fourth Presidency—dealing with this issue. This issue has not been handled. We have not sanctioned this regime. We have not enforced those sanctions. We have not obtained multilateral sanctions. We have not ever given the Kim dictatorship one reason to think that our government and our allied friends around the world are serious about ending the nuclear threat from North Korea.

Mr. Speaker, I thank my friend from Kentucky for standing up in the Financial Services Committee and leading the way for secondary sanctions. I thank my friends, Chairman ROYCE and Ranking Member ENGEL in the Foreign Affairs Committee, for their work with this administration to end this threat to not only north Asia, our economic allies, our national security allies, but also our friends around the world.

Mr. Speaker, I urge all my colleagues to support this important legislation.

Ms. MAXINE WATERS of California. Mr. Speaker, I reserve the balance of my time.

Mr. BARR. Mr. Speaker, I yield 2 minutes to the gentleman from North Carolina (Mr. BUDD), a member of the Financial Services Committee.

Mr. BUDD. Mr. Speaker, I rise today in support of Representative BARR's bill, the Otto Warmbier North Korea Nuclear Sanctions Act.

Mr. Speaker, how is it that a tiny, isolated country like North Korea has the ability to fund and develop a nuclear weapons program with the capability to strike American soil?

The answer to that question is found in part through correspondent and payable-through accounts, which are tools used by North Korea to bypass the existing U.S. and U.N. sanctions against them.

Non-North Korean actors use these accounts to fund the government through shell and front companies. While these sanctions are implemented in good faith, it is time to acknowledge that sometimes they just don't work.

There is some good news, Mr. Speaker. If enacted, this bill requires the Treasury Secretary to impose strict conditions on those who knowingly do business with North Korea through those accounts.

We have also seen the United Nations take action recently by banning North Korea's export of iron ore, which is another legitimate step in stopping the continued development of their nuclear weapons program.

Finally, the Trump administration's executive orders will help us more easily target companies that do business with North Korea.

These actions, plus the enactment of this legislation, will create the most debilitating sanctions package Pyongyang and their financial surrogates have ever seen.

Of all the positive things in this bill, though, I am most excited by the language amending the Bretton Woods Agreement Act to instruct U.S. executive directors at international financial institutions, like the IMF and the World Bank, to use our ''voice and vote'' to oppose financial assistance to governments that knowingly support the Kim regime.

□ 1445

The United States has long used its economic influence, a more aggressive element of soft power, to advance an agenda that liberates the oppressed in the darkest corners of the world like North Korea.

Mr. Speaker, I thank the gentleman from Kentucky for introducing this bill, and I urge its adoption.

Mr. BARR. Mr. Speaker, may I inquire how much time is remaining.

The SPEAKER pro tempore. The gentleman from Kentucky has 3 minutes remaining, and the gentlewoman from California has 7 minutes remaining.

Mr. BARR. Mr. Speaker, I yield 1½ minutes to the gentleman from Indiana (Mr. HOLLINGSWORTH), another distinguished member of the Financial Services Committee.

Mr. HOLLINGSWORTH. Mr. Speaker, I, too, rise in strong support of this legislation.

Every single week, I make phone calls to Hoosiers back home, and I hear every night on those phone calls how hard they are working to build a better and brighter future for themselves, for their families, and for their children; but they understand that, in order to have a brighter, better future, they must have a future. I hear on the phone every single night how concerned they are that there won't be a future with all that they see, all that they read, all that they hear about these threats from North Korea.

We in Congress have heard their pleas to do something, that enough is enough, that threats against Guam, that ICBMs flying off the Peninsula, that nuclear tests, that the time has come for decisive action, and decisive action is what we are taking here.

The toughest financial sanctions ever put in place, that is what this bill does, and that is what we need to put in place to ensure that we demand real change from North Korea, that we demand that they stop threatening Americans and the American way of life.

