal Laws Relating to Cybersecurity: Discussion of Proposed Revisions*, by Eric A. Fischer. For more general analysis

[1] Pipeline and Hazardous Materials Safety Administration, "Natural Gas Transmission, Gas Distribution, & Hazardous Liquid Pipeline Annual Mileage," online table, July 3, 2012, http://www.phmsa.dot.gov/pipeline/library/data-stats. Hazardous liquids primarily include crude oil, gasoline, jet fuel, diesel fuel, home heating oil, propane, and butane. Other hazardous liquids transported by pipeline include anhydrous ammonia, carbon dioxide, kerosene, liquefied ethylene, and some petrochemical feedstocks.

[2] 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.

[3] Jack Cloherty, "Virtual Terrorism: Al Qaeda Video Calls for 'Electronic Jihad'," ABC News, May 22, 2012.

[4] 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.

of federal pipeline safety and security issues, see CRS Report R41536, *Keeping America's Pipelines Safe and Secure: Key Issues for Congress*, by Paul W. Parfomak.

Pipeline Security Risks

The pipeline sector has long been considered vulnerable to intentional damage by malicious individuals or organizations—either by physical attacks or by cyber attacks on their computerized SCADA systems.[5] Cybersecurity risks reflect both general threats to the pipeline sector as a whole and specific threats to SCADA systems as the focus of attack. These threats are discussed in the following sections.

General Security Threats to U.S. Pipelines

Since September 11, 2001, federal security warnings have identified pipelines as potential terror targets in the United States.[6] Until recently, attention was most heavily focused on physical threats to pipelines, especially in light of several actual plots involving physical pipeline attacks on U.S. soil. In 2006, for example, federal authorities acknowledged the discovery of a detailed posting on a website linked to Al Qaeda that reportedly encouraged attacks on U.S. pipelines using weapons or hidden explosives.[7] In 2007, the U.S. Department of Justice arrested members of a terrorist group planning to blow up jet fuel pipelines and storage tanks at the John F. Kennedy International Airport in New York.[8] Also in 2007, a U.S. citizen was convicted of trying to conspire with Al Qaeda to attack the Trans Alaska Pipeline System as well as a major natural gas pipeline in the eastern United States.[9] In 2011, federal agents arrested a U.S. citizen for planting an explosive device (which failed to detonate) under a natural gas pipeline in Oklahoma.[10] In June 2012, a man was critically injured attempting to plant an improvised explosive device along a natural gas pipeline in Plano, Texas.[11]

Notwithstanding the security incidents cited above, a January 2011 federal threat assessment concluded "with high confidence that the terrorist threat to the U.S. pipeline industry is low."[12] However, this assertion appears to have taken account of primarily physical threats, because the assessment also stated that "terrorist groups have discussed attacks on unspecified SCADA systems, but it is uncertain whether al-Qa'ida or any other group has the capability to conduct a

[5] J.L. Shreeve, "Science & Technology: The Enemy Within," *The Independent*. London, UK, May 31, 2006, p. 8.

[6] "Already Hard at Work on Security, Pipelines Told of Terrorist Threat," *Inside FERC*, McGraw-Hill Companies, January 3, 2002.

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

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

[9] 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.

[10] Carol Cratty, "Man Accused in Attempted Bombing of Oklahoma Gas Pipeline," CNN, August 12, 2011.

[11] "Grand Jury Indicts Plano Gas Pipeline Bomb Suspect on Weapons Charge," Associated Press, July 11, 2012.

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

successful cyber attack on these systems."[13] Subsequent events have increased pipeline sector concerns about cyber threats.

SCADA System Security Risks

Supervisory control and data acquisition (SCADA) systems are software-based industrial control systems used to monitor and control many aspects of network operation for railways, utility power grids, water and sewer systems, and pipeline networks. In the pipelines sector, SCADA systems collect data (e.g., line pressure) in real time from sensors throughout a pipeline network, displaying those data to human operators in remote network control rooms. These operators can send computerized commands from SCADA workstations to control geographically dispersed pipeline equipment such as valves, pumps, and compressor stations. The SCADA system provides continuous feedback about conditions all along a pipeline, generating safety alarms when operating conditions fall outside prescribed levels.[14] Communications links throughout the pipeline network may employ dedicated telephone landlines, wireless communications (satellite, microwave, and radio), cellular telephone service, Wi-Fi, and the Internet. As SCADA technology has matured, system control has become more intelligent and more automated, requiring less human intervention.[15]

