

STRENGTHENING CYBERSECURITY INFORMATION SHARING AND COORDINATION IN OUR PORTS ACT OF 2017

OCTOBER 19, 2017.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. McCAUL, from the Committee on Homeland Security, submitted the following

R E P O R T

[To accompany H.R. 3101]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom was referred the bill (H.R. 3101) to enhance cybersecurity information sharing and coordination at ports in the United States, and for other purposes, having considered the same, report favorably thereon without amendment and recommend that the bill do pass.

CONTENTS

	Page
Purpose and Summary .....	2
Background and Need for Legislation .....	2
Hearings .....	3
Committee Consideration .....	3
Committee Votes .....	3
Committee Oversight Findings .....	3
New Budget Authority, Entitlement Authority, and Tax Expenditures .....	3
Congressional Budget Office Estimate .....	3
Statement of General Performance Goals and Objectives .....	5
Duplicative Federal Programs .....	6
Congressional Earmarks, Limited Tax Benefits, and Limited Tariff Benefits ...	6
Federal Mandates Statement .....	6
Preemption Clarification .....	6
Disclosure of Directed Rule Makings .....	6
Advisory Committee Statement .....	6
Applicability to Legislative Branch .....	6
Section-by-Section Analysis of the Legislation .....	6
Changes in Existing Law Made by the Bill, as Reported .....	7
Committee Correspondence .....	15

## PURPOSE AND SUMMARY

H.R. 3101 requires the Secretary of Homeland Security to develop and implement a maritime risk assessment model that focuses on cybersecurity vulnerabilities at our Nation's ports. This bill also requires the Secretary to seek participation of information sharing and analysis organizations and the National and Area Maritime Security Advisory Committees in analyzing the cybersecurity risks in the maritime domain and addressing the cyber vulnerabilities at each port.

The United States Coast Guard is the government agency responsible for the physical security of our Nation's port infrastructure, but their authority for cyber security is less clear. Under the Maritime Transportation Security Act (MTSA) of 2002 (Pub. L. 107–295), the U.S. Coast Guard was granted responsibility for the protection of "communication systems," including information that flows through the Marine Transportation System, but does not clearly spell out the Coast Guard's responsibility for cybersecurity at ports.

This bill removes this ambiguity by including cybersecurity as an enumerated responsibility under MTSA. While this bill clarifies that the Coast Guard is the appropriate agency for reviewing cybersecurity in the maritime domain, the Committee believes the Coast Guard should coordinate with other DHS entities as appropriate.

## BACKGROUND AND NEED FOR LEGISLATION

In recent years there have been many high-profile cyber-related attacks upon the United States. These include the U.S. Office of Personnel Management breach (July 2015), the release of the Central Intelligence Agency (CIA) "Vault 7" by Wikileaks (March 2017), the WannaCry ransomware attack (July 2017), and Equifax breach (September 2017).

The maritime domain is not immune from such cyber threats. While they may not have been as newsworthy as other notable cyber incidents, the maritime industry—including both individual companies and maritime authorities—has been the target of several cyber-related crimes and attacks.

More than \$1 trillion dollars of goods, from cars to oil to corn and everything in between, move through the Nation's seaports every year. Terror groups, nation-States, criminal organizations, hackers and even disgruntled employees could breach computer systems at the Nation's ports, resulting in major detrimental effects on global trade and shipping and damage to the domestic economy.

Increasingly, cargo is moving through our ports using automated industrial control systems. These computer systems are controlling machinery in port facilities to move containers, fill tanks and on-load and off-load ships. The growing automation of business operations systems, industrial control systems and onboard vessel control systems at the Nation's ports, while fostering efficiencies, have created cybersecurity vulnerabilities in areas that were previously safe from these threats.

For instance, in 2017, a major U.S. shipping carrier suffered a system disruption that shut down a significant number of its computer systems for days. In fact, the Petya cyberattack forced the

largest terminal at the Port of Los Angeles to shut down operations for several days while port operators contained the impact of the attack. In Europe, drug smugglers attempted to hack into cargo tracking systems to rearrange containers and hide illicit narcotics. Similarly, a foreign military is suspected of compromising several systems aboard a commercial ship contracted by the U.S. Transportation Command.

