BRACEWELL

INSIGHTS

TSA Revises Cybersecurity Directive for Critical Pipeline and LNG Facilities

July 29, 2022

*By: **Catherine D. Little**, **Annie Cook**, **Seth D. DuCharme**, **Anissa L. Adas**, and **Mandi Moroz***

Following significant collaboration with the industry, the Transportation Security Administration (TSA) issued a revised ***directive***, effective July 27, 2022, which updates one of the prior directives issued in the wake of a May 2021 cyberattack on one of the nation's largest interstate oil pipelines. Similar to the prior ***directives***, this latest version, Security Directive Pipeline-2021-02C, incorporates several key modifications that provide more flexibility for operators of critical pipeline and LNG infrastructure who are subject to the directives. This includes reliance on a performance-based, rather than prescriptive, security outcome model, which is more aligned with the federal pipeline safety regulations and allows operators to develop plans that are tailored to their pipeline systems. The updated directive, along with a portion of previous Directive 2021-02B, is set to expire within one year, on July 27, 2023, during which time the TSA intends to pursue formal rulemaking.

TSA remains concerned that risks to critical pipeline systems and LNG facilities continue to be high. As such, TSA mandates in its most recent directive that the following additional protocols be developed and incorporated into response plans:

- **Cybersecurity Implementation Plan.** This plan must be submitted to TSA for approval within 90 days of the effective date of the directive (i.e., by Oct. 25, 2022). The plan must provide specific measures and a proposed schedule for implementation of network segmentation policies and controls, access control measures, policies and controls to manage access rights; policies that limit the availability and use of shared accounts, continued monitoring and detection procedures; and policies to reduce the exploitation risks of unpatched systems.

- **Cybersecurity Incident Response Plan**.

- **Cybersecurity Assessment Program** (including annual submission of plans to assess cybersecurity effectiveness and vulnerabilities).

Notably, until a Cybersecurity Implementation Plan is approved by TSA, owner/operators of critical pipeline and LNG facilities are required to continue to implement the July 2021 Security Directive Pipeline-2021-02B, attached to the new Security Directive Pipeline-2021-02C, along with any TSA approved action plans or alternative measures. In part, these new requirements reflect feedback from the pipeline and LNG industry on the prior directives, particularly with respect to allowing more flexibility for security practices involving operational technology (OT) systems as opposed to the previous emphasis on information technology (IT) systems. In addition, updated ***Security Directive Pipeline-2021-01B*** (which, on May 29, 2022, replaced and superseded the May 2021 Security Directive Pipeline-2021-01A) revised the reporting requirements to mandate reporting within 24 hours (rather than 12 hours).

TSA's demands on owners and operators of critical pipelines and LNG facilities, however, remain stringent. In a ***press release*** about the latest directive, TSA Administrator David Pekoske said, "We recognize that every company is different, and we have developed an approach that accommodates that fact, supported by continuous monitoring and auditing to assess achievement of the needed cybersecurity outcomes." Whether or not the performance-based approach actually facilitates sufficient flexibility for critical pipeline and LNG owners and operators remains to be seen, and a number of prescriptive requirements remain in the updated directive.

While the latest revision is encouraging and the directive's language indicates more flexible requirements for the industry, pipeline and LNG critical facility owners and operators should seek expert advice when developing, implementing, and assessing their incident response plans to ensure that they remain on track with the ever-evolving standards.