BRACEWELL

INSIGHTS

Pipeline Security and Cybersecurity: Are Guidelines Enough to Protect Critical Infrastructure?

June 4, 2018

*By: **Catherine D. Little**, **Annie Cook** and **Mandi Moroz***

Since 9/11, no new rules or regulations have been promulgated to address pipeline or LNG facility security or cybersecurity. Although the Transportation Security Administration (TSA) recently released an updated version of its "***Pipeline Security Guidelines***" (Guidelines) that were last issued in 2011, those Guidelines remain advisory. And both the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) have made only informal outreach to pipeline and LNG industry as issues have arisen. As the threat of both cyber and physical attacks on critical energy infrastructure continues, however, some question whether minimal standards for prevention of threats should be in place. In particular, there has been recent attention by the U.S. Government Accountability Office (GAO), members of Congress, and at least one Federal Energy Regulatory Commission (FERC) commissioner. (See E&E News Article of May 29, 2018). These discussions, along with recent proposed legislation in the House and the fact that the Pipeline Safety Act is up for reauthorization later this year, are likely to bring these issues into sharper focus.

Agency Guidelines

Although TSA predominantly oversees aviation security, it also has authority over other U.S. Department of Transportation (DOT) modes of transportation, including natural gas and liquid pipelines (transmission and distribution) and LNG facilities. Despite that authority, it was DOT that issued guidance to the industry on the heels of 9/11, in the form of both Pipeline Security Contingency Planning Guidance and a Pipeline Security Information Circular in 2002. TSA relied on DOT's documents until it prepared its first set of Guidelines in 2010 in conjunction with industry, government and other stakeholders. Those Guidelines were last revised in 2011 until the updated version was released in March of this year. TSA has also developed pipeline security training courses and materials that are available at their website.

The purpose of the updated Guidelines is to encourage industry to implement the security measures that are identified by TSA, as part of TSA's stated mission to "protect the nation's transportation systems to ensure freedom of movement for people and commerce." In addition, as with the 2011 Guidelines, TSA will rely on them in conducting voluntary Pipeline Security Program Corporate Security Reviews as well as Critical Facility Security Reviews of various pipeline facilities. There are several notable changes since the 2011 version, such as some modifications to the suggested site-specific security measures set forth in Table 1 (Baseline and Enhanced Security Measures). Additionally, consistent with a recommended action in a 2017 GAO report entitled "***Cybersecurity: Actions Needed to Strengthen***

U.S. Capabilities," the Guidelines promote the use of the "Framework for Improving Critical Infrastructure Cybersecurity" developed by the National Institute of Standards and Technology (NIST). Specifically, in Section 7 of the Guidelines, TSA suggests that operators (1) use the NIST framework to both classify their "Operational technologies" as either "critical" or "non-critical" pipeline cyber assets; (2) apply baseline security measures to both and enhanced security measures to "critical" pipeline cyber assets; and (3) consider, in addition to the NIST framework, other guidance issued by other federal agencies (DHS, Department of Energy (DOE) and Department of Commerce) and other industry standards in planning and implementing a cyber security program (see Guidelines, Section 7.4, citing to for example, guidance or standards issued by the American Gas Association, API Standard 1164 (Pipeline SCADA Security), etc.).

As before, TSA makes it clear that the Guidelines are just that, stating that the "document is guidance and does not impose requirements on any person or company. The term "should" means that TSA recommends the actions described." (Guidelines, p. 1) That said, Guidelines are nevertheless likely to be perceived as minimum best industry practices and thus it is advisable for operators to review and consider their own plans and procedures to ensure they incorporate relevant revisions to be consistent with the Guidelines, as appropriate. Even though not mandatory, an operator could be found negligent for not following the guidance in the event of an incident under various common law theories. An operator that does not have a plan in place that incorporates applicable agency guidance and industry standards could be challenged as to whether it would have been "reasonably prudent" to have a plan and if it would have helped to avoid an incident.