Despite the fact that Government Accountability Office (GAO) has placed cybersecurity of our Nation's critical infrastructure on the "High Risk" list since 2003, the Coast Guard, and the Department of Homeland Security (DHS) as a whole, have been slow to fully engage on cybersecurity efforts at the Nation's 360 seaports. The first step in reducing this risk is to conduct the appropriate risk assessments called for by this bill.

#### HEARINGS

No hearings were held on H.R. 3101 in the 115th Congress.

#### COMMITTEE CONSIDERATION

The Committee met on September 7, 2017, to consider H.R. 3101, and ordered the measure to be reported to the House with a favorable recommendation, without amendment, by voice vote.

#### COMMITTEE VOTES

Clause 3(b) of Rule XIII of the Rules of the House of Representatives requires the Committee to list the recorded votes on the motion to report legislation and amendments thereto.

No recorded votes were requested during consideration of H.R. 3101.

#### COMMITTEE OVERSIGHT FINDINGS

Pursuant to clause 3(c)(1) of Rule XIII of the Rules of the House of Representatives, the Committee has held oversight hearings and made findings that are reflected in this report.

#### NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

In compliance with clause 3(c)(2) of Rule XIII of the Rules of the House of Representatives, the Committee finds that H.R. 3101, the Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2017, would result in no new or increased budget authority, entitlement authority, or tax expenditures or revenues.

#### CONGRESSIONAL BUDGET OFFICE ESTIMATE

The Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

U.S. CONGRESS,  
CONGRESSIONAL BUDGET OFFICE,  
*Washington, DC, October 6, 2017.*

Hon. MICHAEL MCCAUL,  
*Chairman, Committee on Homeland Security,  
House of Representatives, Washington, DC.*

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 3101, the Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2017.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Megan Carroll.

Sincerely,

MARK P. HADLEY  
(For Keith Hall, Director).

Enclosure.

*H.R. 3101—Strengthening Cybersecurity Information Sharing and  
Coordination in Our Ports Act of 2017*

Summary: H.R. 3101 would require the Department of Homeland Security (DHS) to expand efforts to enhance the cybersecurity of U.S. ports. The bill also would clarify that the Coast Guard, the agency within DHS primarily responsible for activities related to maritime security, is authorized to pursue efforts related to cybersecurity. Based on information from DHS, CBO estimates that implementing H.R. 3101 would cost \$38 million over the 2018–2022 period, assuming appropriation of the necessary amounts.

Enacting the bill would not affect direct spending or revenues; therefore, pay-as-you-go procedures do not apply. CBO estimates that enacting H.R. 3101 would not increase net direct spending or on-budget deficits in any of the four consecutive 10-year periods beginning in 2028.

H.R. 3101 would impose intergovernmental and private-sector mandates, as defined in the Unfunded Mandates Reform Act (UMRA), on owners and operators of port facilities and vessels. Based on an analysis of information from the Coast Guard about current practices related to cybersecurity among maritime facilities and vessels, CBO estimates that the cost of complying with the mandates for public and private entities would fall below the annual thresholds established in UMRA for intergovernmental and private-sector mandates (\$78 million and \$156 million in 2017, respectively, adjusted annually for inflation).

Estimated cost to the Federal Government: The estimated budgetary effect of H.R. 3101 is shown in the following table. The costs of this legislation fall primarily within budget functions 050 (defense), 400 (transportation), and 450 (community and regional development).

	By fiscal year, in millions of dollars—					
	2018	2019	2020	2021	2022	2018– 2022
INCREASES IN SPENDING SUBJECT TO APPROPRIATION						
Estimated Authorization Level .....	8	8	8	9	9	42
Estimated Outlays .....	5	8	8	8	9	38

Basis of estimate: For this estimate CBO assumes the bill will be enacted near the end of 2017 and that the estimated amounts will be appropriated each year. Estimated outlays are based on historical spending patterns for similar activities.

H.R. 3101 would direct DHS to pursue a variety of activities to enhance cybersecurity, particularly by increasing the capacity for information sharing among maritime stakeholders in the federal, state, local, and private sectors. Under the bill, DHS would need to develop a model for assessing maritime-related cybersecurity risks and require area maritime security advisory committees—stakeholder groups formed to address security-related issues at specific U.S. ports—to share information related to cybersecurity threats and develop plans to address port-specific vulnerabilities.

