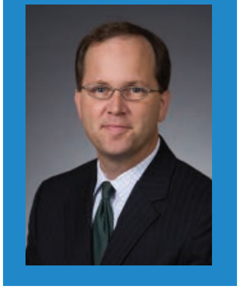
Pipeline & Gas Journal
connecting you to the pipeline industry worldwide



Improving Pipeline Cybersecurity with Public-Private Partnerships

By **Andrew R. Lee, Jones Walker LLP,** New Orleans

From an environmental, safety, and health perspective, pipelines are widely considered the optimal mode of transporting fossil fuel products. Release failures and loss-of-life incidents remain on a downward trend that began decades ago.

But with over 2.5 million miles of pipelines moving natural gas, refined petroleum products, ethanol, chemicals, and other liquids, the U.S. oil and gas infrastructure also presents an array of high-value targets to technologically sophisticated terrorist groups and foreign state actors.

After the false starts and failures of separate industry- and government-led efforts to improve the cybersecurity framework, public-private cybersecurity partnerships that follow the guidelines published by the National Institute of Standards and Technology (NIST), a non-regulatory agency of the Department of Commerce, have emerged as the best hope for broad-based implementation of an effective defense against cyber-threats.

A Trailing Response

Since private companies own the vast majority of pipeline infrastructure, they are also responsible for all aspects of pipeline safety, subject to federal and state regulations. Owners generally rely on automated monitoring and control systems, otherwise known as Supervisory Control and Data Acquisition (SCADA) industrial control systems (ICS) to manage unmanned facilities. Given the lack of standardization of SCADA systems, however, private owner-operators that have sub-par cybersecurity defense systems present attractive opportunities for hackers intent on launching large-scale attacks.

Awareness of this threat to U.S. pipelines began reaching the public consciousness only in recent years, following a series of attempted and successful cyberattacks. First, in March 2012, the U.S. Department of Homeland Security (DHS) revealed that an active "spear-phishing" campaign had targeted the natural gas pipeline industry. (Spear-phishing is a specific type of "phishing" in which an email that appears to be from a known acquaintance or colleague, but it is in fact from a criminal hacker, attempts to entice the recipient to click a link that will deploy malware designed to steal data and hijack computers.)

A report compiled by the DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) confirmed that targeted attempts and intrusions into multiple natural gas pipeline owners' SCADA systems had begun several months earlier. Analysis of the malware and artifacts of the successful breaches indicated that the cyber threats were all related to a single campaign that targeted personnel with emails designed to appear as if they had been sent from someone within their respective companies.

A DHS study confirmed that the campaign targeted 23 gas pipeline companies and stole sensitive operational and technical data sufficient to give the cyber thief sufficient insider knowledge to blow up many compressor stations simultaneously. A report prepared by the independent cybersecurity consulting firm Mandiant and published in February 2013 fingered an arm of the Chinese People's Liberation Army as the likely culprit.

In early 2013, a number of pipeline gas compressor stations were the targets of "brute force" attempts to compromise their networks. In each case, it was determined that the victims' SCADA systems were connected to the public internet. The targets had ignored long-published government and industry recommendations that SCADA systems not be internet-facing.

Iranian hackers also have actively attacked U.S. energy systems. In 2013, the *Wall Street Journal* reported that Iran-based hacker-agents were able to gain access to critical infrastructure, including SCADA systems, before they were detected and the systems were salvaged. The hackers were believed to have taken advantage of the fact that the systems were internet-facing.

Finally, in early 2013, *Infosecurity Magazine* reported that a Russian hacker group going by the name "Energetic Bear" caused significant disruption to U.S. energy companies, including petroleum pipeline operators. The group used a highly effective malware to break into the targets' SCADA systems. Once the malware infected a company's ICS, it then relayed the sensitive company data and information back to the hackers.

These are not the only examples of attempted hacking of pipeline systems. Despite these clear red flags, however, a 2014 DHS survey revealed that 82,000 known ICS hardware or software systems (including SCADA systems) were directly accessible from the public internet, making those systems particularly vulnerable to cyberattacks.

