New cybersecurity framework profile to ensure safe transfer of hazardous liquids at ports

November 11 2016

Credit: Ryutaro Tsukata from Pexels

The U.S. Coast Guard (USCG) oversees approximately 800 waterfront facilities that, among other activities, transfer hazardous liquids between

marine vessels and land-based pipelines, tanks or vehicles. These "maritime bulk liquid transfers" increasingly rely on computers to operate valves and pumps, monitor sensors and perform many other vital safety and security functions. This makes the whole system more vulnerable to cybersecurity issues ranging from malware to human error, and is the reason behind a new voluntary cybersecurity guide for the industry.

Maritime bulk liquid transfer processes are part of a complex and sophisticated supply chain of the oil and natural gas industry that brings together various types of organizations and systems. The USCG and industry representatives joined with the National Cybersecurity Center of Excellence (NCCoE), part of the National Institute of Standards and Technology (NIST), to develop a profile to help those organizations assess their cybersecurity risk .

The document is the first in a series of planned profiles that will help maritime industry organizations make the most of the voluntary Framework for Improving Critical Infrastructure Cybersecurity, published by NIST in February 2014. The profile pulls into one document recommended cybersecurity safeguards to provide a starting point for organizations to review and adapt their risk management processes, and it describes a desired minimum state of cybersecurity.

"Working with the U.S. Coast Guard to engage the oil and natural gas industry in creating this profile is a prime example of the collaboration that takes place at the NCCoE," said Don Tobin, NIST senior security engineer. "Organizations working in this critical mission area can leverage the profile to develop a plan to reach their desired state of cybersecurity."

The profile is aimed at those involved in overseeing, developing, implementing and managing the cybersecurity components of maritime

bulk liquid transfer. This includes operations executives, risk managers, cybersecurity professionals and vessel operators. It recognizes a need for security controls on operational technologies such as storage, transfer, pressure and vapor monitoring, emergency response and spill mitigation systems. The profile provides guidance on appropriate security controls for information technology to reliably support these increasingly connected processes, as well as traditional ones such as human resources, training and business communication.

"These facilities face inherent cybersecurity vulnerabilities and the U.S. Coast Guard hopes this profile will assist organizations with mitigating them, and provide a long-term process for developing an internal cyber risk management program," said Lt. Josephine Long, a marine safety expert in the Critical Infrastructure Branch within the USCG's Office of Port & Facility Compliance.

The profile can help individual companies clarify how cybersecurity fits into their mission priorities and how best to allocate resources to secure their information and operational systems. Benefits also include improved understanding of the environment to foster consistent analysis of cybersecurity risks, and alignment of industry and USCG cybersecurity priorities.

According to Long, the USCG plans to work with the NCCoE to build additional profiles that will cover mobile offshore drilling operations, passenger vessel and terminal operations.

The NCCoE works with industry, academia and other government agencies to address real-world cybersecurity problems with existing technology.

Provided by National Institute of Standards and Technology