119TH CONGRESS
2D SESSION

S. _____

To amend title 46, United States Code, to require the Secretary of the department in which the Coast Guard is operating to assess cybersecurity risks of certain software and hardware used in certain maritime facilities, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. SCOTT of Florida (for himself and Mr. KIM) introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To amend title 46, United States Code, to require the Secretary of the department in which the Coast Guard is operating to assess cybersecurity risks of certain software and hardware used in certain maritime facilities, 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 ''Maritime Cybersecurity Act''.

SEC. 2. CYBERSECURITY VULNERABILITY ASSESSMENTS OF CERTAIN MARITIME FACILITY SOFTWARE AND HARDWARE.

Section 70102 of title 46, United States Code, is amended—

(1) in subsection (b)—

(A) in paragraph (1)(C), by inserting ''(including, with respect to covered facilities, cybersecurity risks of covered software or hardware as provided under subsection (d)(1))'' after ''cybersecurity risks'';

(B) in paragraph (3), by inserting before the period '', except that, for covered facilities, the Secretary shall annually update each such vulnerability assessment with respect to the identification of weaknesses in security and cybersecurity risks of covered software or hardware in accordance with subsection (d)(1)''; and

(C) in paragraph (4)—

(i) by striking ''In lieu'' and inserting ''(A) Except as provided in subparagraph (B), in lieu''; and

(ii) by adding at the end the following:

''(B) In the event that the Secretary accepts an alternative assessment described in subparagraph

(A) for a covered facility, the Secretary shall still conduct an assessment under paragraph (1) of weaknesses in security and cybersecurity risks of covered software or hardware used at the facility in accordance with subsection (d)(1).''; and

(2) by adding at the end the following:

''(d) ASSESSING CYBERSECURITY RISKS OF COVERED SOFTWARE OR HARDWARE.—

''(1) ASSESSMENTS.—

''(A) IN GENERAL.—Not later than 1 year after the date of enactment of this subsection, and annually thereafter, the Secretary, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall conduct an assessment under subsection (b)(1) with respect to weaknesses in security and cybersecurity risks of covered software or hardware.

''(B) REDUCING BARRIERS.—The Secretary may conduct an assessment under this paragraph—

''(i) notwithstanding any provision of an end user licensing agreement or other contract that would otherwise hinder such assessment; and

''(ii) without obtaining the consent of any owner or operator of a covered facility, or any other person, notwithstanding any other provision of law.

''(2) COVERED FACILITY REPORTS AND COMPLIANCE.—

''(A) IN GENERAL.—Not later than 180 days after the date of enactment of this subsection, and annually thereafter, the owner or operator of a covered facility shall submit a report to the Secretary that—

''(i) identifies—

''(I) any covered software or hardware that—

''(aa) the owner or operator is using, plans to use, or during the previous year used at the facility; and

''(bb) was manufactured—

''(AA) by a foreign entity of concern or a foreign country of concern;

''(BB) by a company controlled or operated by a foreign entity of concern or

a foreign country of concern; or

''(CC) in a foreign country of concern;

''(II) any instance with respect to the facility of a cybersecurity risk resulting in a transportation security incident involving the marine transportation system or any port security system; and

''(III) any other cybersecurity risk with respect to the facility, without regard to whether the risk resulted in a transportation security incident; and

''(ii) except as provided under subparagraph (B)(ii), certifies that any covered software or hardware that the owner or operator is using, plans to use, or during the previous year used has been assessed for consistency with standards of the National Institute of Standards and Technology or equivalent standards within the previous year and the owner or oper-

ator has mitigated against any inconsistencies with such standards.

"(B) COMPLIANCE.—

"(i) IN GENERAL.—Except as provided in clause (ii), the owner or operator of a covered facility may not use any covered software or hardware described in subparagraph (A)(ii) for which it cannot certify consistency with standards of the National Institute of Standards and Technology or equivalent standards.

"(ii) WAIVER PROCESS.—The Secretary may issue a waiver to allow an owner or operator of a covered facility to use covered software or hardware for which it cannot certify consistency with standards of the National Institute of Standards and Technology or equivalent standards if the Secretary determines that there is low risk to national security which is outweighed by the benefit to commerce.

"(3) ANNUAL REPORTS TO CONGRESS.—Not later than 1 year after the date of enactment of this subsection, and annually thereafter, the Secretary, in coordination with the Director of the Cybersecu-

rity and Infrastructure Security Agency, shall provide a report, to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives, on—

"(A) the findings of the most recent assessment under paragraph (1);

"(B) the findings of the most recent reports under paragraph (2);

"(C) any actions taken by the Secretary, or the Director of the Cybersecurity and Infrastructure Security Agency, to mitigate cybersecurity risks with respect to covered software or hardware; and

"(D) any recommendations to Congress on strengthening maritime transportation and port security with respect to cybersecurity risks of covered software or hardware.

"(4) NONDISCLOSURE.—Subject to paragraph (5), information in any assessment or report under this subsection shall not be disclosed to the public, pursuant to section 552(b)(3) of the United States Code.

"(5) COORDINATION.—The Secretary shall coordinate, as appropriate, with Federal entities, and

any other entities that have an agreement in effect with the Secretary for the sharing of information, to make information compiled by the Secretary under this subsection available to such entities for the purposes of maritime transportation security, cybersecurity risk mitigation, or compliance assistance related to covered facilities or covered software or hardware.

''(e) DEFINITIONS.—In this section:

''(1) COVERED FACILITY.—The term 'covered facility' means a facility—

''(A) that is described in subsection (b)(1); and

''(B) to which part 105 or 106 of title 33, Code of Federal Regulations (or successor regulations), applies.

''(2) COVERED SOFTWARE OR HARDWARE.—The term 'covered software or hardware' means any software or hardware that—

''(A) connects to the internet or otherwise poses a cybersecurity risk;

''(B) is used at a covered facility; and

''(C) is used in—

''(i) the marine transportation system, including in a crane manufactured—

''(I) by a foreign entity of concern or a foreign country of concern;

''(II) by a company controlled or operated by a foreign entity of concern or a foreign country of concern; or

''(III) in a foreign country of concern; or

''(ii) a business system that, if compromised or exploited, could result in a transportation security incident;

''(iii) a system whose ownership, operation, maintenance, or control is delegated wholly or in part to any other party; or

''(iv) any other maritime infrastructure determined by the Secretary to be a high cybersecurity risk to the security of any covered facility or to maritime transportation security.

''(3) CYBERSECURITY VULNERABILITY.—The term 'cybersecurity vulnerability' means a characteristic or specific weakness that renders software or hardware or affiliated systems open to exploitation by a given threat or susceptible to a given hazard.

"(4) FOREIGN COUNTRY OF CONCERN; FOREIGN ENTITY OF CONCERN.—The terms 'foreign country of concern' and 'foreign entity of concern' have the meanings given such terms in section 10612(a) of the Research and Development, Competition, and Innovation Act (42 U.S.C. 19221(a)).".