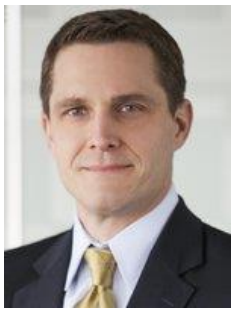
Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Coming Soon: More Federal Action On Pipeline Cybersecurity

By **Arjun Ramadevanahalli, Levi McAllister and Lewis Csedrik**
(December 19, 2019, 4:43 PM EST)

Arjun Ramadevanahalli

Levi McAllister



Lewis Csedrik

Over the past few years, headlines have drawn more attention to the troubling trend of cyberattacks on critical energy infrastructure. Those attacks have taken various forms, and have presented different degrees of risk.

Publicly available reports have detailed attacks that disrupted everything from communication networks used to monitor remote power generation sites to scheduling and billing services used by natural gas utilities. And recent FBI reports have cautioned that state-sponsored hackers are targeting critical energy infrastructure operators with what appear to be longer-term infiltration or reconnaissance campaigns.

These continued attacks have created a heightened focus on the cyber threats facing the pipeline industry. The nation's pipeline infrastructure spans millions of miles, and is used for the interstate transportation and intrastate distribution of natural gas, oil, fuels and other hazardous liquids. These pipeline systems are vital for supporting other critical sectors, such as the electric industry that relies increasingly on natural gas supplies for large-scale power generation and grid stabilization.

Cyberattacks on the nation's pipeline system could disrupt operations, resulting in an energy emergency or safety-significant event. Not surprisingly, the destructive potential of these types of attacks has raised the profile of pipeline cybersecurity for federal government and industry stakeholders alike.

Below, we discuss recent trends in federal efforts to oversee pipeline cybersecurity, and potential challenges facing the industry as those efforts progress.

What the Federal Government Is Doing Now

Coordinated federal efforts to protect critical infrastructure have existed for years, but federal regulatory oversight of the nation's pipeline cybersecurity has remained relatively static. Although a variety of federal entities have participated in efforts to secure pipelines, there is currently no mandatory regulatory regime or a clear lead agency to oversee pipeline cybersecurity.

However, as cyber risks facing critical infrastructure continue to expand globally, a growing chorus of voices within the industry and the federal government is calling for more integrated action to guard pipeline infrastructure against cyber threats.

This has resulted in stakeholders and federal officials taking a harder look at the current regulatory framework, the operational and safety impacts of cybersecurity risks, and the benefits of cross-sector collaboration and industry cooperation in preparing for a cyber incident response.

Scrutiny of Existing Programs

Currently, the primary federal program governing pipeline cybersecurity is administered by the U.S. Transportation Security Administration. The TSA's Pipeline Security Guidelines contain voluntary security measures (e.g., implementing a corporate security program, steps to identify and assess critical facilities) applicable to natural gas and hazardous liquid transmission pipeline systems, natural gas distribution pipeline systems and liquefied natural gas facility operators.

The TSA last revised the Pipeline Security Guidelines in March 2018 to reflect changes in the pipeline operating environment, and to incorporate some of the critical infrastructure cybersecurity practices issued by the National Institute of Standards and Technology, or NIST.

In a December 2018 report, the Government Accountability Office issued a report identifying weaknesses in key aspects of the TSA's pipeline security program related to cybersecurity, such as the lack of a process to regularly update the guidelines or assess their efficacy. The report also suggested that the TSA has not maintained an adequate level of cybersecurity subject matter expertise within the organization.

Another GAO report, issued in June 2019, concluded that the TSA's security incident response plan was outdated, noting that it does not identify the cybersecurity roles and responsibilities of other relevant federal agencies, including the U.S. Department of Energy and the Federal Energy Regulatory Commission, or the establishment of the Cybersecurity Infrastructure and Security Agency, or CISA, within the U.S. Department of Homeland Security.

Similarly, the GAO report also examined the TSA's coordination of security-related efforts with the Pipeline and Hazardous Materials Safety Administration, or PHMSA, and recommended that the TSA and PHMSA develop and implement a timeline for reviewing an earlier 2006 memorandum of understanding, which identifies their agreed-upon roles and responsibilities in the area of pipeline security.

As noted in the GAO report, the memorandum of understanding has not been reviewed to consider pipeline security developments since its inception. Although the TSA is considered the lead agency over pipeline security, PHMSA also remains responsible for ensuring pipeline safety, which security-related events can impact.

In this regard, PHMSA's Office of the Inspector General recently initiated an audit to assess PHMSA's efforts to foster a positive safety culture. It remains to be seen, however, whether the audit considers the relationship between cybersecurity and a strong safety culture.

In response to the two GAO reports, the TSA agreed to address all of the GAO's recommendations, but various federal stakeholders have called for stricter action on pipeline cybersecurity over the past year.

In February, FERC Chairman Neil Chatterjee testified before the Senate Committee on Energy and Natural Resources that more work is needed to improve the TSA's oversight of pipeline cybersecurity. And in November, FERC staff members announced that the agency's new strategic focus areas will encompass security controls for natural gas pipelines, because disruption of pipelines could pose a significant impact on the bulk electric system.

Members of Congress have echoed similar concerns. For example, this past summer, members of the House Committee on Energy and Commerce expressed concerns about the gaps identified in the GAO's December 2018 report, with one House member suggesting that the DOE, and not the TSA, should take responsibility for fillings those gaps.

