E&E News

Battle lines form over pipeline cyberthreat

Blake Sobczak, E&E News reporter **Published: Thursday, July 25, 2019**

A natural gas well pad in northern Pennsylvania. Blake Sobczak/E&E News

Under pressure to ensure U.S. oil and gas pipelines don't fall prey to hackers and pose a threat to public safety, lawmakers on Capitol Hill are puzzling over which agency should have cyber oversight.

Among the questions: Does the Department of Energy, with its depth of expertise and new cybersecurity office, fit the bill? What about the Pipeline and Hazardous Materials Safety Administration, which already inspects pipeline safety and is up for reauthorization in Congress — a prime opportunity to shuffle authorities? Where goes the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, with its stable of experts versed in the complexities of energy control systems? Or does pipeline security oversight deserve to stay at the Transportation Security Administration, which, despite a staff of six people, has overseen a period of relative cyber stability for U.S. oil and gas operators?

"It's a political football," said Marco Ayala, senior life-cycle solutions manager at aeSolutions in Houston, who often works with pipeline companies on their cybersecurity practices. "DOE's point is that they're moving the ball forward with cybersecurity. Yet TSA and PHMSA are the law of the land for pipelines."

Many pipeline companies already deal with DOE across various other parts of their businesses, he pointed out. "For them, it's just, 'Tell us who to talk to.'"

Top intelligence and homeland security officials have warned that new reliance on digital controls, online threats from adversaries like China and Russia, and cybersecurity workforce shortages collectively pose a huge risk to the hundreds of thousands of energy pipelines crisscrossing the nation. Though cyberattacks on control systems are extraordinarily rare, researchers have shown how pipeline networks could be disrupted by skilled hackers, potentially harming other sectors or even resulting in leaks or explosions.

A Department of Homeland Security office in Washington, D.C. GAO

Dan Coats, director of U.S. national intelligence, warned in a threat assessment early this year that China has the ability to bring down an American gas pipeline for "days to weeks" through cyber means. Pipeline operators later said they had not received word of a specific threat from Coats or other top national security officials.

"As more of the risks become well-publicized, to the extent that they're not being addressed, that creates a poor defense for any potential litigator," said David Katz, partner at the Adams and Reese LLP law firm. "My sense is that the industry would welcome some very clear guidance on some of these issues."

A cyberattack isn't known to have disrupted the flow of oil or gas anywhere in the United States. However, hackers crashed the networks of a third-party pipeline vendor early last year, forcing many major utilities to revert to alternate billing and scheduling services for their gas deliveries (***Energywire***, April 6, 2018).

The debate over how to lower the risks is revving up on Capitol Hill as lawmakers on both sides of the aisle have variously drafted legislation to cement TSA's oversight — or slammed that agency's handling of the issue. The outcome could change how pipeline operators do business and shape digital defenses for a cornerstone of U.S. energy infrastructure.

The security of U.S. natural gas transmission lines has come under particular scrutiny, given the electricity sector's growing reliance on the fuel for power generation. Grid officials at the North American Electric Reliability Corp. have floated the possibility of extending mandatory cybersecurity and physical security rules to gas utilities, many of which have electricity businesses that must already comply with NERC's Critical Infrastructure Protection Committee standards.

The natural gas industry, led by groups like the American Gas Association, American Petroleum Institute and Interstate Natural Gas Association of America, has pushed back against potential cybersecurity regulations. Gas utilities claim that prescriptive rules aren't suited to address fast-moving cyberthreats and that the danger to their infrastructure is distinct from that to the power grid, where conditions can change in fractions of a second. The gas industry has generally favored TSA to stay at the helm, citing progress from a new "Pipeline Security Initiative" looping in DHS and DOE, as well as a memorandum of understanding delineating PHMSA's role vis-a-vis TSA.

Lawmakers aren't so sure. At a hearing earlier this month Rep. Frank Pallone (D-N.J.), chairman of the House Energy and Commerce Committee, said he "remain[s] concerned about the lack of resources and expertise at the Transportation Security Administration's Pipeline Security Program. I look forward to hearing from DOE about possible ways they could help address these safety gaps."

He added that "if TSA continues to devote scant resources or attention to these matters, we must start looking at other options to keep our pipes secure."

A slew of bills

TSA officials have pushed back against the notion that they've put pipeline cybersecurity on a backburner, despite a sharply worded report from the Government Accountability Office last December that called the regulator's priorities into question (***Energywire***, Dec. 20, 2018). In a letter this March to Sen. Maria Cantwell (D-Wash.), who pressed the issue while serving as ranking member for the Senate Energy and Natural Resources Committee last year, TSA Administrator David Pekoske laid out his agency's efforts to check up on pipeline operators' most critical computer systems.

