Executive Order 13636 – Improving Critical Infrastructure Cybersecurity
Section 10(a) and 10(b) Report on the United States Coast Guard and Maritime Critical Infrastructure Cyber Security Standards

Background

On February 12, 2013, the President issued Executive Order (EO) 13636 on Improving Critical Infrastructure Cybersecurity. Under Section 7(a) of Executive Order 13636, the National Institute of Standards and Technology (NIST) was directed to develop a Cybersecurity Framework to reduce cyber risks to critical infrastructure. Pursuant to Section 10(a) of Executive Order 13636, all agencies with responsibility for regulating the security of critical infrastructure are required to review the preliminary Cybersecurity Framework and determine if current cybersecurity regulatory requirements are sufficient in light of current and projected risks. Pursuant to Section 10(b) of the Executive Order, agencies covered under Section 10(a) shall propose prioritized, risk-based, efficient, and coordinated actions if current regulatory requirements are deemed insufficient. This Report is the Coast Guard's response to Section 10(a) and 10(b) of Executive Order 13636.

Findings

Cybersecurity is a complex interdisciplinary field, and the Coast Guard does not have clear, unambiguous authority to specifically "regulate" cybersecurity in the maritime transportation sector. However, the Coast Guard does have clear unambiguous authority to regulate maritime transportation security under the Maritime Transportation Security Act (MTSA) of 2002 and the Security and Accountability For Every (SAFE) Port Act of 2006, codified in Title 46, U.S. Code, Chapter 701. These statutes provide for the regulation of security on vessels and facilities to provide for and maintain physical security, passenger and cargo security, and personnel security. 46 U.S. Code 70103(c)(3)(C)(i). Additionally, these statutes require the Coast Guard to plan for deterrence and response to a transportation security incident, which is a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area. 46 U.S. Code 70103(a). Therefore, the Coast Guard may regulate cybersecurity in the maritime transportation sector under the Maritime Transportation Security Act and the Security and Accountability For Every Port Act so long as the regulations stay within the confines of those statutes; i.e. regulations are limited to the prevention of and response to cybersecurity incidents that may result in a transportation security incident in the maritime transportation system or that threaten physical security, passenger and cargo security, and personnel security on waterfront facilities and vessels. The Coast Guard has issued general cybersecurity guidance both unilaterally, and in collaboration with industry under the National Infrastructure Protection Plan and related Sector-Specific plans. Going forward, the Coast Guard will continue to work with the Department of Homeland Security, and other agencies such as the Department of Justice, Department of Defense, Department of Commerce on the most appropriate use of our authorities to address cyber risks, and will advise Congress on any possible legislative changes that might enable the Coast Guard to better serve the country in the area of cyber security.

The Coast Guard has also participated in the Department of Homeland Security Integrated Task Force (ITF) and contributed to the implementation of the tenets of Executive Order 13636. With the release of the National Institute of Standards and Technology preliminary Cybersecurity Framework, the Coast Guard has been promoting its voluntary adoption by the maritime industry. Since the release of the framework the Coast Guard has also promoted the Department of Homeland Security Critical Infrastructure Cyber Community (C-Cubed) and continues to encourage voluntary adoption of the Cybersecurity Framework by maritime stakeholders.

Additionally, the Coast Guard is collaborating with the Department of Homeland Security National Protection and Programs Directorate, the Transportation Security Agency, and industry, through Area Maritime Security Committees to develop a methodology for identifying and mitigating port cybersecurity risk. The Coast Guard intends to evaluate the Department of Homeland Security Cybersecurity Assessment and Risk Management Approach (CARMA) as a tool for evaluating and prioritizing port cybersecurity risk. Once port risk is evaluated, the Coast Guard will work closely with those owners/operators with the highest cyber risk and encourage completion of the Department of Homeland Security Cybersecurity Resilience Review to further evaluate their cybersecurity posture. This approach will provide each Captain of the Port with fidelity as to the level of cyber risks and vulnerabilities within their respective zones and help to shed light on the cyber risk landscape facing the maritime domain. This process also allows assists owners/operators to understand their level of cyber vulnerability and should lead to a more secure and resilient maritime cyber domain. The Coast Guard will be promoting the use of the Cybersecurity Resilience Review and a modified for maritime version of the Department of Energy's Cybersecurity Capability Maturity Model (C2M2) to aid in Cybersecurity Framework adoption. The Coast Guard envisions that, through the Critical Infrastructure Cyber Community and this methodology, the Service will lay a solid foundation for a more granular assessment of the maritime transportation system's cybersecurity risk and establish baseline metrics for evaluating that risk. Working with international maritime community partners the Coast Guard will also evaluate, and where required, identify cybersecurity standards, capabilities and tools to assess and evaluate cybersecurity risks and impacts to the maritime domain.

The Coast Guard routinely issues guidance through Navigation and Vessel Inspection Circulars (NVICs); whereas guidance has been provided in the past related to general cybersecurity, the Service is also in the planning phase of developing more specific guidance through on how to prepare, prevent, respond and aid in recovery from cybersecurity events or incidents.

The Coast Guard intends to soon release a Coast Guard Cyber Strategy for public view. To counter and protect against maritime cyber threats over the next decade, the Coast Guard's Cyber Strategy emphasizes three strategic priorities: defending our (CG) networks, achieving maritime superiority (decision advantage for CG operations through cyber capability), and, protecting maritime critical infrastructure. Given the growing role of cyber systems in the MTS, the Coast Guard is, and will continue to integrate cyber security into our mission. The Coast Guard is cognizant of the cyber threat environment and also recognizes the importance and continued need for a resilient workforce with operational cyber competencies.