According to DHS, many of the activities required under the bill are consistent with current administrative policy, but implementing some efforts—particularly those aimed at increasing the capacity for information sharing among maritime stakeholders—would require additional spending. Based on an analysis of information from DHS, CBO estimates that fully funding such efforts would cost \$38 million over the 2018–2022 period, mostly for additional staff required to design and implement data-sharing systems and provide analytical support related to risk assessment.

Pay-As-You-Go considerations: None.

Increase in long term direct spending and deficits: CBO estimates that enacting H.R. 3101 would not increase net direct spending or on-budget deficits in any of the four consecutive 10-year periods beginning in 2028.

Intergovernmental and private-sector impact: H.R. 3101 would impose intergovernmental and private-sector mandates, as defined in UMRA, on owners and operators of port facilities and vessels by requiring them to incorporate cybersecurity information into their vulnerability assessments. The bill also would require facilities to address cybersecurity risks and develop a mitigation plan if they submit security plans for approval after DHS has developed a model for assessing maritime-related cybersecurity risk. Based on an analysis of information from the Coast Guard about current practices among maritime facilities and vessels, CBO estimates that the incremental cost of complying with the mandates for public and private entities would fall below the annual thresholds established in UMRA for intergovernmental and private-sector mandates (\$78 million and \$156 million in 2017, respectively, adjusted annually for inflation).

Estimate prepared by: Federal costs: Megan Carroll; Impact on state, local, and tribal governments: Jon Sperl; Impact on the private sector: Paige Piper/Bach.

Estimate approved by: H. Samuel Papenfuss, Deputy Assistant Director for Budget Analysis.

#### STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of Rule XIII of the Rules of the House of Representatives, H.R. 3101 contains the following general performance goals and objectives, including outcome related goals and objectives authorized.

The general performance goals and objectives of H.R. 3101 are to require the U.S. Coast Guard to conduct cybersecurity risk assess-

ments at the Nation’s seaports; increase cybersecurity information sharing; and develop plans to mitigate prevent, manage, and respond to such cybersecurity risks.

#### DUPLICATIVE FEDERAL PROGRAMS

Pursuant to clause 3(c) of Rule XIII, the Committee finds that H.R. 3101 does not contain any provision that establishes or reauthorizes a program known to be duplicative of another Federal program.

#### CONGRESSIONAL EARMARKS, LIMITED TAX BENEFITS, AND LIMITED TARIFF BENEFITS

In compliance with Rule XXI of the Rules of the House of Representatives, this bill, as reported, contains no congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(e), 9(f), or 9(g) of the Rule XXI.

#### FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

#### PREEMPTION CLARIFICATION

In compliance with section 423 of the Congressional Budget Act of 1974, requiring the report of any Committee on a bill or joint resolution to include a statement on the extent to which the bill or joint resolution is intended to preempt State, local, or Tribal law, the Committee finds that H.R. 3101 does not preempt any State, local, or Tribal law.

#### DISCLOSURE OF DIRECTED RULE MAKINGS

The Committee estimates that H.R. 3101 would require no directed rule makings.

#### ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

#### APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

#### SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

##### *Section 1. Short Title.*

This section provides that this bill may be cited as the “Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2017”.

*Sec. 2. Improving Cybersecurity Risk Assessments, Information Sharing, and Coordination.*

The Committee believes that cyber threats of critical infrastructure present one of the most serious threats faced by the United States and the Nation's maritime facilities specifically. The ability of ports and vessels to operate in a secure and efficient manner is vital to the Nation's economy. To that end, this section requires the Secretary of Homeland Security to create a maritime cybersecurity risk assessment model within 120 days of enactment of this act and evaluate its effectiveness not less than every 2 years; ensure information sharing and analysis organizations coordinate with the National Cybersecurity and Communications Integration Center for maritime cybersecurity risks; establish guidelines for the voluntary reporting of maritime related cybersecurity risks and incidents; and request that the National Maritime Security Advisory Committee make recommendations on how to best share maritime cybersecurity risks and incidents with Federal, State, local and tribal government.

The Committee believes that through creating a structure to share, analyze risk, and coordinate best practices nationwide, the maritime critical infrastructure sector will be better able to protect and mitigate against cyber threats at maritime facilities.