Historically, pipeline SCADA systems employed highly customized proprietary software and were physically isolated from outside communications and computer networks. Because many of these systems were largely unique to a specific pipeline operator, it would have been difficult for malicious individuals outside the company to access a SCADA system and know what to do with it. However, due to improvements in computer technology and the ongoing development of communications and Internet-based control system applications, SCADA systems have become much more vulnerable to outside intrusion and manipulation.[16] Specific SCADA security weaknesses include the adoption of standardized control system technologies with known vulnerabilities, increased connection to external networks, insecure communication connections, and the public availability of sensitive information about control systems and infrastructure.[17]

Once accessible to a knowledgeable attacker, a SCADA system can be exploited in a number of specific ways to carry out a pipeline cyber attack:

- issuing unauthorized commands to control equipment;
- sending false information to a control-system operator that initiates inappropriate actions;

[13] Ibid.

[14] National Transportation Safety Board, *Supervisory Control and Data Acquisition (SCADA) in Liquid Pipelines*, NTSB/SS-05/02, November 29, 2005, pp 1-2.

[15] General Accounting Office (GAO), *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*, GAO-04-354, March 2004, p. 11.

[16] Tobias Walk, "Cyber-attack Protection for Pipeline SCADA Systems," *Pipelines International Digest*, January 2012, p. 6; Rose Tsang, Cyberthreats, "Vulnerabilities and Attacks on SCADA Networks," working paper, University of California, Goldman School of Public Policy, 2009, p. 2, http://gspp.berkeley.edu/iths/Tsang_SCADA%20Attacks.pdf.

[17] GAO, 2004, pp. 12-13; Eric Byres, "Next Generation Cyber Attacks Target Oil and Gas SCADA," *Pipeline & Gas Journal*, February 2012; Robert O'Harrow, Jr., "Cyber Search Engine Exposes Vulnerabilities," *Washington Post*, June 3, 2102.

- disrupting control system operation by delaying or blocking the flow of information through the control network;
- making unauthorized changes to control system software to modify alarm thresholds or other configuration settings; and
- rendering resources unavailable by propagating malicious software (e.g., a virus, worm, Trojan horse) through the control network.[18]

Depending upon the configuration of a particular pipeline system, such cyber attacks could potentially disrupt pipeline service, damage pipeline equipment (e.g., with excessive pressure), or cause a hazardous release of pipeline commodities into the environment. Even if a hacker did not intend to damage or disrupt the pipeline system, by gaining access to or control of the SCADA system, the intruder could cause serious harm unintentionally.

There have been no major pipeline commodity releases in the United States that investigators have attributed to malicious cyber activity, but SCADA-related problems were a primary cause or contributing factor in several recent pipeline accidents which had catastrophic consequences.

- **San Bruno, CA**—A 2010 natural gas pipeline explosion killed 8 people, injured 60 others, and destroyed 37 homes. Erroneous and unavailable SCADA pressure readings and other SCADA deficiencies were partly responsible for excessive line pressure which ruptured the pipeline.[19]
- **Marshall, MI—**A 2010 pipeline spill released 819,000 gallons of crude oil into a tributary of the Kalamazoo River. Various SCADA control center deficiencies, including the mishandling of pressure alarms, delayed the spill response and increased the size of the spill.[20]
- **Bellingham, WA—**A 1999 gasoline pipeline explosion killed three people and caused $45 million in damage to a city water plant and other property. The SCADA system used to operate the pipeline became unresponsive, making it difficult to analyze pipeline conditions and respond to operational problems that led to the pipeline failure.[21]

While these incidents were all accidental, they are indicative of physical consequences that could result from a pipeline release initiated by a cyber attacker.

Cyber Threats to U.S. Pipelines

In March 2012, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) within the Department of Homeland Security (DHS) identified an ongoing series of cyber intrusions among U.S. natural gas pipeline operators dating back to December 2011. According to

[18] Tobias Walk, 2012, pp. 7-8.

[19] National Transportation Safety Board (NTSB), *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, pp. 5-12.

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

[21] National Transportation Safety Board (NTSB). *Pipeline Rupture and Subsequent Fire in Bellingham, Washington, June 10, 1999*, NTSB/PAR-02/02, October 8, 2002, p. 56.

the agency, various pipeline companies described targeted spear-phishing[22] attempts and intrusions into multiple natural gas pipeline sector organizations "positively identified … as related to a single campaign."[23] 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.[24] 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 Siemens industrial SCADA systems.[25] The Stuxnet program was reportedly developed thorough a joint United States-Israeli effort to target Iranian computer systems, but it may serve as a model for similar types of malicious programs that could be developed by others in the future.[26] Computer security specialists claim that malicious software developers have already created new software programs tailored to target the kinds of SCADA system weaknesses revealed by Stuxnet.[27]

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. Federal agencies and pipeline operators are aware of these threats, however, and have programs in place to counter them. These programs are discussed in the following section.

