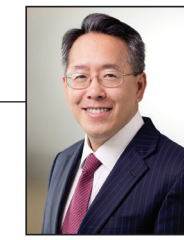
Pipeline & Gas Journal
connecting you to the pipeline industry worldwide

GUEST COMMENTARY

By **Paul Tiao,** Partner, **Hunton Andrews Kurth LLP**



Regulatory Developments in Pipeline Cybersecurity

The Transportation Security Administration (TSA) is overhauling its strategy for cybersecurity in the pipeline sector. Since 2007, Congress has authorized TSA to issue prescriptive pipeline cybersecurity requirements, but until May of this year, TSA instead adopted a collaborative approach with industry using voluntary Pipeline Security Guidelines.

During this period, U.S. pipeline companies participated in TSA's voluntary programs, developed collaborative arrangements with TSA, and improved overall cybersecurity risk management in the face of increasing attacks.

Nevertheless, the worsening cyber-threat, and pressure from Congress and other agencies, led to the widespread belief among most industry insiders that a prescriptive regulatory scheme from TSA was imminent. The May 2021 ransomware attack on Colonial Pipeline likely served as the straw that broke the proverbial camel's back.

TSA took action in May and July of 2021, issuing two distinct Security Directives, respectively, both independent of existing TSA cybersecurity programs or guidelines. Notably, the Directives do not rely on TSA's 2007 pipeline security authority, which would have required notice-and-comment rulemaking. Instead, TSA used general transportation emergency security directive powers granted when Congress first formed TSA in 2001.

However, TSA has long been criticized for being under-equipped to oversee even voluntary pipeline security standards. A recent Government Accountability Office (GAO) report highlighted these operational staffing deficiencies. As a result, the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) is assisting TSA's staff with enforcement of the Security Directives, and DHS intends to hire additional cybersecurity staff at both agencies.

The Security Directives create a set of mandatory oversight and reporting obligations that apply to "critical" pipeline owner/operators. According to TSA's May 2021 Security Directive, an owner/operator of a hazardous liquid and natural gas pipeline or liquified natural gas facility will be considered "critical" for the purposes of these Security Directives if notified by TSA of this designation. In other words, TSA has sole authority to make this determination.

The first Security Directive states that TSA is required by law to "review pipeline security plans and inspect critical facilities of the 100 most critical pipeline operators" and that "[i]n general, criticality is determined based on factors such as the volume of product transported, service to other critical sectors, etc."

The May 2021 Security Directive requires critical owner/operators to report "cybersecurity incidents" to CISA within 12 hours of identification. Such incidents may include unauthorized access of information technology or operational technology systems, discovery of malware, denial of service activities, physical attacks against network infrastructure, and any cybersecurity activity that results in or has the potential to cause operational disruption.

The Security Directive also required owner/operators to designate a Cybersecurity Coordinator to be available 24 hours a day, seven days a week. Finally, this Directive required owner/operators to review and assess their current practices against Section 7 of the 2018 Pipeline Security Guidelines and identify any gaps and related remediation measures to address cyber-related risks, all within 30 days of the issuance of Directive.

Since its issuance, affected companies have almost universally achieved complete and timely compliance with the first Security Directive's mandatory requirements. TSA recently announced that it had received close to 500 notifications pursuant to this Directive, of which CISA rated one as having a "low" impact and the rest as having "negligible" or "minor" impact.

The second Security Directive, issued in July 2021, is shielded from public disclosure because it contains Sensitive Security Information. Nevertheless, TSA provided some public insight into the Security Directive's contents.

Specifically, the DHS announcement of this Directive states that it requires "TSA-designated critical pipelines to implement specific mitigation measures to protect against ransomware attacks and other known threats to information technology and operational technology systems, develop and implement a cybersecurity contingency and recovery plan, and conduct a cybersecurity architecture design review."

This second Security Directive has required a very significant level of effort by critical pipeline owner/operators, with many if not all dedicating thousands of person-hours, scores of employees, and mil-

lions of dollars to compliance efforts.

Despite best efforts, however, strict compliance with all the requirements mandated by the second Security Directive does not appear to be attainable. Owners/operators are achieving compliance with most of the requirements, but for certain requirements, they are requesting extensions pursuant to TSA's established action plan process or seeking approval of alternative security measures.

TSA has come under criticism from industry associations and certain U.S. Senators for inflexible prescriptive requirements, the use of emergency authority instead of notice and comment rulemaking, and the failure to give adequate consideration to input from non-government subject matter experts and stakeholders.

Thus far, TSA has not adopted strict enforcement practices. If owner/operators are demonstrating a good faith effort toward compliance, which includes notifying TSA within the time limits prescribed in the Security Directive, TSA has been responsive and receptive to requests for extensions.

Assuming TSA retains this mandatory approach, the use of regular notice-and-comment rulemaking would allow for broad perspectives from a wide range of stakeholders, considered input, greater transparency and potentially a workable long-term cybersecurity framework that reflects industry, academic and government collaboration. ***P&GJ***

Author: Paul Tiao, *In addition to being a partner at Hunton Andrews Kurth LLP, Paul Tiao is Chair of Hunton Andrews Kurth's National Security Practice and Co-Chair of Hunton Andrews Kurth's Energy Sector Security Team.*