*Sec. 3. Cybersecurity Enhancements to Maritime Security Activities.*

This section requires the Secretary of Homeland Security to request that Area Maritime Security Committees share cybersecurity risks and incidents to increase port-specific awareness and coordination; ensure Area Maritime Security Plans and Facility Security Plans address cybersecurity threats, and have plans to mitigate, prevent, manage and respond to cybersecurity risks.

The Committee believes that cybersecurity risk must be incorporated into every aspect of port and maritime security and that encouraging the Area Maritime Security Committees to address this important vulnerability is important to coordinating cybersecurity practices throughout the maritime community.

*Sec. 4. Vulnerability Assessments and Security Plans.*

This section amends the Maritime Transportation Security Act of 2002, Title 46, United States Code, to include cybersecurity in the vulnerability assessments at ports and in vessel and facility security plans.

The Committee believes that this small but important amendatory provision clarifies that the Coast Guard has the specific authority to require maritime vessels and facilities to incorporate cybersecurity into their assessments and plans and highlights the importance of cybersecurity in the maritime environment.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic,

and existing law in which no change is proposed is shown in roman):

**TITLE 46, UNITED STATES CODE**

\* \* \* \* \*

**SUBTITLE VII—SECURITY AND DRUG ENFORCEMENT**

\* \* \* \* \*

**CHAPTER 701—PORT SECURITY**

\* \* \* \* \*

**SUBCHAPTER I—GENERAL**

\* \* \* \* \*

**§ 70102. United States facility and vessel vulnerability assessments**

(a) INITIAL ASSESSMENTS.—The Secretary shall conduct an assessment of vessel types and United States facilities on or adjacent to the waters subject to the jurisdiction of the United States to identify those vessel types and United States facilities that pose a high risk of being involved in a transportation security incident.

(b) FACILITY AND VESSEL ASSESSMENTS.—(1) Based on the information gathered under subsection (a) of this section and by not later than December 31, 2004, the Secretary shall conduct a detailed vulnerability assessment of the facilities and vessels that may be involved in a transportation security incident. The vulnerability assessment shall include the following:

(A) Identification and evaluation of critical assets and infrastructures.

(B) Identification of the threats to those assets and infrastructures.

(C) Identification of weaknesses in physical security, *cybersecurity*, passenger and cargo security, structural integrity, protection systems, procedural policies, communications systems, transportation infrastructure, utilities, contingency response, and other areas as determined by the Secretary.

(2) Upon completion of an assessment under this subsection for a facility or vessel, the Secretary shall provide the owner or operator with a copy of the vulnerability assessment for that facility or vessel.

(3) The Secretary shall update each vulnerability assessment conducted under this section at least every 5 years.

(4) In lieu of conducting a facility or vessel vulnerability assessment under paragraph (1), the Secretary may accept an alternative assessment conducted by or on behalf of the owner or operator of the facility or vessel if the Secretary determines that the alternative assessment includes the matters required under paragraph (1).

(c) SHARING OF ASSESSMENT INTEGRATION OF PLANS AND EQUIPMENT.—The owner or operator of a facility, consistent with any Federal security restrictions, shall—

(1) make a current copy of the vulnerability assessment conducted under subsection (b) available to the port authority with jurisdiction of the facility and appropriate State or local law enforcement agencies; and

(2) integrate, to the maximum extent practical, any security system for the facility with compatible systems operated or maintained by the appropriate State, law enforcement agencies, and the Coast Guard.

**§ 70103. Maritime transportation security plans**

(a) NATIONAL MARITIME TRANSPORTATION SECURITY PLAN.—(1) Not later than April 1, 2005, the Secretary shall prepare a National Maritime Transportation Security Plan for deterring and responding to a transportation security incident.

(2) The National Maritime Transportation Security Plan shall provide for efficient, coordinated, and effective action to deter and minimize damage from a transportation security incident, and shall include the following:

(A) Assignment of duties and responsibilities among Federal departments and agencies and coordination with State and local governmental agencies.

(B) Identification of security resources.

(C) Procedures and techniques to be employed in deterring a national transportation security incident.

