Insight

Pipeline Security

EWELINA CZAPLA | MAY 21, 2021

Executive Summary

- The Pipeline and LNG Facility Cybersecurity Preparedness Act was reintroduced in the House of Representatives in response to the cyberattack on Colonial Pipeline's facilities.
- The bill would create a new program within the Department of Energy to oversee the development of coordination procedures, technology and tools, and demonstration projects that industry may voluntarily adopt.
- The bill fails to directly address the issue at hand—a lack of cybersecurity standards—while creating new government tools that duplicate private-sector technology.

Introduction

Last week, the pipeline operating company Colonial Pipeline shut down service following a cyberattack. Colonial Pipeline operates over 5,000 miles of pipeline that carry gasoline, diesel fuel, and jet fuel. Colonial's accounting system was subject to a ransomware attack that led the company to halt the physical operation of its pipeline, resulting in fuel shortages along the Eastern Seaboard. The pipeline's service was fully restored about a week later, but only after 16,000 filling stations failed to receive fuel.[1]

In response to the cyberattack, the U.S. House Committee on Energy and Commerce reintroduced bipartisan legislation, the Pipeline and LNG Facility Cybersecurity Preparedness Act, which would create a new office to addresses pipeline security at the Department of Energy (DOE).[2] (The bill was initially introduced in 2019 but did not receive a vote.[3]) The bill fails to directly address the larger issue at hand: Cybersecurity is an issue throughout critical infrastructure, not just in pipelines, and a narrowly targeted bill

doesn't address this broad vulnerability. The bill would, however, create new government tools that duplicate other, ongoing government efforts and private-sector technology.

More Regulatory Oversight of Pipeline Safety

The Pipeline and LNG Facility Cybersecurity Preparedness Act applies to natural gas pipelines, including natural gas transmission and distribution pipelines, hazardous liquid pipelines, and liquefied natural gas (LNG) facilities. The Department of Transportation's Pipeline and Hazardous Materials Safety Administration (PHMSA) is currently tasked with maintaining the safety of pipelines, and it administers both compliance and enforcement programs for natural gas and hazardous liquid transportation pipelines and LNG facilities.[4] PHMSA maintains a national pipeline safety inspection and enforcement program and provides national coordination for regional operations, emergency support, and physical security.[5]

The proposed legislation, however, calls for "the Secretary of Energy to carry out a program relating to physical security and cybersecurity for pipelines and liquefied natural gas facilities"—a mandate that clearly overlaps with that of PHMSA. Nevertheless, the bill states that it would not modify other agencies' existing obligations. This language suggests that DOE would become responsible for additional compliance measures related to the physical operation of pipelines on top of those already required by PHMSA.

The Bill's Provisions

The bill tasks the Secretary of Energy, in consultation with federal, state, and industry stakeholders, with the creation of policies and procedures to coordinate stakeholders in their analysis of security issues, mentioning a "council" as a potential means of this coordination. The events surrounding Colonial Pipeline serve as an example of the kind of threat that infrastructure faces and provides government agencies and companies alike with the opportunity to take away lessons learned about preparedness for attacks as well as responsiveness to their impacts. In 2020, critical infrastructure in the United States was subject to nearly 400 ransomware attacks, suggesting that a broader approach rather than one simply focused on pipelines is necessary.[6]

DOE would be responsible for the coordination of response and recovery to physical and cyber events. The bill instructs DOE to develop pilot projects with industry "relating to physical security and cybersecurity" and workforce development curricula. The DOE is not the obvious agency to lead this effort, as expertise focused on national security and cyberattacks exists within the federal government at agencies such as the Cybersecurity and Infrastructure Security Agency (CISA) rather than DOE.[7] The House Homeland

Security Committee has introduced several additional bills related to expanding existing federal programming for cybersecurity preparedness to energy infrastructure.[8]

DOE is also tasked with the development of "cybersecurity applications and technologies" that pipeline companies may choose to use. Finally, DOE would be responsible for providing "technical tools" (presumably distinct from the "technologies," but undefined) to industry so that it can "voluntarily evaluate, prioritize, and improve" both physical and cyber security. The digital applications and technical tools necessary to address security threats to pipeline infrastructure, however, already exist in the private sector (even though they may not be deployed adequately, as the Colonial Pipeline attack demonstrates). While there are currently no mandates to implement particular technologies or employ specific techniques to secure pipeline infrastructure, companies have nevertheless instituted various kinds of security and engaged with CISA to improve them.[9]

Conclusion

While the events surrounding the Colonial Pipeline attack provide the opportunity to educate both industry and the government, these lessons are only valuable when applied to the outstanding issues. The breadth of critical infrastructure subject to cyberattacks suggests that an approach simply focused on energy infrastructure is inefficient at best and fails to secure infrastructure at worst. The vague language of the Pipeline and LNG Facility Cybersecurity Preparedness Act fails to recognize the ongoing efforts, particularly at CISA, to address critical infrastructure more broadly. Instead, it proposes to make "tools" and "technologies" specifically tailored and voluntarily available to the pipeline industry.

[1] https://www.reuters.com/business/energy/colonial-pipeline-nomination-system-shut-tuesday-market-sources-2021-05-18/

[2] https://subscriber.politicopro.com/f/?id=00000179-80b0-d9cd-af7f-e7bb45340000&source=email

[3] https://www.govtrack.us/congress/bills/116/hr370

[4] https://www.phmsa.dot.gov/regulations#:~:text=PHMSA%20is%20responsible%20for%20regulating,modes%20of%20transportation%2C%20including%20pipelines.

[5] https://www.phmsa.dot.gov/about-phmsa/offices/office-pipeline-safety

[6] https://www.washingtonpost.com/business/2021/05/12/ransomware-attack/

[7] https://www.cisa.gov/energy-sector

[8] https://www.washingtonpost.com/politics/2021/05/19/cybersecurity-202-colonial-pipeline-hack-sparks-concerns-about-economic-security/

[9]https://www.cisa.gov/pipeline-cybersecurity-initiative