U.S. Pipeline Cybersecurity Initiatives

The federal program for U.S. pipeline security began under the Department of Transportation (DOT)[28] immediately after the terror attacks of September 11, 2001. The Aviation and Transportation Security Act of 2001 (P.L. 107-71), which established the Transportation Security Administration within the DOT, authorized the agency "to issue, rescind, and revise such regulations as are necessary" to carry out its functions (§101). TSA was transferred to the Department of Homeland Security (DHS), newly created under the Homeland Security Act of 2002 (P.L. 107-296). Homeland Security Presidential Directive 7 maintained DHS as the lead agency for pipeline security, and instructed the DOT to "collaborate in regulating the transportation of hazardous materials by all modes (including pipelines)." The Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) directs TSA to promulgate

[22] "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.

[23] 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.

[24] 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

[25] Tobias Walk, 2007, p. 7.

[26] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *New York Times*, June 1, 2012.

[27] Eric Byres, February 2012.

[28] The DOT regulates natural gas and hazardous liquid pipelines safety.

pipeline security regulations and carry out necessary inspection and enforcement if the agency determines that regulations are appropriate (§1557(d)). Thus, TSA has primary responsibility and regulatory authority for the security of natural gas and hazardous liquid (e.g., oil, carbon dioxide) pipelines in the United States. Pipeline security activities at TSA are led by the Pipeline Security Division (PSD) within the agency's Office of Security Policy and Industry Engagement (OSPIE). The PSD is staffed by 13 employees funded out of TSA's general budget.

Although 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.[29] This guidance includes a number of general cybersecurity provisions.[30] Under its Corporate Security Review program, TSA visits the largest pipeline and natural gas distribution operators to review their security plans and inspect their facilities to evaluate whether each company is following the intent of its security guidance. Pipelines are also included in DHS's multi-modal cybersecurity initiatives, such as its Control System Security Program (CSSP).[31] TSA also has established a public/private partnership-based cybersecurity program supporting the National Infrastructure Protection Plan. The agency's initial focus was on raising cybersecurity awareness and performing outreach to the various transportation modes, including pipelines.[32] The Interstate Natural Gas Association of America maintains its own extensive cyber security guidelines for natural gas pipeline control systems.[33] The American Petroleum Institute likewise maintains an industry standard for oil pipeline control system security.[34] Pipeline operators have scheduled participation in DHS-sponsored control systems cybersecurity training and also participate in the DHS Industrial Control Systems Joint Working Group.[35]

In addition to these efforts, 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.[36] Sandia Laboratories also performs authorized, defensive cybersecurity assessments for government, military, and commercial customers through its Information Design Assurance Red Team (IDART) program.[37]

---

[29] Transportation Security Administration (TSA), *Pipeline Security Guidelines*, April 2011, pp. 16-19, and *Pipeline Security Smart Practice Observations*, September 19, 2011, pp. 4-8.

[30] 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.

[31] Department of Homeland Security, U.S. Computer Emergency Readiness Team, *Control System Security Program (CSSP)*, web page, February 27, 2012, http://www.us-cert.gov/control_systems/index.html.

[32] Jack Fox, General Manager, Pipeline Security Division, Transportation Security Administration (TSA), personal communication, February 22, 2012.

[33] Interstate Natural Gas Association of America (INGAA), *Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry*, Washington, DC, January 31, 2011.

[34] American Petroleum Institute, *Pipeline SCADA Security*, Second Edition, API Std. 1164,Washington, DC, June 2009.

[35] TSA, February 22, 2012.

[36] U.S. Department of Energy, "National SCADA Test Bed," Web page, July 12, 2012, http://energy.gov/oe/national-scada-test-bed.

[37] Sandia National Laboratories, "The Information Design Assurance Red Team (IDART)," Web page, 2009, http://idart.sandia.gov/.

Adequacy of Voluntary Pipeline Cybersecurity

Although Congress has been concerned about various issues related to U.S. pipeline security in recent years, a key subject of debate is the adequacy of 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.[38]

Although the IG report did not elaborate on this recommendation, covert testing of vulnerabilities would likely include testing of cybersecurity measures 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[39] and the Cybersecurity Act of 2012 (S. 2105) both would mandate the promulgation of cybersecurity regulations for pipelines, among other provisions. A revised version of S. 2105, S. 3414, would permit the issuance of regulations but would focus on the use of voluntary cybersecurity measures. S. 3414 would not necessarily confer upon TSA any authority it does not already have to regulate pipeline cybersecurity.

