

119TH CONGRESS
2D SESSION

S. 4564

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

MAY 19, 2026

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

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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Maritime Cybersecu-
5 rity Act”.

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

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

6 (1) in subsection (b)—

7 (A) in paragraph (1)(C), by inserting “(in-
8 cluding, with respect to covered facilities, cyber-
9 security risks of covered software or hardware
10 as provided under subsection (d)(1))” after “cy-
11 bersecurity risks”;

12 (B) in paragraph (3), by inserting before
13 the period “, except that, for covered facilities,
14 the Secretary shall annually update each such
15 vulnerability assessment with respect to the
16 identification of weaknesses in security and cy-
17 bersecurity risks of covered software or hard-
18 ware in accordance with subsection (d)(1)”; and

19 (C) in paragraph (4)—

20 (i) by striking “In lieu” and inserting
21 “(A) Except as provided in subparagraph
22 (B), in lieu”; and

23 (ii) by adding at the end the fol-
24 lowing:

25 “(B) In the event that the Secretary accepts an
26 alternative assessment described in subparagraph

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

6 (2) by adding at the end the following:

7 “(d) ASSESSING CYBERSECURITY RISKS OF COV-
 8 ERED SOFTWARE OR HARDWARE.—

9 “(1) ASSESSMENTS.—

10 “(A) IN GENERAL.—Not later than 1 year
 11 after the date of enactment of this subsection,
 12 and annually thereafter, the Secretary, in co-
 13 ordination with the Director of the Cybersecu-
 14 rity and Infrastructure Security Agency, shall
 15 conduct an assessment under subsection (b)(1)
 16 with respect to weaknesses in security and cy-
 17 bersecurity risks of covered software or hard-
 18 ware.

19 “(B) REDUCING BARRIERS.—The Sec-
 20 retary may conduct an assessment under this
 21 paragraph—

22 “(i) notwithstanding any provision of
 23 an end user licensing agreement or other
 24 contract that would otherwise hinder such
 25 assessment; and

1 “(ii) without obtaining the consent of
2 any owner or operator of a covered facility,
3 or any other person, notwithstanding any
4 other provision of law.

5 “(2) COVERED FACILITY REPORTS AND COMPLI-
6 ANCE.—

7 “(A) IN GENERAL.—Not later than 180
8 days after the date of enactment of this sub-
9 section, and annually thereafter, the owner or
10 operator of a covered facility shall submit a re-
11 port to the Secretary that—

12 “(i) identifies—

13 “(I) any covered software or
14 hardware that—

15 “(aa) the owner or operator
16 is using, plans to use, or during
17 the previous year used at the fa-
18 cility; and

19 “(bb) was manufactured—

20 “(AA) by a foreign en-
21 tity of concern or a foreign
22 country of concern;

23 “(BB) by a company
24 controlled or operated by a
25 foreign entity of concern or

1 a foreign country of concern;

2 or

3 “(CC) in a foreign

4 country of concern;

5 “(II) any instance with respect to

6 the facility of a cybersecurity risk re-

7 sulting in a transportation security in-

8 cident involving the marine transpor-

9 tation system or any port security sys-

10 tem; and

11 “(III) any other cybersecurity

12 risk with respect to the facility, with-

13 out regard to whether the risk re-

14 sulted in a transportation security in-

15 cident; and

16 “(ii) except as provided under sub-

17 paragraph (B)(ii), certifies that any cov-

18 ered software or hardware that the owner

19 or operator is using, plans to use, or dur-

20 ing the previous year used has been as-

21 sessed for consistency with standards of

22 the National Institute of Standards and

23 Technology or equivalent standards within

24 the previous year and the owner or oper-

1 ator has mitigated against any inconsis-
2 encies with such standards.

3 “(B) COMPLIANCE.—

4 “(i) IN GENERAL.—Except as pro-
5 vided in clause (ii), the owner or operator
6 of a covered facility may not use any cov-
7 ered software or hardware described in
8 subparagraph (A)(ii) for which it cannot
9 certify consistency with standards of the
10 National Institute of Standards and Tech-
11 nology or equivalent standards.

12 “(ii) WAIVER PROCESS.—The Sec-
13 retary may issue a waiver to allow an
14 owner or operator of a covered facility to
15 use covered software or hardware for which
16 it cannot certify consistency with stand-
17 ards of the National Institute of Standards
18 and Technology or equivalent standards if
19 the Secretary determines that there is low
20 risk to national security which is out-
21 weighed by the benefit to commerce.

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

1 rity and Infrastructure Security Agency, shall pro-
2 vide a report, to the Committee on Homeland Secu-
3 rity and Governmental Affairs of the Senate and the
4 Committee on Homeland Security of the House of
5 Representatives, on—

6 “(A) the findings of the most recent as-
7 sessment under paragraph (1);

8 “(B) the findings of the most recent re-
9 ports under paragraph (2);

10 “(C) any actions taken by the Secretary,
11 or the Director of the Cybersecurity and Infra-
12 structure Security Agency, to mitigate cyberse-
13 curity risks with respect to covered software or
14 hardware; and

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

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

24 “(5) COORDINATION.—The Secretary shall co-
25 ordinate, 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—

1 “(I) by a foreign entity of con-
 2 cern or a foreign country of concern;

3 “(II) by a company controlled or
 4 operated by a foreign entity of con-
 5 cern or a foreign country of concern;
 6 or

7 “(III) in a foreign country of
 8 concern; or

9 “(ii) a business system that, if com-
 10 promised or exploited, could result in a
 11 transportation security incident;

12 “(iii) a system whose ownership, oper-
 13 ation, maintenance, or control is delegated
 14 wholly or in part to any other party; or

15 “(iv) any other maritime infrastruc-
 16 ture determined by the Secretary to be a
 17 high cybersecurity risk to the security of
 18 any covered facility or to maritime trans-
 19 portation security.

20 “(3) CYBERSECURITY VULNERABILITY.—The
 21 term ‘cybersecurity vulnerability’ means a char-
 22 acteristic or specific weakness that renders software
 23 or hardware or affiliated systems open to exploi-
 24 tation by a given threat or susceptible to a given
 25 hazard.

1 “(4) FOREIGN COUNTRY OF CONCERN; FOREIGN
2 ENTITY OF CONCERN.—The terms ‘foreign country
3 of concern’ and ‘foreign entity of concern’ have the
4 meanings given such terms in section 10612(a) of
5 the Research and Development, Competition, and
6 Innovation Act (42 U.S.C. 19221(a)).”.

○