(D) Establishment of procedures for the coordination of activities of—

(i) Coast Guard maritime security teams established under this chapter; and

(ii) Federal Maritime Security Coordinators required under this chapter.

(E) A system of surveillance and notice designed to safeguard against as well as ensure earliest possible notice of a transportation security incident and imminent threats of such a security incident to the appropriate State and Federal agencies.

(F) Establishment of criteria and procedures to ensure immediate and effective Federal identification of a transportation security incident, or the substantial threat of such a security incident.

(G) Designation of—

(i) areas for which Area Maritime Transportation Security Plans are required to be prepared under subsection (b); and

(ii) a Coast Guard official who shall be the Federal Maritime Security Coordinator for each such area.

(H) A risk-based system for evaluating the potential for violations of security zones designated by the Secretary on the waters subject to the jurisdiction of the United States.

(I) A recognition of certified systems of intermodal transportation.

(J) A plan for ensuring that the flow of cargo through United States ports is reestablished as efficiently and quickly as possible after a transportation security incident.

(3) The Secretary shall, as the Secretary considers advisable, revise or otherwise amend the National Maritime Transportation Security Plan.

(4) Actions by Federal agencies to deter and minimize damage from a transportation security incident shall, to the greatest extent possible, be in accordance with the National Maritime Transportation Security Plan.

(5) The Secretary shall inform vessel and facility owners or operators of the provisions in the National Transportation Security Plan that the Secretary considers necessary for security purposes.

(b) AREA MARITIME TRANSPORTATION SECURITY PLANS.—(1) The Federal Maritime Security Coordinator designated under subsection (a)(2)(G) for an area shall—

(A) submit to the Secretary an Area Maritime Transportation Security Plan for the area; and

(B) solicit advice from the Area Security Advisory Committee required under this chapter, for the area to assure preplanning of joint deterrence efforts, including appropriate procedures for deterrence of a transportation security incident.

(2) The Area Maritime Transportation Security Plan for an area shall—

(A) when implemented in conjunction with the National Maritime Transportation Security Plan, be adequate to deter a transportation security incident in or near the area to the maximum extent practicable;

(B) describe the area and infrastructure covered by the plan, including the areas of population or special economic, environmental, or national security importance that might be damaged by a transportation security incident;

(C) describe in detail how the plan is integrated with other Area Maritime Transportation Security Plans, and with facility security plans and vessel security plans under this section;

(D) include consultation and coordination with the Department of Defense on matters relating to Department of Defense facilities and vessels;

(E) establish area response and recovery protocols to prepare for, respond to, mitigate against, and recover from a transportation security incident consistent with section 202 of the SAFE Port Act of 2006 (6 U.S.C. 942) and subsection (a) of this section;

(F) include any other information the Secretary requires;

(G) include a salvage response plan—

(i) to identify salvage equipment capable of restoring operational trade capacity; and

(ii) to ensure that the waterways are cleared and the flow of commerce through United States ports is reestablished as efficiently and quickly as possible after a maritime transportation security incident; and

(H) be updated at least every 5 years by the Federal Maritime Security Coordinator.

(3) The Secretary shall—

(A) review and approve Area Maritime Transportation Security Plans under this subsection; and

(B) periodically review previously approved Area Maritime Transportation Security Plans.

(4) In security zones designated by the Secretary in each Area Maritime Transportation Security Plan, the Secretary shall consider—

(A) the use of public/private partnerships to enforce security within the security zones, shoreside protection alternatives, and the environmental, public safety, and relative effectiveness of such alternatives; and

(B) technological means of enhancing the security zones of port, territorial waters, and waterways of the United States.

(c) VESSEL AND FACILITY SECURITY PLANS.—(1) Within 6 months after the prescription of interim final regulations on vessel and facility security plans, an owner or operator of a vessel or facility described in paragraph (2) shall prepare and submit to the Secretary a security plan for the vessel or facility, for deterring a transportation security incident to the maximum extent practicable.

(2) The vessels and facilities referred to in paragraph (1)—

(A) except as provided in subparagraph (B), are vessels and facilities that the Secretary believes may be involved in a transportation security incident; and

(B) do not include any vessel or facility owned or operated by the Department of Defense.