Mr. Speaker, I support this legislation, support the work that is being done to confront this challenge once and for all, and this bill demands the question: Will you do business with the United States or will you do business with North Korea?

Mr. Speaker, I am excited to stand up in support of this legislation.

Ms. MAXINE WATERS of California. Mr. Speaker, I yield back the balance of my time.

Mr. BARR. Mr. Speaker, I yield the balance of my time to the gentleman from Indiana (Mr. MESSER), another distinguished member of the Financial Services Committee.

Mr. MESSER. Mr. Speaker, I want to thank my colleague from Kentucky for his leadership and my colleague from Indiana for his leadership on this legislation as well.

Mr. Speaker, from day one, President Trump's message to North Korea has been clear: the U.S. will not tolerate any North Korean actions that threaten American lives.

Hoosiers appreciate President Trump's leadership and understand the crisis we face. North Korea is an erratic and brutal regime. We simply cannot accept a world in which North Korea has nuclear weapons that can reach American shores.

Unfortunately, with each missile test, we are moving closer to that world becoming a reality. That is why I am proud to work with my colleague from Kentucky and other colleagues on the Otto Warmbier North Korean Nuclear Sanctions Act. With this bill, we will give foreign financial institutions a clear choice: you can either do business with Kim Jong-un in North Korea, or you can do business with the United States—but not both.

By imposing the toughest financial sanctions ever on North Korea, this bill cuts off crucial resources that the regime relies on to finance its weapons program.

Mr. Speaker, I urge my colleagues to support this measure, help us meet the North Korean threat head-on, and do what is necessary to protect our country.

Mr. BARR. Mr. Speaker, I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Kentucky (Mr. BARR) that the House suspend the rules and pass the bill, H.R. 3898, as amended.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds being in the affirmative, the ayes have it.

Mr. BARR. Mr. Speaker, on that I demand the yeas and nays.

The yeas and nays were ordered.

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX, further proceedings on this motion will be postponed.

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

Mr. MCCAUL. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 3101) to enhance cybersecurity information sharing and coordination at ports in the United States, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 3101

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act 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 Secretary of Homeland Security shall—

(1) develop and implement a maritime cybersecurity risk assessment model within 120 days after the date of the enactment of this Act, consistent with the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity and any update to that document pursuant to Public Law 113–274, to evaluate current and future cybersecurity risks (as such term is defined in section 227 of the Homeland Security Act of 2002 (6 U.S.C. 148));

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

(3) seek to ensure participation of at least one information sharing and analysis organization (as such term is defined in section 212 of the Homeland Security Act of 2002 (6 U.S.C. 131)) representing the maritime community in the National Cybersecurity and Communications Integration Center, pursuant to subsection (d)(1)(B) of section 227 of such Act;

(4) establish guidelines for voluntary reporting of maritime-related cybersecurity risks and incidents (as such terms are defined in section 227 of such Act) to the Center (as such term is defined subsection (b) of such section 227), and other appropriate Federal agencies; and

(5) request the National Maritime Security Advisory Committee established under section 70112 of title 46, United States Code, to report and make recommendations to the Secretary on enhancing the sharing of information related to cybersecurity risks and incidents, consistent with the responsibilities of the Center, between relevant Federal agencies and—

(A) State, local, and tribal governments;

(B) relevant public safety and emergency response agencies;

(C) relevant law enforcement and security organizations;

(D) maritime industry;

(E) port owners and operators; and

(F) terminal owners and operators.

SEC. 3. CYBERSECURITY ENHANCEMENTS TO MARITIME SECURITY ACTIVITIES.

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

(1) each Area Maritime Security Advisory Committee established under section 70112 of title 46, United States Code, to facilitate the sharing of cybersecurity risks and incidents to address port-specific cybersecurity risks, which may include the establishment of a working group of members of Area Maritime Security Advisory Committees to address port-specific cybersecurity vulnerabilities; and

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

SEC. 4. VULNERABILITY ASSESSMENTS AND SECURITY PLANS.

