

**Suspend the Rules and Pass the Bill, H.R. 3101, With an Amendment**

**(The amendment strikes all after the enacting clause and inserts a new text)**

115<sup>TH</sup> CONGRESS  
1<sup>ST</sup> 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  
5 Cybersecurity Information Sharing and Coordination in  
6 Our 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  
6 cybersecurity risk assessment model within 120 days  
7 after the date of the enactment of this Act, con-  
8 sistent with the National Institute of Standards and  
9 Technology Framework for Improving Critical Infra-  
10 structure Cybersecurity and any update to that doc-  
11 ument pursuant to Public Law 113–274, to evaluate  
12 current and future cybersecurity risks (as such term  
13 is defined in section 227 of the Homeland Security  
14 Act of 2002 (6 U.S.C. 148));

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

19 (3) seek to ensure participation of at least one  
20 information sharing and analysis organization (as  
21 such 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  
24 Cybersecurity and Communications Integration Cen-  
25 ter, pursuant to subsection (d)(1)(B) of section 227  
26 of such Act;

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 such  
4 Act) to the Center (as such term is defined sub-  
5 section (b) of such section 227), and other appro-  
6 priate Federal agencies; and

7           (5) request the National Maritime Security Ad-  
8 visory Committee established under section 70112 of  
9 title 46, United States Code, to report and make  
10 recommendations to the Secretary on enhancing the  
11 sharing of information related to cybersecurity risks  
12 and incidents, consistent with the responsibilities of  
13 the Center, between relevant Federal agencies and—

14                   (A) State, local, and tribal governments;

15                   (B) relevant public safety and emergency  
16 response agencies;

17                   (C) relevant law enforcement and security  
18 organizations;

19                   (D) maritime industry;

20                   (E) port owners and operators; and

21                   (F) terminal owners and operators.

22 **SEC. 3. CYBERSECURITY ENHANCEMENTS TO MARITIME**  
23 **SECURITY ACTIVITIES.**

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

1 (1) each Area Maritime Security Advisory Com-  
2 mittee established under section 70112 of title 46,  
3 United States Code, to facilitate the sharing of  
4 cybersecurity risks and incidents to address port-  
5 specific cybersecurity risks, which may include the  
6 establishment of a working group of members of  
7 Area Maritime Security Advisory Committees to ad-  
8 dress port-specific cybersecurity vulnerabilities; and

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

18 **SEC. 4. VULNERABILITY ASSESSMENTS AND SECURITY**  
19 **PLANS.**

20 Title 46, United States Code, is amended—

21 (1) in section 70102(b)(1)(C), by inserting  
22 “cybersecurity,” after “physical security,”; and

23 (2) in section 70103(c)(3)(C), by striking  
24 “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”.