(3) A security plan required under this subsection shall—

(A) be consistent with the requirements of the National Maritime Transportation Security Plan and Area Maritime Transportation Security Plans;

(B) identify the qualified individual having full authority to implement security actions, and require immediate communications between that individual and the appropriate Federal official and the persons providing personnel and equipment pursuant to subparagraph (C);

(C) include provisions for—

(i) establishing and maintaining physical security, passenger and cargo security, and personnel security;

(ii) establishing and controlling access to secure areas of the vessel or facility, including access by persons engaged in the surface transportation of intermodal containers in or out of a port facility;

(iii) procedural security policies;

(iv) communications systems; **[and]**

(v) *prevention, management, and response to cybersecurity risks; and*

**[(v)]** (vi) other security systems;

(D) identify, and ensure by contract or other means approved by the Secretary, the availability of security measures necessary to deter to the maximum extent practicable a transportation security incident or a substantial threat of such a security incident;

(E) describe the training, periodic unannounced drills, and security actions of persons on the vessel or at the facility, to be carried out under the plan to deter to the maximum extent practicable a transportation security incident, or a substantial threat of such a security incident;

(F) provide a strategy and timeline for conducting training and periodic unannounced drills;

(G) be updated at least every 5 years;

(H) be resubmitted for approval of each change to the vessel or facility that may substantially affect the security of the vessel or facility; and

(I) in the case of a security plan for a facility, be resubmitted for approval of each change in the ownership or operator of the facility that may substantially affect the security of the facility.

(4) The Secretary shall—

(A) promptly review each such plan;

(B) require amendments to any plan that does not meet the requirements of this subsection;

(C) approve any plan that meets the requirements of this subsection; and

(D) subject to the availability of appropriations, verify the effectiveness of each such facility security plan periodically, but not less than 2 times per year, at least 1 of which shall be an inspection of the facility that is conducted without notice to the facility.

(5) A vessel or facility for which a plan is required to be submitted under this subsection may not operate after the end of the 12-month period beginning on the date of the prescription of interim final regulations on vessel and facility security plans, unless—

(A) the plan has been approved by the Secretary; and

(B) the vessel or facility is operating in compliance with the plan.

(6) Notwithstanding paragraph (5), the Secretary may authorize a vessel or facility to operate without a security plan approved under this subsection, until not later than 1 year after the date of the submission to the Secretary of a plan for the vessel or facility, if the owner or operator of the vessel or facility certifies that the owner or operator has ensured by contract or other means approved by the Secretary to deter to the maximum extent practicable a transportation security incident or a substantial threat of such a security incident.

(7) The Secretary shall require each owner or operator of a vessel or facility located within or adjacent to waters subject to the jurisdiction of the United States to implement any necessary interim security measures, including cargo security programs, to deter to the maximum extent practicable a transportation security incident until the security plan for that vessel or facility operator is approved.

(8)(A) The Secretary shall require that the qualified individual having full authority to implement security actions for a facility described in paragraph (2) shall be a citizen of the United States.

(B) The Secretary may waive the requirement of subparagraph (A) with respect to an individual if the Secretary determines that it is appropriate to do so based on a complete background check of the individual and a review of all terrorist watch lists to ensure that the individual is not identified on any such terrorist watch list.

(d) NONDISCLOSURE OF INFORMATION.—

(1) IN GENERAL.—Information developed under this section or sections 70102, 70104, and 70108 is not required to be disclosed to the public, including—

(A) facility security plans, vessel security plans, and port vulnerability assessments; and

(B) other information related to security plans, procedures, or programs for vessels or facilities authorized under this section or sections 70102, 70104, and 70108.

(2) LIMITATIONS.—Nothing in paragraph (1) shall be construed to authorize the designation of information as sensitive security information (as defined in section 1520.5 of title 49, Code of Federal Regulations)—

(A) to conceal a violation of law, inefficiency, or administrative error;

(B) to prevent embarrassment to a person, organization, or agency;

(C) to restrain competition; or

(D) to prevent or delay the release of information that does not require protection in the interest of transportation security, including basic scientific research information not clearly related to transportation security.

(e) ESPECIALLY HAZARDOUS CARGO.—

(1) ENFORCEMENT OF SECURITY ZONES.—Consistent with other provisions of Federal law, the Coast Guard shall coordinate and be responsible for the enforcement of any Federal security zone established by the Coast Guard around a vessel containing especially hazardous cargo. The Coast Guard shall allocate available resources so as to deter and respond to a transportation security incident, to the maximum extent practicable, and to protect lives or protect property in danger.

