Overview

On October 5, the US Department of Energy’s Office of Cybersecurity, Energy Security and Emergency Response (CESER) reached a $3 million partnership agreement with the National Institute of Standards and Technology (NIST) in order to “research and develop tools and practices that will strengthen the cybersecurity of the nation’s energy sector and maritime transportation system.”

According to CESER, 40% of all maritime traffic is comprised of energy products, which highlights the importance of addressing cybersecurity risks at seaports and in maritime transportation to safeguard US energy security. In the past several years, the incidence of cyber-intrusions, malware attacks and other dangerous lapses in cybersecurity impacting the maritime and energy sectors has increased tremendously across the globe.

As of September 2020, APM-Maersk, COSCO Shipping, CMA CGM, and Mediterranean Shipping Company have all fallen victim to multiple cyberattacks. These attacks include but are not limited to company data centers being breached/taken offline, disabling onboard vessel navigation systems and tampering with container booking systems. In 2018, one attack on Maersk’s global IT system forced the company to reinstall nearly 45,000 computers and 4,000 servers, a multweek effort that caused a 20% drop in container volume.

One of the major deliverables under the DOE-NIST agreement is that over the next two years, using the NIST Cybersecurity Framework Version 1.1 (CSF) as a basis, NIST’s National Cybersecurity Center of Excellence – in consultation with CESER – will develop a maritime transportation system CSF Profile and implementation guide. The CSF is a “voluntary Framework [that] consists of standards, guidelines and best practices to manage cybersecurity risk.” Initially developed for operators of critical infrastructure, CSF adoption has spread across industries and beyond the United States.
This US initiative joins an international effort to strengthen the cybersecurity of the maritime industry. In June 2017, the International Maritime Organization (IMO) adopted a resolution that "encourages administrations to ensure that cyber risks are appropriately addressed in existing safety management systems" before the beginning of 2021. In July 2017, the IMO also issued a circular with guidelines that provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities; those guidelines have been incorporated into the shipping industry's Guidelines on Cyber Security onboard Ships. The United States – which as an IMO member is encouraged to give effect to IMO resolutions – appears to be doing so through the DOE-NIST agreement. At the same time, the IMO resolution and circular were heavily influenced by the CSF.

Given that the CSF was developed through a public-private sector collaborative effort, we anticipate that NIST and DOE will provide opportunities for interested parties to provide input into the process, including through public workshops and soliciting public comment.

Practices
Privacy & Cybersecurity