Title 46, United States Code, is amended—

(1) in section 70102(b)(1)(C), by inserting ''cybersecurity,'' after ''physical security,''; and

(2) in section 70103(c)(3)(C), by striking ''and'' after the semicolon at the end of clause (iv), by redesignating clause (v) as clause (vi), and by inserting after clause (iv) the following:

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

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Texas (Mr. MCCAUL) and the gentleman from Texas (Mr. VELA) each will control 20 minutes.

The Chair recognizes the gentleman from Texas (Mr. MCCAUL).

GENERAL LEAVE

Mr. MCCAUL. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days within which to revise and extend their remarks and include extraneous material on the bill under consideration.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Texas?

There was no objection.

Mr. MCCAUL. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I rise today in support of the Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act.

More than $1.3 trillion in cargo travels through American seaports along our coasts every year. A safe but constant and unrestricted flow of goods and services through our maritime transportation system have played a vital role in allowing the United States to become the global superpower it is today. To put it simply, our seaports are the gateways to our economic survival.

Unfortunately, as our port systems increasingly benefit from new technology, high-capacity information technology, and computer systems, they are also increasingly finding themselves in the crosshairs of those who are waging a cyber war against the United States. These attacks originate from rogue hackers, terrorist groups, and adversarial nation-states, and America is a constant target.

In recent years, China successfully stole over 20 million security clearances from OPM. Russia has waged a cyber war against our political system. Equifax had a breach that jeopardized sensitive information on over 43 million people.

In June, the Port of Los Angeles, one that several of our committee members will be visiting next week, was briefly shut down because of a cyber attack. This is one of our busiest ports, and it is estimated that it cost nearly $300 million in economic damage. We must do more to strengthen cybersecurity of these essential maritime hubs.

Fortunately, we have that opportunity. The legislation before us requires the Department and the Secretary of Homeland Security to implement a risk assessment model which focuses on cybersecurity vulnerabilities and risk. This assessment will be reviewed periodically so we can determine the best security practices to implement at each port.

The bill also requires that the DHS Secretary work with the National and Area Maritime Security Advisory Committees to analyze and share cyber risks and to report to Congress measures that have been taken to improve cybersecurity at our Nation's ports. This bill will strengthen the security of our homeland and protect our economic assets.

Mr. Speaker, I want to thank Congresswoman TORRES and other members of the Homeland Security Committee for their hard work on this issue. I urge my colleagues to support this commonsense bill, and I reserve the balance of my time.

COMMITTEE 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.

Mr. VELA. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I stand today in support of H.R. 3101, the Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act.

Port facilities serve as a vital economic function for our Nation and the communities in which they are located. The approximately 360 commercial maritime ports operating across the United States handle more than $1.3 trillion in cargo, annually.

To facilitate and maintain this level of economic activity, the maritime sector increasingly relies on technology to facilitate the movement of cargo into and through port facilities. Collectively, navigation, operations, and communication technologies enhance the competitiveness, safety, and reliability of the U.S. maritime sector.

However, as port operations have become more automated, exposure to cyber threats and attacks have also increased. This homeland security threat is not unique to the maritime sector. In fact, since 2003, the Government Accountability Office has warned about the vulnerability of critical infrastructure and has called on the Federal Government to support efforts to bolster cybersecurity.

To better protect port facilities from cyber attacks, Congress must ensure that expertise in both the private and public sector is leveraged effectively. H.R. 3101 would direct DHS to be more proactive in how it addresses cybersecurity risks at our Nation's ports.

The first step in reducing cyber vulnerabilities is identifying the weak points in network security through risk assessments. H.R. 3101 requires these assessments. The bill directs the Coast Guard to provide port facilities with guidelines on how to report cybersecurity risks in order to enhance the ability of both the Coast Guard and port operators to respond effectively to such attacks.

