115TH CONGRESS
1ST SESSION

S. 2083

To enhance cybersecurity information sharing and coordination at ports in the United States, and for other purposes.

IN THE SENATE OF THE UNITED STATES

NOVEMBER 7, 2017

Ms. HARRIS (for herself and Mr. SULLIVAN) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

---

A BILL

To enhance cybersecurity information sharing and coordination at ports in the United States, and for other purposes.

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2017''.

SEC. 2. IMPROVING CYBERSECURITY RISK ASSESSMENTS, INFORMATION SHARING, AND COORDINATION.

The Secretary of Homeland Security shall—

(1) develop and implement a maritime cybersecurity risk assessment model within 120 days after the date of the enactment of this Act, consistent with the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity and any update to that document pursuant to Public Law 113–274, to evaluate current and future cybersecurity risks (as such term is defined in section 227 of the Homeland Security Act of 2002 (6 U.S.C. 148));

(2) evaluate, on a periodic basis but not less often than once every 2 years, the effectiveness of the maritime cybersecurity risk assessment model under paragraph (1);

(3) seek to ensure participation of at least one information sharing and analysis organization (as such term is defined in section 212 of the Homeland Security Act of 2002 (6 U.S.C. 131)) representing the maritime community in the National Cybersecurity and Communications Integration Center, pursuant to subsection (d)(1)(B) of section 227 of such Act;

(4) establish guidelines for voluntary reporting of maritime-related cybersecurity risks and incidents (as such terms are defined in section 227 of such Act) to the Center (as such term is defined subsection (b) of such section 227), and other appropriate Federal agencies; and

(5) request the National Maritime Security Advisory Committee established under section 70112 of title 46, United States Code, to report and make recommendations to the Secretary on enhancing the sharing of information related to cybersecurity risks and incidents, consistent with the responsibilities of the Center, between relevant Federal agencies and—

(A) State, local, and tribal governments;

(B) relevant public safety and emergency response agencies;

(C) relevant law enforcement and security organizations;

(D) maritime industry;

(E) port owners and operators; and

(F) terminal owners and operators.

SEC. 3. CYBERSECURITY ENHANCEMENTS TO MARITIME SECURITY ACTIVITIES.

The Secretary of Homeland Security, acting through the Commandant of the Coast Guard, shall direct—

(1) each Area Maritime Security Advisory Committee established under section 70112 of title 46, United States Code, to facilitate the sharing of cybersecurity risks and incidents to address port-specific cybersecurity risks, which may include the establishment of a working group of members of Area Maritime Security Advisory Committees to address port-specific cybersecurity vulnerabilities; and

(2) that any area maritime transportation security plan and any vessel or facility security plan required under section 70103 of title 46, United States Code, approved after the development of the cybersecurity risk assessment model required by paragraph (1) of section 2 include a mitigation plan to prevent, manage, and respond to cybersecurity risks (as such term is defined in section 227 of the Homeland Security Act of 2002 (6 U.S.C. 148)).

SEC. 4. VULNERABILITY ASSESSMENTS AND SECURITY PLANS.

Title 46, United States Code, is amended—

(1) in section 70102(b)(1)(C), by inserting ''cybersecurity,'' after ''physical security,''; and

(2) in section 70103(c)(3)(C), by striking ''and'' after the semicolon at the end of clause (iv),

by redesignating clause (v) as clause (vi), and by inserting after clause (iv) the following:

"(v) prevention, management, and response to cybersecurity risks; and".

○