Cyberattacks could not only be responsible for damaging explosions, but they could also interrupt the flow of natural gas to electricity-generating power plants, resulting in widespread blackouts. Multiple publicly traded pipeline companies regularly disclose these risks in SEC filings. One reported experiencing "ongoing, often sophisticated, cyberattacks by a variety of sources with the apparent aim to breach our cyber-defenses."

The reporting company further explained that a security breach could negatively impact the reliability of its transmission and storage systems as well as subject the company "to harm associated with theft or inappropriate release of certain types of information such as system operating information."

Going Solo

In 2012, the *Christian Science Monitor* reported that an earlier industry effort to defend pipeline SCADA infrastructure had been scuttled. The report focused on a 2006 initiative that had the goal of creating a powerful encryption system to shield pipeline compressors, substations, and other pipeline infrastructure from cyberattack, and which had self-destructed on the eve of its rollout.

Sponsored by the American Gas Association and led by William Rush, a now-retired scientist formerly with the Gas Technology Institute, the five-year AGA-12 effort charged the AGA 12 Cryptography Working Group with developing a suite of open standards designed to protect data transmitted by SCADA systems, authenticate the originators of messages on SCADA systems, and to ensure data integrity.

That effort failed, however, but recently the AGA announced that it would adopt the TSA's voluntary Pipeline Cybersecurity Guidelines (promulgated in 2011) and the NIST framework (2015). Its members who are actively addressing cybersecurity challenges will find that antiquated legacy SCADA systems are not easily adaptable to a critical path leading to a successful cybersecurity program.

At the federal level, recent regulatory efforts have had poor results.

Months after the Chinese PLA attack, Congress attempted to pass legislation mandating cybersecurity regulations for privately owned critical infrastructures, including pipelines. The bill, however, failed in the Senate, prompting one if its sponsors, former U.S. Sen. Joe Lieberman (D-CT), to remark, "This is one of those days when I fear for our country. We've got a crisis, and it's one that we all acknowledge. It's not just that there's a theoretical or speculative threat of cyberattack against our country – it's real."

Shortly thereafter, chairman of the House Committee on Homeland Security Rep. Michael McCaul (R-TX), also lamented the lack of statutory and regulatory mandates. He highlighted the threat posed by China, which, according to a 2014 Internet Security Alliance report, was targeting via remote access more than 60% of oil and gas pipelines in North America.

Cyber-Partnerships

Frustrated by Congress's failure to pass comprehensive cybersecurity legislation, President Obama issued Executive Order 13636 in early 2013. In the order, the president directed NIST to follow a public-private approach and develop a set of voluntary cybersecurity guidelines for use by companies managing critical infrastructure, including those in the oil and gas industry. Over the next 12 months, NIST solicited extensive input from industry, academia, and sector-focused government agencies and, in February 2014, released the "Framework for Improving Critical Infrastructure Cybersecurity."

The NIST Framework is a set of practices, standards, and guidelines created to help critical infrastructure owners and operators manage cyber-risks and defend against cyber-threats. The guidelines are strictly voluntary, and it has been difficult to determine with reasonable certainty how widely they have been adopted in key business segments. The framework also has been criticized for failing to meet President Obama's directive that it incorporate cost-effectiveness as a key component.

Despite these challenges, the campaign to encourage adoption of the NIST Framework has been an active one. In early 2014, shortly after NIST issued the framework, DHS announced its Critical Infrastructure Cyber Community Voluntary Program (or the C-cubed (C^3) Voluntary Program). The key goals of this program have been to support cyber resiliency, increase use of the Framework, and encourage businesses to manage cybersecurity as part of an all-hazards approach to enterprise risk management."

In January 2017, NIST published a draft update and, as of this writing, continues to solicit public comment. The draft "Version 1.1" delves deeper into the business of managing cyber supply chain risks and introduces new cybersecurity measurement methods. When finalized, the update will serve to benefit those businesses that are serious about adopting fortified cybersecurity defenses.

