Articles + Publications | October 5, 2021

Locke Lord QuickStudy: Developments in Energy Pipeline ?Security: TSA Directives, and Recommendations for Owners ??and Operators

Locke Lord LLP

WRITTEN BY

Theodore P. Augustinos | Laura L. Ferguson | Brandan Montminy | Alexander R. Cox | Berne C. Kluber

RELATED OFFICES

Dallas | Hartford | Houston

In the wake of the disruptive ransomware attack on the Colonial Pipeline in early May 2021, the U.S. Transportation Security Administration ("TSA") issued two security directives to the pipeline industry. The first, Security Directive Pipeline-2021-01 (the "First Directive"), had an effective date of May 28, 2021, was sent directly to certain owners and operators of pipelines that TSA determined were critical and is now publicly available. Issued July 20, 2021, the second TSA security directive, ?Security Directive Pipeline-2021-02: Pipeline Cybersecurity Mitigation Actions, Contingency ?Planning, and Testing (the "Second Directive") was also sent directly to certain pipeline owners and operators, but has not been disclosed to the public. A subsequent Government Accountability Office ("GAO") report, however, reveals general requirements of the Second Directive for owners and operators. This Quick Study reviews the requirements of these directives. In the case of the Second Directive, which is not publicly available, we rely on the related GAO report. This Quick Study also offers recommendations for all pipeline owners and operators, whether or not they received the TSA Directives.

The First Directive contains three core requirements: (i) report cybersecurity incidents to CISA; (ii) designate a coordinator to act as a point of contact for cybersecurity issues; and (iii) perform a self-review of cybersecurity readiness and report the results to the TSA and CISA.

The first of these core requirements requires owners and operators to designate a primary and alternate Cybersecurity Coordinator who is required to be available to the TSA and CISA to coordinate cybersecurity practices and address any incidents that arise. The Coordinator must: (i) be a U.S. citizen eligible for security clearance; (ii) serve as the primary contact for cyber-related intelligence information and cybersecurity-related activities and communications with TSA and CISA; (iii) be accessible to the TSA and CISA 24 hours a day, seven days a week; (iv) coordinate cyber and related security practices and procedures internally; and (v) work with appropriate law enforcement and emergency response agencies.

The second core requirement involves the reporting of a variety of types of cybersecurity related incidents, but these are not limited to just information systems and data. Owners and operators must report cybersecurity incidents no later than 12 hours after the incident is identified, to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ("CISA"). Reportable incidents are: (i) unauthorized access of an information or operational technology system; (ii) discovery of malicious software on an information or

operational technology system; (iii) activity resulting in a denial of service to any information or operational technology system; (iv) a physical attack against the Owners/Operator's network infrastructure, such as deliberate damage to communication lines; and (v) any other cybersecurity incident that causes or has the potential to cause operational disruption to information systems, operational technology, or other pipeline systems or facilities, or that may adversely affect the safe and efficient transportation of liquids and gases (not limited to large scale impacts), or that impacts national security, economic security, or public health and safety.

The third core requirement mandates that owners and operators review their current activities by performing a "Vulnerability Assessment" using the TSA's recommendations for pipeline cybersecurity contained in Section 7 of the TSA's 2018 Pipeline Security Guidelines (with Change 1 (April 2021)) to assess cyber risks, identify any gaps, develop remediation measures, and report the results to the TSA and CISA. For the owners and operators contacted directly by the TSA, the Vulnerability Assessment was required to be completed by June 27, 2021. Owners and operators that believe they will be unable to implement the required measures of the First Directive (including the Vulnerability Assessment) may submit proposed alternative measures to the TSA for approval.

According to the GAO report referenced above, the Second Directive requires owners and operators to, among other things: (i) implement cybersecurity mitigation measures; (ii) develop a cybersecurity contingency and recovery plan in the event of an incident; and (iii) undergo an annual cybersecurity architecture design review.

Prior to these directives, the TSA promulgated only voluntary guidelines for privately owned and operated pipelines. This shift away from voluntary compliance has been met with pushback from industry groups, including the Interstate Natural Gas Association of America, which notes that the directives were issued without going through the typical notice and comment rulemaking process. While it is uncertain whether these directives will survive challenges to their process of implementation, there is no question that the TSA and CISA are focused on pipeline cybersecurity, and owners and operators will in any event be working to secure their systems, even while maintaining protests on government procedure. These new directives, and those to follow, represent an effort to address recently identified weaknesses in pipeline security and are likely to continue to expand in the coming years.

On September 21, 2021, the Secretary of the Department of Homeland Security offered testimony to the Senate Committee on Homeland Security and Governmental Affairs (available here). The Secretary's testimony referenced the two directives for pipelines, and referenced a series of 60-day cybersecurity sprints to improve security. The fourth of these sprints, which is currently underway, is dedicated to the cybersecurity of transportation systems, and focused on leveraging the lessons learned from the Colonial Pipeline attack. For additional information concerning the current DHS posture on pipeline security, and the sprints, see Secretary Mayorkas Urges Small Businesses to Protect Themselves Against Ransomware | Homeland Security (dhs.gov) and DHS Actions: Cybersecurity | Homeland Security

What Should Owners and Operators Be Doing? Whether or not technically subject to the First Directive and Second Directive, all owners and operators should be taking steps to improve their security, in order to safeguard their businesses and our critical infrastructure.

1. Vulnerability Assessments. For owners and operators that were required to complete a vulnerability assessment by June 27, 2021, the satisfaction of this requirement is the priority. As vulnerability assessments drive the implementation of security safeguards, all owners and operators, including those that are not technically subject

to this requirement, are well advised to conduct vulnerability assessments. To address changes in the threat environment, and internal developments in systems, service providers and uses of data, all vulnerability assessments must be periodically updated.

2. Designation of CISO. A core element of the First Directive is the appointment of a Cybersecurity Coordinator with certain, specific duties, but all owners and operators need to designate someone who will be ultimately responsible for cybersecurity, including the information security program.
3. Information Security Program. All owners and operators should adopt (or update) a written information security program that provides for appropriate technical, physical and administrative safeguards to protect important systems and data.
4. Security Awareness Training. The risk of cybersecurity incidents can be significantly reduced by raising awareness of all personnel as to the potential threats presented by malicious actors. Security awareness training, updated to reflect the current threat environment, and repeated and reinforced in creative ways, must be a key part of the defensive strategy of all owners and operators.
5. Incident Response Planning. Especially given the DHS emphasis on rapid reporting of cybersecurity events affecting certain owners and operators, all owners and operators must be prepared to respond quickly in the event of a suspected incident. Incident response planning, and the development of a plan, are critical to the ability to respond effectively and quickly to an attack.

RELATED INDUSTRIES + PRACTICES

- Energy
- Privacy + Cyber