(2) RESOURCE DEFICIENCY REPORTING.—

(A) IN GENERAL.—When the Secretary submits the annual budget request for a fiscal year for the department in which the Coast Guard is operating to the Office of Management and Budget, the Secretary shall provide to the Committees on Homeland Security and Transportation and Infrastructure of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report that includes—

(i) for the last full fiscal year preceding the report, a statement of the number of security zones established for especially hazardous cargo shipments;

(ii) for the last full fiscal year preceding the report, a statement of the number of especially hazardous cargo shipments provided a waterborne security escort, subdivided by Federal, State, local, or private security; and

(iii) an assessment as to any additional vessels, personnel, infrastructure, and other resources necessary to provide waterborne escorts to those especially hazardous cargo shipments for which a security zone is established.

(B) ESPECIALLY HAZARDOUS CARGO DEFINED.—In this subsection, the term “especially hazardous cargo” means anhydrous ammonia, ammonium nitrate, chlorine, liquefied natural gas, liquefied petroleum gas, and any other substance, material, or group or class of material, in a particular amount and form that the Secretary determines by

regulation poses a significant risk of creating a transportation security incident while being transported in maritime commerce.

\* \* \* \* \*

## COMMITTEE CORRESPONDENCE

COMITTEE ON TRANSPORTATION AND INFRASTRUCTURE,  
HOUSE OF REPRESENTATIVES,  
*Washington, DC, October 19, 2017.*

Hon. MICHAEL T. MCCAUL,  
*Chairman, Committee on Homeland Security,*  
*Washington, DC.*

I write concerning H.R. 3101, the Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2017. This legislation includes matters that fall within the Rule X jurisdiction of the Committee on Transportation and Infrastructure.

I recognize and appreciate your desire to bring this legislation before the House of Representatives in an expeditious manner, and accordingly, the Committee on Transportation and Infrastructure will forego action on the bill. However, this is conditional on our mutual understanding that foregoing consideration of the bill does not prejudice the Committee with respect to the appointment of conferees or to any future jurisdictional claim over the subject matters contained in the bill or similar legislation that fall within the Committee's Rule X jurisdiction. Further, this is conditional on our understanding that mutually agreed upon changes to the legislation will be incorporated into the bill prior to floor consideration. Lastly, should a conference on the bill be necessary, I request your support for the appointment of conferees from the Committee on Transportation and Infrastructure during any House-Senate conference convened on this or related legislation.

Finally, I would ask that a copy this letter and your response acknowledging our jurisdictional interest be included in the bill report filed by the Committee on Homeland Security, as well as in the Congressional Record during consideration of the measure on the House floor, to memorialize our understanding. I look forward to working with the Committee on Homeland Security as the bill moves through the legislative process.

Sincerely,

BILL SHUSTER,  
*Chairman.*

---

HOUSE OF REPRESENTATIVES,  
COMMITTEE ON HOMELAND SECURITY,  
*Washington, DC, October 19, 2017.*

Hon. BILL SHUSTER,  
*Chairman, Committee on Transportation and Infrastructure,*  
*Washington, DC.*

DEAR CHAIRMAN SHUSTER: Thank you for your letter regarding H.R. 3101, the "Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2017." I appreciate your support in bringing this legislation before the House of Representatives, and accordingly, understand that the Committee on Transportation and Infrastructure will forego further consideration of the bill.

The Committee on Homeland Security concurs with the mutual understanding that by foregoing consideration of this bill at this

time, the Committee on Transportation and Infrastructure does not waive any jurisdiction over the subject matter contained in this bill or similar legislation in the future. In addition, should a conference on this bill be necessary, I would support your request to have the Committee represented on the conference committee. Further, the Committee on Homeland Security agrees that mutually agreed upon changes to the legislation will be incorporated into the bill prior to floor consideration.

I will insert copies of this exchange in the report on the bill and in the Congressional Record during consideration of this bill on the House floor. I thank you for your cooperation in this matter.

Sincerely,

MICHAEL T. MCCAUL  
*Chairman.*

○