Focus on Cross-Sector Impacts and Coordination

In the energy industry, a catastrophic cyber event affecting the reliability of the interstate gas pipeline network could create a devastating ripple effect. The loss of critical natural gas supplies could result in widespread power outages and lead to cascading failures in other critical sectors, forcing those sectors to operate in a degraded state for an extended period of time.

In light of those concerns, federal entities are placing an increasing focus on interagency coordination and private industry cooperation in order to prepare for responses to such large-scale emergencies. For example, the TSA, the DOE and DHS (with the CISA) partnered together to launch the Pipeline Cybersecurity Initiative, a cooperative program that leverages each agency's expertise to mitigate risks to pipeline infrastructure.

DHS recently established a Tri-Sector Executive Working Group that links senior representatives from the finance, communications and electric power industries with senior DHS, DOE, and U.S. Department of the Treasury officials to coordinate intelligence sharing and assess cross-sector risks.

In addition, this year's Grid Security Exercise — a massive, cross-sector security exercise coordinated every two years by the North American Electric Reliability Corporation, or NERC — emphasized the electric sector's reliance on natural gas pipeline supplies.

Potential Challenges as the Industry Looks Ahead

As coordinated federal efforts to oversee cyber threats to pipelines begin to take shape, private industry participants may want to consider the following challenges.

Preparing for Mandatory Standards

It is unclear whether Congress will take action to authorize the TSA or another agency to impose mandatory cybersecurity standards on the pipeline industry. As noted above, some on Capitol Hill believe that responsibilities for pipeline cybersecurity oversight should be shared, and have introduced legislation to accomplish just that.

While they could be years away, legislation and agency regulations may ultimately take cues from cybersecurity measures that exist today. Therefore, it may be a worthwhile exercise for pipeline operators to consider the cybersecurity programs used in other industrial sectors.

For example, future mandatory standards could require the implementation of a program that generally

aligns with leading cybersecurity guidelines (such as NIST's Cybersecurity Framework, or the ISO/IEC 27000 series of standards) or they could be more prescriptive and require specific controls (like the NERC CIP standards, which rely heavily on implementing controls based on the criticality of in-scope facilities).

In the meantime, existing controls should allow operators to mature their practices, policies and procedures to not only maintain a sound cybersecurity posture, but to also adapt to future regulatory action. Operators should also consider the relationship between cybersecurity and pipeline safety to ensure operational programs and safety policies address the possibility of cyberattacks and other security-related events that could impact safety.

Managing the Cyber Risks of New Technologies

Pipelines can present unique technical challenges to owners and operators, who are tasked with managing widespread systems that rely on infrastructure that can be over a century old. Cybersecurity risks complicate those challenges, especially as new technologies are used to update pipeline control system networks.

For example, many energy industry participants are turning to cloud-based solutions to provide operational and administrative efficiencies. Cloud services enable operators to leverage powerful remote computing power to run their operational applications while achieving cost savings at the same time. However, cloud services can present their own set of security risks if operators are required to not only entrust third-parties with critical applications and information, but to also ensure the confidentiality of that data in motion.

Similarly, the use of distributed internet of things devices, such as sensors, can help provide operators maintain situational awareness through a more granular understanding of pipeline operations and system health. On the other hand, the large number of interconnected internet of things devices can provide malicious actors with a significantly larger attack surface.

Pipeline operators should pay particular attention to managing these cybersecurity risks as they modernize or update their systems, especially if future regulatory controls have not been adapted to reflect the industry's use of new technologies.

Recovery of Capital Investment Costs

Any decisions requiring the expenditure of monies to fund the development, implementation, construction or operation of cybersecurity-related policies, procedures or control systems will undoubtedly raise questions about who is responsible for the costs.

Depending on the extent to which a federal agency (or agencies) mandates mandatory standards or otherwise directs pipeline operators to implement pipeline cybersecurity safeguards, the requisite costs associated with compliance can be substantial. Mechanisms for recovery of associated costs are likely to vary, depending on the pipeline at issue that is incurring the costs associated with compliance.

For example, FERC's modernization cost recovery policy statement issued in 2015 permits interstate natural gas pipelines to establish a surcharge or tracker mechanism to recover certain safety, environmental or reliability capital expenditures made to modernize pipeline system infrastructure outside of a Natural Gas Act, or NGA, Section 4 rate case.

Pipelines seeking to utilize the tracker must satisfy certain criteria laid out by FERC, including the criterion that the pipeline be able to demonstrate that the incurred costs are eligible costs, as defined under the policy statement and subsequent precedent. In the event that a pipeline were able to satisfy the five criteria with respect to costs incurred in connection with pipeline cybersecurity compliance, the interstate pipeline could recover costs from ratepayers.

However, pipelines not subject to FERC's NGA rate regime cannot avail themselves to the policy. For those pipelines, cost recovery mechanisms could potentially be sought through state regulatory approval processes — depending on the state in which the pipeline operates and the applicable rules there.

Conclusion

Addressing cybersecurity risks to critical infrastructure will continue to be a priority for policy makers and agency officials. Undoubtedly, efforts to mitigate those risks in the pipeline industry will be subject to further scrutiny, given the importance of pipeline operations to other critical sectors and the absence today of mandatory controls and a clear, lead cybersecurity regulator.

Amid these shifting sands, pipeline operators should continue to consider the challenges outlined above to prepare for heightened federal cybersecurity oversight, which may not be far off.

Arjun P. Ramadevanahalli is an associate, and Levi McAllister and Lewis M. Csedrik are partners at Morgan Lewis & Bockius LLP.