Freshfields Bruckhaus Deringer

DHS Continues Expanding Cybersecurity Regulations to New Sectors

Authored by: Brock Dahl, Rachel Johnson
December 9, 2021

The Transportation Security Administration (TSA) recently announced two new security directives and additional voluntary guidance for surface transportation owners and operators as part of the Biden Administration's ongoing efforts to address cybersecurity threats to critical infrastructure. Though the directives are targeted at surface transportation owners and operators, the release is part of a trend of expanding DHS regulation of new sectors, and companies in any of the sixteen critical infrastructure sectors as defined by DHS should take note and expect similar requirements to emerge in their sectors in 2022 and beyond. One of the directives applies to all owners and operators of freight railroad carriers. The other applies to owners and operators of passenger railroad carriers or rail transit systems. The directives contain identical measures that will require these surface transportation owners and operators to:

- designate a cybersecurity coordinator to implement and manage cybersecurity plans and coordinate with TSA and CISA on cybersecurity-related matters;
- report cybersecurity incidents to CISA within 24 hours;
- develop and implement a cybersecurity incident response plan to reduce the risk of operational disruption; and
- complete a cybersecurity vulnerability assessment to identify potential gaps or vulnerabilities in their systems.

Critically, the definition of cybersecurity incidents is fairly broad, and generally includes any event that is or is likely to "jeopardize, disrupt, or otherwise impact, the integrity, confidentiality, or availability of" a variety of listed information systems. Importantly, it also notes that the definition includes "an event that is under investigation or evaluation by the owner/operator *as a possible* cybersecurity incident." The directives list a non-exclusive set of examples, but leave some ambiguity about a range of potential events.

The directive also requires that affected companies appoint the Cybersecurity Coordinator within 7 days of the effective date of the directives (December 31, 2021), conduct and submit the vulnerability assessment and remediation plan within 90 days of the effective date, and adopt the incident response plans within 180 days of the effective date.

Additional TSA Rulemaking and Aviation Requirements

TSA also released voluntary guidance calling for all other lower-risk surface transportation owners and operators to voluntarily adopt the same measures. The TSA further announced that it planned

to initiate formal rulemaking (as opposed to what are arguably these directives' more fragile legal basis) regarding cybersecurity measures for surface transportation entities.

In the same announcement, moreover, the TSA also noted that it had updated requirements for airport and airline operators to also designate cyber coordinators and report incidents within 24 hours. The TSA also disclosed that it would issue additional cybersecurity requirements and guidance for the aviation industry.

Expansion of mandatory requirements

These directives are only the most recent TSA mandates requiring private industry to adopt measures to address cybersecurity threats. This past summer, the TSA adopted similar notification requirements and review protocols for pipeline companies. Accordingly, although these newest directives address the surface transportation industry, the TSA's (read, DHS's) announcement has broad implications for other critical infrastructure industries. With pipelines, surface, and then aviation, the regulatory trend is unlikely to halt. One can expect similar future requirements to be rolled out across the sixteen other critical infrastructure sectors, to the degree that they are not currently covered by applicable law.

In light of the expected proliferation of mandatory cybersecurity requirements across other industries, companies in such sectors can begin preparing now for likely change. Preparation can include:

- Ensuring that incident identification and management policies and procedures are in place to govern corporate (i) recognition and categorization of potentially impacted events and (ii) escalation to proper decision makers;
- Ensuring policies are in place to govern communications with regulators, including who is permitted to communicate, what information can be passed, and any authorities on which the company may be relying to protect its information (it remains to be seen whether DHS will permit sharing under current regimes that provide certain liability protections for companies);
- Preparing for the rapid conduct of vulnerability assessments and, to the degree the cybersecurity budget can sustain doing so and as a matter of good practice, conducting an assessment and remediating key issues in advance, foregoing the need to later report such open issues to the government; and
- Reviewing the company's Cybersecurity Incident Response Plan, or to the degree not already established, creating such a plan. Recent guidance from DHS to federal government entities is available here and provides a helpful start. These federal playbooks, however, do not touch upon critical legal components of a response, and companies should consider consulting outside counsel to calibrate plans to evolving regulatory expectations.