

[Floor Situation](#) | [Summary](#) | [Background](#) | [Cost](#) | [Staff Contact](#)

## [H.R. 3878, Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2015, as amended](#)

### FLOOR SITUATION

On Wednesday, December 16, 2015, the House will consider [H.R. 3878](#), *the Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2015, as amended*, under suspension of the rules. H.R. 3878 was introduced on November 2, 2015 by Rep. Norma Torres (D-CA) and was referred to the Committee on Homeland Security, and in addition, to the Committee on Transportation and Infrastructure. The Homeland Security Committee ordered the bill reported, as amended, by voice vote, on November 4, 2015.

### SUMMARY

H.R. 3878 requires the Secretary of the Department of Homeland Security (DHS) to develop a maritime cybersecurity risk assessment model to evaluate current and future cybersecurity risks in the maritime environment. The bill requires the Secretary to implement the model within 120 days of enactment and, not less than once every two years, evaluate its effectiveness.

The bill also requires the Secretary to ensure the participation of at least one information sharing and analysis organization representing the maritime community in the National Cybersecurity and Communications Integration Center (NCCIC) and establish guidelines for the voluntary reporting of maritime-related cybersecurity risks and incidents to NCCIC.

The bill also directs the Secretary to request that the National Maritime Security Advisory Committee report and make recommendations on enhancing information sharing related to cybersecurity risks and incidents between federal agencies and state, local, and tribal governments and relevant law enforcement organizations, the maritime industry, and port and terminal owners and operators.

The bill further requires the Commandant of the Coast Guard to direct each Area Maritime Security Advisory Committee to facilitate the sharing of cybersecurity risks and incidents to address port-specific cybersecurity risks and ensure that any maritime or facility security plan include a mitigation plan to prevent, manage, and respond to cybersecurity risks.

## BACKGROUND

The National Cybersecurity and Communications Integration Center (NCCIC) within the Department of Homeland Security “shares information among public and private sector partners to build awareness of vulnerabilities, incidents, and mitigations. Cyber and industrial control systems users can subscribe to information products, feeds, and services at no cost.”<sup>1</sup> The Center serves as an around-the-clock centralized location for the coordination and integration of cyber situational awareness and management. NCCIC partners include: all Federal departments and agencies; State, local, Tribal, and territorial governments; the private sector; and intergovernmental entities.

NCCIC provides its partners with enhanced situational awareness of cybersecurity incidents and risks, as well as information to manage cyber vulnerabilities, threats, and incidents. In 2014, NCCIC received more than 97,000 incident reports, and issued nearly 12,000 actionable cyber-alerts or warnings. NCCIC teams detected more than 64,000 significant vulnerabilities on Federal and non-Federal systems and directly responded to 115 significant cyber incidents last year.<sup>2</sup>

The National Maritime Security Advisory Committee is a “national committee that advises the U.S. Secretary of Homeland Security on maritime security matters.”<sup>3</sup> NMSAC “is comprised of 22 members representing all segments of the industry and provides advice to the Secretary of the Department of Homeland Security via the Commandant of the U.S. Coast Guard on matters such as national security strategy and policy, actions required to meet current and future security threats, international cooperation on security issues, and security concerns of the maritime transportation industry.”<sup>4</sup> The Committee

According to the bill sponsor, “During a recent hearing, the Port of Long Beach brought up significant cyber security vulnerabilities at U.S. ports. This is due in part to port landlords not always coordinating with port tenants and also to federal agencies only beginning to consider the impact of a cyber-attack on our maritime infrastructure in its security assessments and strategies. [The bill will] “improve information sharing and cooperation in addressing cyber security risks at our nation’s ports.”<sup>5</sup>

## COST

The Congressional Budget Office (CBO) [estimates](#) that implementing H.R. 3878, as ordered reported by the Committee on Homeland Security, would cost \$37 million over the 2016 to 2020 period, assuming appropriation of the necessary amounts. Pay-as-you-go procedures do not apply to this legislation because enacting it would not affect direct spending or revenues.

## STAFF CONTACT

For questions or further information please contact [Jerry White](#) with the House Republican Policy Committee by email or at 5-0190.

---

<sup>1</sup> <http://www.dhs.gov/national-cybersecurity-communications-integration-center>

<sup>2</sup> See [testimony](#) of the Honorable Suzanne E. Spaulding, Under Secretary, National Protection and Programs Directorate, U.S. Department of Homeland Security, at 2, before the House Committee on Homeland Security. February 25, 2015.

<sup>3</sup> <http://uscg-nmsac.blogspot.com/>

<sup>4</sup> Id.

<sup>5</sup> See Press Release—“[Torres Introduces Bills to Improve LA Ports' Security](#),” October 30, 2015.