By promoting cybersecurity information sharing and coordination between public and private partners at maritime facilities, H.R. 3101 seeks to make a positive difference in how quickly terminal and port operators are able to prevent, mitigate, and recover from such attacks.

H.R. 3101, if enacted, will help foster an environment in which DHS, the Coast Guard, ports, and port stakeholders work together to enhance the cybersecurity at our Nation's ports.

Lastly, I would like to note the bipartisan support for this bill in the Homeland Security Committee. I thank Chairman MCCAUL, Ranking Member THOMPSON, and my colleague Congresswoman TORRES for their hard work and leadership in this matter.

Mr. Speaker, when this bill was considered last Congress and earlier this fall, committee colleagues on both sides of the aisle agreed that H.R. 3101 is a timely and worthwhile measure to support. I urge my colleagues to support H.R. 3101.

Mr. Speaker, I yield 5 minutes to the gentlewoman from California (Mrs. TORRES).

Mrs. TORRES. Mr. Speaker, before I begin, I want to thank the chairman and also Ranking Member THOMPSON and Ranking Member VELA and all of their committee staff for their great work and support of this very important legislation. We would not be here today without their commitment to keeping our ports safe. Thank you.

Mr. Speaker, you can't turn on the television or visit your favorite website without seeing cyber threats dominating the news. All industries, including our own Federal agencies, have been targets, costing our economy dearly and exposing the personal information of hundreds of millions of employees.

This is a growing problem that is not going away. Rather, these threats are becoming more common and more severe. From the interference in our elections to attacks on government workers, email hacks, and the theft of credit card information, cyber threats are everywhere, and it is time that we modernize the Federal Government's planning and response to these threats.

In June, a Danish shipping company was infected with malware that affected 17 of its shipping container terminals worldwide. The virus spread to 2 million computers within a 2-hour period. As a result, the largest terminal at the Port of Los Angeles shut down for 4 days from the cyber attack.

A recent study estimated the cost of a shutdown of the Port of Los Angeles and Long Beach at $1 billion per day to the local economy.

More than $1.3 trillion in cargo moves, annually, through our Nation's 360 commercial ports, and many of the goods that enter through the Port of Los Angeles and the Port of Long Beach come to my district before being shipped to the rest of the country.

With this much economic activity and the increased use of cyber technology to manage port operations ranging from communications and navigation to engineering, safety, and cargo, it is critical to protect our maritime cyber infrastructure.

□ 1500

It is time that Congress modernize our Federal agencies. This is why I am proud to bring the Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act to the floor today.

This legislation would improve information sharing and cooperation in addressing cybersecurity risks at our Nation's ports through several measures: setting standards for reporting, providing guidance to ports, bringing port representatives to the table for future planning, and modernizing how the Coast Guard addresses cyber threats.

Mr. Speaker, these are commonsense measures. This bill has bipartisan support. The Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act passed the House unanimously last year, and I am confident that passage today will push the Senate into action.

This legislation is supported by the Port of Los Angeles, Congressional PORTS Caucus chairs, and it is endorsed by the Maritime & Port Security Information Sharing and Analysis Organization. I urge my colleagues to support this legislation because we simply can't afford not to. Ports are too critical to our economy and our Nation.

Mr. MCCAUL. Mr. Speaker, I have no other speakers. If the gentleman from Texas has no other speakers, I am prepared to close once the gentleman does.

Mr. Speaker, I reserve the balance of my time.

Mr. VELA. Mr. Speaker, I yield myself the balance of my time.

H.R. 3101 will help improve the way we manage cybersecurity risks at our Nation's commercial maritime ports. With the increased need for and use of technology at maritime facilities, it is in our national and economic interest for there to be better cyber information sharing and coordination efforts at our Nation's ports.

By assessing cyber risks at individual port facilities and establishing countermeasures to mitigate these risks, the U.S. maritime sector will be better prepared to protect these important centers of economic activity.

