

Union Calendar No. 260

115TH CONGRESS
1ST SESSION

H. R. 3101

[Report No. 115–356, Part I]

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

IN THE HOUSE OF REPRESENTATIVES

JUNE 28, 2017

Mrs. TORRES introduced the following bill; which was referred to the Committee on Homeland Security, and in addition to the Committee on Transportation and Infrastructure, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

OCTOBER 19, 2017

Additional sponsors: Mr. CORREA, Ms. WILSON of Florida, Mr. EVANS, Mr. KILMER, Ms. BARRAGÁN, and Mr. POE of Texas

OCTOBER 19, 2017

Reported from the Committee on Homeland Security

OCTOBER 19, 2017

The Committee on Transportation and Infrastructure discharged; committed to the Committee of the Whole House on the State of the Union and ordered to be printed

A BILL

To enhance cybersecurity information sharing and coordination at ports in the United States, 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 “Strengthening Cyber-
5 security Information Sharing and Coordination in Our
6 Ports Act of 2017”.

7 **SEC. 2. IMPROVING CYBERSECURITY RISK ASSESSMENTS,**
8 **INFORMATION SHARING, AND COORDINA-**
9 **TION.**

10 The Secretary of Homeland Security shall—

11 (1) develop and implement a maritime cyberse-
12 curity risk assessment model within 120 days after
13 the date of the enactment of this Act, consistent
14 with the National Institute of Standards and Tech-
15 nology Framework for Improving Critical Infrastruc-
16 ture Cybersecurity and any update to that document
17 pursuant to Public Law 113–274, to evaluate cur-
18 rent and future cybersecurity risks (as that term is
19 defined in section 227 of the Homeland Security Act
20 of 2002 (6 U.S.C. 148));

21 (2) evaluate, on a periodic basis but not less
22 than once every two years, the effectiveness of the
23 cybersecurity risk assessment model established
24 under paragraph (1);

1 (3) seek to ensure participation of at least one
2 information sharing and analysis organization (as
3 that term is defined in section 212 of the Homeland
4 Security Act of 2002 (6 U.S.C. 131)) representing
5 the maritime community in the National Cybersecu-
6 rity and Communications Integration Center, pursu-
7 ant to subsection (d)(1)(B) of section 227 of the
8 Homeland Security Act of 2002 (6 U.S.C. 148);

9 (4) establish guidelines for voluntary reporting
10 of maritime-related cybersecurity risks and incidents
11 (as such terms are defined in section 227 of the
12 Homeland Security Act of 2002 (6 U.S.C. 148)) to
13 the Center (as that term is defined subsection (b) of
14 section 227 of the Homeland Security Act of 2002
15 (6 U.S.C. 148)), and other appropriate Federal
16 agencies; and

17 (5) request the National Maritime Security Ad-
18 visory Committee established under section 70112 of
19 title 46, United States Code, to report and make
20 recommendations to the Secretary on enhancing the
21 sharing of information related to cybersecurity risks
22 and incidents between relevant Federal agencies and
23 State, local, and tribal governments and consistent
24 with the responsibilities of the Center (as that term
25 is defined subsection (b) of section 227 of the

1 Homeland Security Act of 2002 (6 U.S.C. 148));
2 relevant public safety and emergency response agen-
3 cies; relevant law enforcement and security organiza-
4 tions; maritime industry; port owners and operators;
5 and terminal owners and operators.

6 **SEC. 3. CYBERSECURITY ENHANCEMENTS TO MARITIME**
7 **SECURITY ACTIVITIES.**

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

10 (1) each Area Maritime Security Advisory Com-
11 mittee established under section 70112 of title 46,
12 United States Code, to facilitate the sharing of cy-
13 bersecurity risks and incidents to address port-spe-
14 cific cybersecurity risks, which may include the es-
15 tablishment of a working group of members of Area
16 Maritime Security Advisory Committees to address
17 port-specific cybersecurity vulnerabilities; and

18 (2) that any area maritime security plan and
19 facility security plan required under section 70103
20 of title 46, United States Code, approved after the
21 development of the cybersecurity risk assessment
22 model required by paragraph (1) of section 2 include
23 a mitigation plan to prevent, manage, and respond
24 to cybersecurity risks.

1 **SEC. 4. VULNERABILITY ASSESSMENTS AND SECURITY**
2 **PLANS.**

3 Title 46, United States Code, is amended—

4 (1) in section 70102(b)(1)(C), by inserting “cy-
5 bersecurity,” after “physical security,”; and

6 (2) in section 70103(c)(3)(C), by striking
7 “and” after the semicolon at the end of clause (iv),
8 by redesignating clause (v) as clause (vi), and by in-
9 serting after clause (iv) the following:

10 “(v) prevention, management, and re-
11 sponse to cybersecurity risks; and”.

Union Calendar No. 260

115TH CONGRESS
1ST Session

H. R. 3101

[Report No. 115-356, Part I]

A BILL

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

OCTOBER 19, 2017

Reported from the Committee on Homeland Security

OCTOBER 19, 2017

The Committee on Transportation and Infrastructure discharged; committed to the Committee of the Whole House on the State of the Union and ordered to be printed