In contrast to the IG's conclusions and the legislative proposals above, the pipeline industry has long expressed concern that security regulations, presumably including cybersecurity, could be "redundant" and "may not be necessary to increase pipeline security."[40] Echoing this sentiment, a DOT official testified in 2007 that enhancing security "does not necessarily mean that we must impose regulatory requirements."[41]

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. 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.[42] 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

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

[39] 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.

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

[41] 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.

[42] 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.

security assessments. Because TSA believes the most critical U.S. pipeline systems generally meet or exceed industry security guidance, the agency believes it achieves better security with voluntary guidelines, and maintains a more cooperative and collaborative relationship with its industry partners as well.[43]

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.[44]

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 TSA believes its voluntary approach to pipeline security is adequate, Canadian pipeline regulators have come to a different conclusion. In 2010 the National Energy Board of Canada mandated security regulations for jurisdictional Canadian petroleum and natural gas pipelines, some of which are cross-border pipelines serving export markets in 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.[45] 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.

TSA Pipeline Cybersecurity Resources

An important consideration in TSA's approach to pipeline security is its staff resources. At its current staffing level of 13 full-time equivalent employees, TSA's Pipeline Security Division (PSD) has limited capabilities. (By comparison, the DOT is authorized for up to 145 federal inspection and enforcement personnel for the U.S. pipeline safety program, and also formally draws upon over 400 state pipeline safety inspectors.) Furthermore, none of the PSD staff have

[43] Jack Fox, General Manager, Pipeline Security Division, Transportation Security Administration (TSA), Remarks before the Louisiana Gas Association Pipeline Safety Conference, New Orleans, LA, July 25, 2012.

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

[45] 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.

the specialized computer system expertise needed to support more extensive cybersecurity activities, although such expertise is available in other TSA divisions.[46]

Congress has long been concerned about staff resources available to implement the nation's pipeline security program. For example, as one Senator 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."[47] At a congressional field hearing in April 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.[48] TSA focuses its security inspections on only the 100 largest pipeline and distribution system operators in an effort to make the best use of its limited resources. However, there are questions as to whether the agency as currently structured could develop and implement new security regulations, conduct rigorous security plan verification, and pose a credible threat of enforcement. Developing specific cybersecurity regulations would pose a particular challenge as the PSD has limited existing capability to do so.

Conclusions

While the pipelines sector has many cybersecurity issues in common with other critical infrastructure sectors, it is somewhat distinct in several ways:

- Pipelines in the United States have been the target of several confirmed terrorist plots and attempted physical attacks since September 11, 2001.
- Changes to pipeline computer networks over the past 20 years, more sophisticated hackers, and the emergence of specialized malicious software have made pipeline SCADA operations increasingly vulnerable to cyber attacks.
- There recently has been a coordinated series of cyber intrusions specifically targeting U.S. pipeline computer systems.
- TSA already has statutory authority to issue cybersecurity regulations for pipelines if the agency chooses to do so, but may not have the resources to develop, implement, and enforce such regulations if they are mandated.

TSA maintains that voluntary cybersecurity standards have been effective in protecting U.S. pipelines from cyber attacks. Based on the agency's corporate security reviews, TSA believes cybersecurity among major U.S. pipeline systems is good. However, without formal cybersecurity plans and reporting requirements, it is difficult for Congress to know for certain. To a great extent, the public must therefore rely on the pipeline industry's self-interest to protect itself from cyber threats. Whether this self-interest is sufficient to generate the level of cybersecurity appropriate for a critical infrastructure sector, and whether imposing formal regulations would be counterproductive, is open to debate. Faced with this uncertainty, legislators are forced to rely

[46] TSA, July 25, 2012.

[47] Senator 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.

[48] 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.

upon their own best judgment to reach conclusions about the federal pipelines cybersecurity program. If Congress concludes that current voluntary measures are insufficient to ensure pipeline cybersecurity, it may decide to provide specific direction to TSA to develop regulations and provide additional resources to support them, as such an effort may be beyond the TSA Pipeline Security Division's existing capabilities.

Author Contact Information

Paul W. Parfomak
Specialist in Energy and Infrastructure Policy
pparfomak@crs.loc.gov, 7-0030