The TSA Pipeline Security Directive: Six Key Points for Boards and Executives
June 7, 2021

By now, the owners and operators of the nation's pipelines comprising critical infrastructure have spent a week intently focused on the Security Directive for pipeline companies issued by the U.S. Department of Homeland Security Transportation Security Administration (TSA). Security Directive Pipeline-2021-01, issued May 27, 2021 and effective May 28 for pipeline Owners/Operators[1], requires: 1) reporting of cybersecurity incidents within 12 hours to the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA), 2) designation by June 4 of a Cybersecurity Coordinator to be available around the clock to coordinate with TSA and CISA, and 3) an assessment and report to TSA and CISA of the pipeline's current state of cybersecurity within 30 days of the Directive.

While the pipeline industry, along with TSA, CISA, and other government regulators, have focused intently on cybersecurity for many years, the abrupt imposition of weighty requirements and short deadlines might nevertheless have come as a surprise. Boards of directors and leadership teams have had only a short time to understand the Directive while also taking action to comply.

Here are six key points to keep in mind:

1) What are the specific reasons for the Security Directive?

The TSA simply states that it is issuing the Directive to address the ongoing cybersecurity threat to pipeline systems and associated infrastructure. It also states that information gathered pursuant to the Directive may be used by the TSA and CISA for vulnerability identification, trend analysis, or to generate tools to prevent other cybersecurity incidents. The requirements of the Directive are all geared towards pipeline and TSA or CISA coordination and collaboration in response to a security incident. Only a few days after the cyberattack that forced the shutdown of Colonial Pipeline in early May 2021, President Biden issued an Executive Order that, among other things, requires improved information sharing between the U.S. government and the private sector on cybersecurity issues.[2] While the TSA's recent

[1] The Directive applies to TSA-specified Owners/Operators; Owner/Operator is defined as "a person who owns or maintains operational control over pipeline facilities or engages in the transportation of hazardous liquids or natural gases and who has been identified by TSA as one of the most critical."

[2] Improving the Nation's Cybersecurity, Exec. Order No. 14028, 18 Fed. Reg. 93, May 17, 2021.

Directive was not mandated by the Executive Order, it is certainly consistent with the theme of requiring robust information sharing and collaboration between public and private sectors.[3]

2) How was TSA able to issue this Directive without a notice and comment rulemaking process?

The TSA issued the Directive under a federal statute that authorizes the TSA Administrator to immediately issue a regulation or security directive in order to protect transportation security, without providing notice or an opportunity for comment and without prior approval of the Secretary of Homeland Security.[4]

3) Is there a process for pipeline companies to comment on the Directive?

The TSA has specifically stated that Owner/Operators may comment on the Directive. Data, views, or arguments may be submitted in writing via email to the TSA at SurfOps-SD@tsa.dhs.gov, and the TSA may in turn amend the Security Directive based on comments received. TSA emphasized that the Directive's effective date will not change.

It seems likely that pipeline companies will submit comments. Within organizations, the Directive may create practical issues. For example, if ownership and operation are in separate entities, may the required submittals be combined? Is 30 days adequate time to perform an accurate and meaningful vulnerability assessment, assess whether current practices and activities align with the TSA's 2018 Pipeline Security Guidelines, identify all gaps, and identify remediation measures and timeline for remediation, all on the form provided by TSA? Are the costs of regulation excessive in relation to the enhancement of security the regulation will provide? One could argue that, while a review of pipeline's security program vis-à-vis TSA's recommendations is a good practice, conducting such a review and submitting a complete report within a compressed timeframe may involve unreasonable expense. Most organizations are staffed for day-to-day operations, they have not planned for this new project, and they might need to bring in additional resources on short notice to assist with the review.

4) How secure is the information once submitted to TSA and CISA?

The information is sensitive security information that is subject to protection under the TSA's Protection of Sensitive Security Information Regulations.[5] The Directive requires submittal of highly sensitive information that will be shared among TSA, CISA, the National Response Center and other agencies as appropriate, and, if not kept confidential, could be used by a malicious actor to jeopardize critical infrastructure security. Fortunately, the Directive acknowledges that "all information that must be reported to TSA or CISA pursuant to this Security Directive is sensitive security information subject to the protections of part 1520 of title 49, Code of Federal Regulations." Those regulations contain very specific requirements on the marking, communication, and secure storage of such information in order to preserve its secure status. Information that a pipeline submits should remain secure so long as the various agencies use appropriate and effective encryption and other protections in storage and transit.

---

[3] "Much of our domestic critical infrastructure is owned and operated by the private sector, and those private sector companies make their own determination regarding cybersecurity investments," said the White House in an online briefing.

[4] 49 U.S.C. §114(l)(2)(a).

[5] 49 C.F.R. Part 1520.

5) How should an Owner/Operator address the requirements?

While the TSA's particular requirements are new, the specifics – incident response, assigned responsibility, assessment of cybersecurity risks – are processes that most companies should have in place. Boards should be receiving information on cybersecurity risks regularly, given the importance of the issue generally (regardless of this new Directive) – and executive management should have information ready to address any questions from the Board whenever asked.

6) What are the consequences for failure to comply?

The Directive does not specify the penalties for failure to comply with the new requirements. However, the TSA could certainly use its enforcement or permitting authority to impose consequences for noncompliance.

Importantly, the TSA specifically states that Owners/Operators that are unable to implement any of the measures should notify the TSA by email. Owners/Operators may also propose alternative measures (along with a basis for the measures) to the TSA for approval. As a strategic matter, companies will want to ensure that any alternative measures they propose are consistent with their security assessment, to avoid commitments that they may be unable to fulfill.

See CISA Pipeline Cybersecurity Library for further resources.

Susan Lindberg
Former General Counsel and candidate for M.S.C.S. in cybersecurity
918-595-4826
slindberg@gablelaw.com

Trent Shores
Former United States Attorney and National Security Cyber Specialist
918-595-4805
tshores@gablelaw.com

Tom Vincent
Certified Regulatory Compliance Manager and Certified Information Privacy Professional
918-595-4857
tvincent@gablelaw.com