Encouragingly, the pipeline industry has taken meaningful steps to embrace the NIST Framework. Its LNG trade group has also announced the formation of an industry threat-sharing center, the Downstream Natural Gas Information Sharing and Analysis Center (DNG ISAC). The DNG ISAC represents a recognition that "a meaningful partnership between the private sector and the federal and state governments is the key to addressing cybersecurity threats to our nation's critical infrastructure."

The enactment of the Cybersecurity Information Sharing Act of 2015 (CISA) has put the public-private model to the test. Passed in part as a response to North Korea's notorious hack of the cyber assets of Sony Pictures Entertainment, CISA is designed to create a voluntary cybersecurity and cyber-threat information-sharing process to further encourage public-private sharing of cyber-threat information by removing legal barriers and the threat of litigation.

For a private entity, CISA offers private entities certain liability protections related to monitoring information systems and disclosures of information, if the entities follow DHS's guidance, published in June 2016.

Industry reaction to CISA prior to the release of the DHS Guidance in June 2016 was lukewarm, with leaders indicating a desire for increased transparency in DHS's process and more clarity as to what mutually beneficial participation would look like. But most observers saw the tide turn in mid-2016 toward more cooperation for the shared goal of greater security.

Before We Sleep

Four years after Executive Order 13636 was issued, an anti-cyberattack infrastructure that protects SCADA systems throughout the nation's pipeline network remains slow to materialize. During this time, a number of legislative and regulatory initiatives have been proposed or launched, but none have reached full maturity or achieved their stated objectives.

For example, while the TSA has established the National Cybersecurity and Communications Integration Center (NCCIC), the stated mission of which is to reduce the likelihood and severity of incidents that may significantly compromise the security and resilience of the nation's critical information technology and communications networks, its inspection workforce is widely reported to be inadequate. The TSA will have difficulty fulfilling its duty of inspecting interstate gas pipeline cybersecurity when, as is widely known, the TSA division responsible for this critically important job is severely understaffed.

The completely separate Department of Transportation (DOT) Pipelines and Hazardous Materials Safety Administration (PHMSA) oversees the including implementation and enforcement of the Pipeline Safety Act of 2016 (PIPES Act), which requires DOT to propose regulations that enact cybersecurity measures for such pipelines and mandates that the DOT secretary prescribe minimum operating and maintenance standards for LNG pipeline facilities, including consideration of cybersecurity measures. Despite this charge, PHMSA's most recent strategic plan fails to make any mention of cybersecurity, and the agency has been slow to respond to the PIPES Act.

Security Under Trump

Shortly after taking office in January 2017, President Trump signed an executive order severely restricting the issuance of new federal regulations, specifically by requiring that government agencies must eliminate two existing regulations for every one "new" rule they propose. He separately issued a federal agency hiring freeze which has resulted in confusion about impact on unstaffed cybersecurity positions. It remains to be seen whether such measures will negatively impact efforts of agencies that are tasked with regulating privately owned critical infrastructure, including pipelines.

It seems unlikely that the current administration will adopt proposals advocating expansion of government in this critical area (for example, the recent UC Berkeley Center for Long-Term Cybersecurity's suggestion that Congress create a new agency to combine government and private-sector cybersecurity efforts in a single space.)

Time will tell if the public-private cybersecurity partnerships, first proposed and implemented by the Obama administration, and widely adapted by industry leaders as a necessary approach to effective pipeline safety, will hold up during the Trump presidency. The alternative – government-mandated compliance and uniformity – is unlikely to see daylight, so that public-private cooperation is the only viable path to ensuring the security of the nation's pipeline infrastructure against cyberattacks. *P&GJ*

Andrew R. Lee

Partner, Jones Walker LLP

201 St. Charles Ave, Ste 5100, New Orleans LA 70170

alee@joneswalker.com

T: 504.582.8000