Mr. Speaker, I encourage my colleagues to support H.R. 3101, and I yield back the balance of my time.

Mr. MCCAUL. Mr. Speaker, I yield myself the balance of my time.

I once again urge my colleagues to support this important legislation. I want to thank Congresswoman TORRES for her strong leadership on this bill, Mr. VELA, Ranking Member THOMPSON.

Mr. Speaker, we have passed over 50 bills out of my committee, out of the House floor, and sent them to the Senate, where they still sit there with no action whatsoever. And when it comes to homeland security measures, I believe that it is dangerous to do nothing, and I urge the Senate to take up action on this bill and the other 50 bills that we have sent over to the Senate.

Mr. Speaker, I yield back the balance of my time.

Ms. JACKSON LEE. Mr. Speaker, I rise in support of H.R. 3101, the Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2017.

I thank Congresswoman TORRES for introducing this important piece of legislation that addresses security at our nation's ports.

H.R. 3101 requires the Department of Homeland Security (DHS) to facilitate increased information sharing about cybersecurity among maritime interests.

The bill requires DHS to:

Develop, implement, and continually review a maritime cybersecurity risk assessment model to evaluate current and future cybersecurity risks;

Seek input from at least one information sharing and analysis organization representing maritime interests in the National Cybersecurity and Communications Integration Center;

Establish voluntary reporting guidelines for maritime-related cybersecurity risks and incidents;

Request that the National Maritime Security Advisory Committee report and make recommendations to DHS about methods to enhance cybersecurity and information sharing among security stakeholders from federal, state, local, and tribal governments; public safety and emergency response agencies; law enforcement and security organizations; maritime industry participants; port owners and operators; and maritime terminal owners and operators; and

Ensure that maritime security risk assessments include cybersecurity risks to ports and the maritime border of the United States.

As a senior member of the House Committee on Homeland Security and former Ranking Member of the Committee's Subcommittee on Border and Maritime Security, I am well aware of the hard work that the Houston Port Authority, and the Department of Homeland Security has done to secure the port, its workers, and the millions of tons of imports and exports that traverse the waters of the Port of Houston each week.

According to the U.S. Department of Transportation the U.S. maritime border covers 95,000 miles of shoreline with 361 seaports.

Ocean transportation accounts for 95 percent of cargo tonnage that moves in and out of the country, with 8,588 commercial vessels making 82,044 port calls in 2015.

The Port of Houston is a 25-mile-long complex of diversified public and private facilities located just a few hours' sailing time from the Gulf of Mexico.

In 2012, ship channel-related businesses contributed 1,026,820 jobs and generated more than $178.5 billion in statewide economic activity.

In 2014, among U.S. ports the Port of Houston was ranked:

1st in foreign tonnage;

Largest Texas port with 46 percemt of market share by tonnage and 95 percent market share in containers by total TEUS in 2014;

Largest Gulf Coast container port, handling 67 percent of U.S. Gulf Coast container traffic in 2014;

2nd in total foreign cargo value (based on U.S. Dept. of Commerce, Bureau of Census).

The Government Accountability Office (GAO) reports that the Port of Houston port, and its waterways, and vessels are part of an economic engine handling more than $700 billion in merchandise annually.

The Port of Houston houses approximately 100 steamship lines offering services that link Houston with 1,053 ports in 203 countries.

The Port of Houston is a $15 billion petrochemical complex, the largest in the nation and second largest worldwide.

These statistics clearly communicate the potential for a terrorist attack using nuclear or radiological material may in some estimations be low, but should an attack occur the consequences would be catastrophic, and for this reason we cannot be lax in our efforts to deter, detect and defeat attempts by terrorists to perpetrate such a heinous act of terrorism.

The Department of Homeland Security (DHS) plays an essential role in domestic defense against the potential smuggling of a weapon of mass destruction in a shipping container or the use of a bomb-laden small vessel to carry out an attack at a port.

