Maritime Equipment Cybersecurity Test Bed

This proposal implements the recommendation to establish a Maritime Transportation System (MTS)-specific cybersecurity test bed within the Cybersecurity and Infrastructure Security Agency. The program would aim to identify high-priority operational technology (OT) components, perform expert testing, share information about vulnerabilities in the digital supply chain, and inform improvements in component design and manufacturing for maritime systems.

A BILL

To establish a program within the Cybersecurity and Infrastructure Security Agency to identify high-priority operational technology components, perform testing, share information about vulnerabilities in the digital supply chain, and inform improvements in component design and manufacturing for maritime systems.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SEC. 1. XXXX.

(a) DEFINITIONS.—In this section:

(1) SECRETARY.—The term "Secretary" means the Secretary of the Department of Homeland Security.

(2) COMMANDANT.—The term "Commandant" means the Commandant of the United States Coast Guard.

(b) ESTABLISHMENT OF THE MARITIME ECOSYSTEM CYBERSECURITY TESTING CENTER.—Not later than 18 months after the passage of this act, the Secretary, in consultation with the Commandant, shall establish a maritime transportation system-specific cybersecurity test bed within the Cybersecurity and Infrastructure Security Agency. The Center shall—

(1) conduct rigorous security testing to identify vulnerabilities in critical maritime operational technologies;

(2) develop new capabilities for vulnerability discovery, management, and mitigation within such technologies;

(3) audit software in critical maritime operational technologies or upon which critical maritime operational technologies are dependent;

(4) establish a vulnerability disclosure program and publish key vulnerabilities identified, with the goal of incentivizing participation from additional vendors; and

(5) serve as a primary technical training tool for both the Department of Homeland Security and United States Coast Guard Academy and United States Coast Guard personnel.

(c) IDENTIFICATION OF INITIAL DEVICES FOR TESTING.—Not later than 120 days after the establishment of the Testing Center under paragraph (b) the Secretary, in consultation with the maritime industry, the Commandant, the Director of the Cybersecurity and Infrastructure Security Agency, Federally funded research and development centers and national labs, and other agencies as determined by the Secretary, shall develop a comprehensive framework to identify critical maritime operational technologies.

(d) ANNUAL REPORT TO CONGRESS.—The Secretary shall provide an annual report to the Senate Committee on Homeland Security and Governmental Affairs and the House Committee on Homeland Security, containing—

(1) a summary of the work performed by the test bed, including an explanation of how grant funding was allocated and a list of vulnerabilities found, along with the corresponding recommended mitigation process and an assessment of the criticality and severity of each vulnerability;

(2) a list of stakeholders who have engaged with and provide technology for testing, including but not limited to international and private sector partners;

(3) a list of tools, techniques, and procedures used by the Testing Center; and

(4) a list of critical maritime operational technologies examined by the Testing Center.

(e) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to carry out this section $2,000,000 for each of fiscal years 2023 through 2027."