Existing PHMSA Requirements for Security of Pipelines and LNG Facilities

The U.S. DOT's Pipeline and Hazardous Materials Safety Administration (PHMSA) does not have any express regulations in place concerning cyber security for pipelines or LNG facilities, but the Agency has historically exercised its authority to regulate security issues. Regulations governing physical security issues have been on the books since before the events of 9/11. For example, there are express requirements that LNG and liquid pipeline facilities have written security procedures to address both physical and personnel security, to some extent. 49 C.F.R. Parts 193.2509 and .2511; Part 195.436. There are also a number of regulations in place that address the need to monitor activities along pipelines, including aerial surveillance, right-of-way patrols, and damage prevention requirements to avoid third party damage to pipelines. See e.g. Parts 192.613, 192.614 and 192.705; Parts 195.412 and 195.442. In addition, PHMSA requires that pipeline and LNG facility operators have emergency plans in place to anticipate the risks of pipelines. See Parts 192.615; Parts 195.402 and Parts 195.440; Part 193.2509. Lastly, pipeline operators are also required to implement public awareness plans to educate members of the public located along the rights-of-way. See Parts 192.616 and 195.440.

Requests for Mandatory Security and Cybersecurity Requirements

Over the past several years, the GAO has widely criticized various agencies with respect to cyber security issues. As noted above, in early 2017, GAO issued a specific recommendation to strengthen cybersecurity of U.S. critical infrastructure. Following on the heels of that recommendation, Congress spoke out on the issue with two ranking members of the Senate Energy and Natural Resources Committee and House Energy and Commerce Committee penning a letter to the GAO and TSA in July 2017 suggesting that the voluntary Guidelines be

updated or codified. The two members noted that, in contrast to the pipeline industry, the electric utility industry has mandatory requirements in place, yet the utility industry depends on pipelines to provide oil and gas. GAO was requested to further study the issue, and that report is expected later this year. Perhaps keying off that letter, H.R. 5175 "Pipeline and LNG Facility Cybersecurity Preparedness Act," was introduced earlier this year to require that DOE develop both a physical and cyber security program for pipelines and LNG facilities.

Similar observations about the lack of security regulation for pipelines have been made by others, including earlier this week by FERC Commissioner Richard Glick. Noting that FERC has promulgated regulations to protect the cybersecurity of the U.S. electric grid, and the fact that there are only voluntary guidelines in place for the oil and gas pipeline industry, Commissioner Glick commented that "If you just have one weak link—one entity that doesn't follow voluntary standards—it can cause significant damage." Casting doubt on whether TSA was the right agency to be issuing pipeline security regulations, Glick suggested FERC could exercise more oversight of the interstate gas pipeline industry with respect to security but also acknowledged limitations to that approach given the Commission's lack of jurisdiction over intrastate gas pipelines and oil pipelines. Finally, Glick commented that it might be in the best interests for pipelines to have mandatory standards, stating that "If I was a gas pipeline company and something went wrong, I'd rather tell my insurance company or tell a court that I followed government mandatory standards than, 'I just did something on my own.'"

Meanwhile, the ***DOE recently issued its 5-year strategy*** aimed at reducing the impacts or disruptions caused by cyberattacks. The strategy addresses U.S. critical energy infrastructure – both oil and gas pipelines and the electric grid – in an attempt to improve preparedness, and incident response and recovery, among other goals. This strategy is also only recommended; not mandatory.

Both the electric utility industry and the oil and gas industry face increasing cyber threats from nation-states, criminals and terrorists. While oil and gas pipelines and LNG facilities are subject to limited PHMSA regulations regarding physical security, there are no mandatory requirements regarding cybersecurity. TSA Guidelines are designed to assist the industries in developing a reasonable security and cybersecurity plan that is sufficiently protective of its assets. While those requirements are only voluntary, they are nevertheless likely to be perceived as minimum best industry practices by insurance companies and in litigation. For that reason, it is advisable for operators to review and consider any changes to their own plans and procedures. The promulgation of at least minimal security regulatory requirements may be worthy of consideration at this point, given the increase in both cybersecurity threats as well as pipeline sabotage, as well as which agency is best positioned to promulgate them (see our prior pipelaws.com alerts of ***November 27, 2017*** and ***May 2, 2018*** and our ***article appearing in Law 360 on May 24, 2018)***. Both the proposed legislation H.R. 5175 as well as the upcoming PSA reauthorization may provide the opportunity for further engagement with the industry.