"Although there may be some challenges, it is my assessment that TSA's oversight of pipeline security is sound, and I am proud we have been able to work with pipeline stakeholders in a voluntary environment to improve the security posture of the industry," he said, adding that he had heard from "multiple" CEOs who "affirmed the same to me." He pointed out that TSA had assessed 44 out of the 53 pipeline companies that operate the top 100 systems in the country prior to 2019 and would continue ramping up voluntary security reviews of the most critical pipeline networks, ranked by a rubric that accounts for their connections to gas-fired power plants.

TSA's assurances have won over several key lawmakers now pushing to keep pipeline security authority at the agency, which is better-known and -funded for its role in U.S. airports.

Rep. Debbie Lesko (R-Ariz.). U.S. Congress

Arizona Rep. Debbie Lesko, the top Republican on the House Homeland Security Subcommittee on Transportation and Maritime Security, has called securing pipeline networks a "critically important task" and sought additional authority for TSA's pipeline program, including a legal basis for borrowing personnel from other DHS agencies.

She attached an amendment to H.R. 3699, the "Pipeline Security Act," which would formalize and augment TSA's cybersecurity role. The **legislation**, introduced by Rep. Emanuel Cleaver (D-Mo.) and co-sponsored by Rep. Van Taylor (R-Texas), won key approval from the full Homeland Security Committee earlier this month, teeing up the chance for a full vote in the House.

Lesko said she hopes the legislation "will strengthen pipeline transportation security by reasserting many of the positive aspects of TSA's pipeline security program."

"These aspects include reaffirming the voluntary nature of certain risk assessments and encouraging meaningful stakeholder engagement in establishing pipeline security guidelines," she added in a statement.

Another bill from Reps. Fred Upton (R-Mich.) and David Loebsack (D-Iowa) would shift some gas pipeline focus to DOE, by directing the agency "to establish policies and procedures to coordinate federal agencies, states, and the energy sector" handling of gas distribution and transmission security. That legislation, **H.R. 370**, would also authorize Energy Secretary Rick Perry to "develop, for voluntary use, advanced cybersecurity applications and technologies for natural gas pipelines." The bill passed the Energy and Commerce Committee by voice vote earlier this month (***Greenwire***, July 17).

'Seriously damaged'

Outside the halls of Congress, DOE has **sought to collect** additional information from oil and gas pipeline operators on their physical and operational resilience.

"Many oil and natural gas companies, pipeline operators, fuel distribution and delivery firms, and other owners and operators of oil and natural gas infrastructure, as well as the government agencies that regulate them in some respect, are seeking cost-effective ways to make these infrastructure systems more resilient against cyber and physical threats as well as severe weather events," DOE noted in its request for information published July 9.

Experts at the ratings and analytics firm Moody's also have welcomed the added focus on gas pipeline security both in Congress and among federal agencies, calling the development credit positive for both electric utilities and gas pipeline companies in a research note this month.

The Moody's Investors Service report slammed "weak" government oversight, citing TSA's use of "only six full-time employees" to monitor physical and cybersecurity across all major hazardous materials pipelines.

"It just seemed like a very ambitious mandate for a very small team," said Moody's analyst and Assistant Vice President Lesley Ritter, the lead author of that report, in an interview.

Though mandatory requirements would add new costs for pipeline companies accustomed to voluntary oversight, baseline rules would help fill "gaps" in defenses likely to exist at some companies, according to Moody's.

Ritter said she expects mandatory rules would help fend off hackers, ensuring pipeline companies reap "longer-term reliability benefits of having an asset that's operating, versus one that could potentially be seriously damaged."

Katz of the Adams and Reese law firm called the GAO report "pretty compelling" in its indictment of TSA's ability to handle the risk on its own.

"Should some of this authority be transferred, maybe, to other agencies?" he said. "There's just no strategic work plan."

Multiple legal and industry sources said some gas pipeline operators have begun to implement comprehensive cybersecurity protections, not only to protect their networks but also to ease the transition to a mandatory oversight regime, should one emerge from Congress, DOE or even the independent Federal Energy Regulatory Commission. FERC has recently pushed to beef up supply chain safeguards for the bulk power grid, directing NERC to add new mandatory cybersecurity standards for utilities, rules that suppliers say are adding de facto requirements to their own cybersecurity programs.

"We'll see it continue to evolve from a more reactionary system to one that's proactive, as people look at the risk and look at the potential regulation," said Adams and Reese associate Adam Griffin, who works with energy companies along the Gulf Coast, and who with Katz recently authored an analysis of cyber risks to the oil and gas sector.

"Companies of all sizes — even your small operators — are going to shift to a more proactive methodology."

Ayala credited pipeline companies with improving their cyberdefense in recent years, while warning that some firms may be sweating a DOE takeover if they haven't updated their systems.

But for the larger firms he typically works with, "They're doing what they can from a security standpoint, they're assessing their systems, they're deploying best standards," he said. "Whether it's PHMSA, TSA or DOE — what is it going to mean for the private asset owners? 'Now I just need to send my letters somewhere else.'"

Reporter Jeremy Dillon contributed.