

115TH CONGRESS  
1ST SESSION

# H. R. 3101

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

---

## 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”.

1 **SEC. 2. IMPROVING CYBERSECURITY RISK ASSESSMENTS,**  
2 **INFORMATION SHARING, AND COORDINA-**  
3 **TION.**

4 The Secretary of Homeland Security shall—

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

15 (2) evaluate, on a periodic basis but not less  
16 than once every two years, the effectiveness of the  
17 cybersecurity risk assessment model established  
18 under paragraph (1);

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

1           (4) establish guidelines for voluntary reporting  
2 of maritime-related cybersecurity risks and incidents  
3 (as such terms are defined in section 227 of the  
4 Homeland Security Act of 2002 (6 U.S.C. 148)) to  
5 the Center (as that term is defined subsection (b) of  
6 section 227 of the Homeland Security Act of 2002  
7 (6 U.S.C. 148)), and other appropriate Federal  
8 agencies; and

9           (5) request the National Maritime Security Ad-  
10 visory Committee established under section 70112 of  
11 title 46, United States Code, to report and make  
12 recommendations to the Secretary on enhancing the  
13 sharing of information related to cybersecurity risks  
14 and incidents between relevant Federal agencies and  
15 State, local, and tribal governments and consistent  
16 with the responsibilities of the Center (as that term  
17 is defined subsection (b) of section 227 of the  
18 Homeland Security Act of 2002 (6 U.S.C. 148));  
19 relevant public safety and emergency response agen-  
20 cies; relevant law enforcement and security organiza-  
21 tions; maritime industry; port owners and operators;  
22 and terminal owners and operators.

1 **SEC. 3. CYBERSECURITY ENHANCEMENTS TO MARITIME**  
2 **SECURITY ACTIVITIES.**

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

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

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

20 **SEC. 4. VULNERABILITY ASSESSMENTS AND SECURITY**  
21 **PLANS.**

22 Title 46, United States Code, is amended—

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

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

1 by redesignating clause (v) as clause (vi), and by in-  
2 sserting after clause (iv) the following:

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

○