Earlier this year, a global malware attack occurred that caused significant harm to international shipping giant A.P. Moller-Maersk.

That attack revealed serious vulnerabilities in our nation's maritime security, which is still being assessed.

The only way port operations were able to resume following the attack at one of our nation's busiest ports was to revert to a manual system to process cargo and ships.

This was not the first time that cyber criminals used technology against port operations.

Approximately $1.3 trillion in cargo passes through our nation's 360 commercial ports.

The convenience, precision and accuracy provided by digital technology in processing cargo through our nation's ports adds to their capacity to manage tonnage.

Securing cyber technology to manage port operations, ranging from communication and navigation to engineering, safety, and cargo, is critical to protect our nation's maritime cyber infrastructure.

Government leaders and security experts are concerned that the maritime transportation system could be used by terrorists to smuggle personnel, weapons of mass destruction, or other dangerous materials into the United States.

They are also concerned that ships in U.S. ports, particularly large commercial cargo ships or cruise ships, could be attacked by terrorists.

A large-scale terrorist attack at a U.S. port, experts warn, could not only cause local death and damage, but also paralyze global maritime commerce.

This is of particular concern at the Port of Houston, which is the busiest port in the nited States in terms of foreign tonnage, second-busiest in the United States in terms of overall tonnage, and fifteenth-busiest in the world.

DHS, through U.S. Customs and Border Protection, the Transportation Security Administration, and the U.S. Coast Guard, administers several essential programs that secure our Nation's ports and waterways.

I include in the RECORD a letter dated March 30, 2017, that I sent to the Chair and Ranking Member of the Committee on Homeland Security requesting a field hearing on the topic of port security.

I ask my colleagues join me in voting to pass H.R. 3101, the Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2017.

CONGRESS OF THE UNITED STATES,
HOUSE OF REPRESENTATIVES,
Washington, DC, March 30, 2017.

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

Hon. BENNIE THOMPSON,
Ranking Member, House Committee on Homeland Security, House of Representatives, Washington, DC.

DEAR CHAIRMAN MCCAUL AND RANKING MEMBER THOMPSON: Your leadership to secure the homeland from terrorist attacks by putting the needs of the nation first in matters before the Committee is commendable. I am writing to request that as Chair and Ranking Member that you invite senior members of the Committee to join you for a meeting with Houston Port facility security and industrial manufacturing professionals to discuss the work and industry that takes place at that port.

The issue of port security remains integral to our Committee's work, and this opportunity for you, and senior members of the committee to learn more about modern ports is appreciated. Ports are indispensable to our nation's economic health as engines of commercial transportation as well as the gateway for food and essential goods to the nation's interior. The evolution of major ports, like the Port of Houston into co-location sites for manufacturing means port security challenges have expanded.

Thank you for your work to secure our nation from terrorist threats by keeping the committee abreast of the most critical security issues facing our nation. I look forward to your positive reply to this request.

Very truly yours,

SHEILA JACKSON LEE,
Member of Congress.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Texas (Mr. MCCAUL) that the House suspend the rules and pass the bill, H.R. 3101, as amended.

The question was taken; and (two-thirds being in the affirmative) the rules were suspended and the bill, as amended, was passed.

A motion to reconsider was laid on the table.

STOP SETTLEMENT SLUSH FUNDS ACT OF 2017

GENERAL LEAVE

Mr. GOODLATTE. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days within which to revise and extend their remarks and include extraneous materials on H.R. 732.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Virginia?

There was no objection.

The SPEAKER pro tempore. Pursuant to House Resolution 577 and rule XVIII, the Chair declares the House in the Committee of the Whole House on the state of the Union for the consideration of the bill, H.R. 732.

The Chair appoints the gentleman from Oklahoma (Mr. LUCAS) to preside over the Committee of the Whole.

□ 1504

IN THE COMMITTEE OF THE WHOLE

Accordingly, the House resolved itself into the Committee of the Whole