gentleman from Texas (Mr. MCCAUL), the chairman of the Homeland Security Committee.

Mr. MCCAUL. Mr. Speaker, I want to first thank Chairman LOBIONDO for his hard work on this legislation. And I want to thank the House Intelligence Committee for working closely with my committee to get this important legislation done. I can think of no more timely piece of legislation. I want to thank Ranking Member SWALWELL from California for his hard work on this as well.

Mr. Speaker, I rise in support of this bill. Hundreds of our people have been radicalized, lured to the jihadist safe haven in Syria. They have been joined by thousands of Westerners, forming a terrorist army unlike anything we have ever seen.

These foreign fighters represent a triple threat: They strengthen groups like ISIS on the ground; they radicalize others back home; and, worst of all, they may be sent back to conduct terrorist attacks against us in the homeland.

We saw this in the streets of Paris, where battle-hardened extremists returned from Syria prepared to kill. And here at home, we have arrested so-called returnees from Syria, including one individual plotting a terrorist attack in Ohio.

Earlier this year, I launched a bipartisan congressional Task Force on Combating Terrorists and Foreign Fighter Travel. One of their findings was that we must do more to track ''the great jihadi migration'' around the world.

Our intelligence about foreign fighters in Syria is improving, but as we have seen, the threat can change almost overnight. ISIS is already urging its followers to go to its other sanctuaries in places like Afghanistan and Libya.

We need to stay a step ahead of this threat, which is why this legislation requires the intelligence community to track extremist travel patterns and to report on a regular basis to Congress. It also requires agencies to monitor the number of U.S. citizens in terror hotspots and to report on how many individuals have departed those locations.

This is the kind of early-warning intelligence we need in order to create a ''firebreak'' to slow the spread of Islamist terror, and to keep Americans from being lured to new jihadist safe havens.

I would like to commend the task force for their hard work on this, including Mr. KATKO.

And let me just say this. I get regular threat briefings, and I have never seen a higher threat environment than we have seen since 9/11, and it is from the flow of foreign fighters.

We have 5,000 of them that have Western passports, 30,000 foreign fighters from 100 different countries; 250 Americans have left to join the fight, and, Mr. Speaker, that is just who we know about.

Now we know they are communicating in dark space. As the Director of the FBI says, they have one simple message: Come to fight in Syria or kill where you are. Unfortunately, we have seen them too often come to fight in Syria and, unfortunately, just recently, too many that have come to kill here in the United States.

Mr. SWALWELL of California. Mr. Speaker, I yield 2 minutes to the gentleman from Illinois (Mr. QUIGLEY).

Mr. QUIGLEY. Mr. Speaker, in these trying times, Congress needs to provide leadership and answer the question: What really keeps Americans safe?

ISIS has directed U.S. and Western passport holders to launch attacks at home and abroad, and this threat requires our vigilance. But it is foolish to think we can effectively combat this terrorism blindly. Congress needs an accurate estimation of the number of foreign fighters who have traveled to terrorist havens like Syria. We need to know how many U.S. citizens are currently there, and we need to know the whereabouts of those who have left.

Given that many of the terrorist attackers were European nationals, the need for this intelligence is crucial in the fight against ISIS and those who wish to harm the U.S.

The Tracking Foreign Fighters in Terrorist Safe Havens Act provides for a more clear understanding of the real threats to U.S. security and allows Congress to work in partnership with our national security agencies to defend against these threats. I am happy to support this commonsense step to keep Americans safe.

Mr. LOBIONDO. Mr. Speaker, I have no additional speakers on this side, so I reserve the balance of my time.

Mr. SWALWELL of California. Mr. Speaker, I yield myself such time as I may consume.

Again, I want to thank the gentleman from New Jersey for working in a bipartisan way to address one of the greatest threats that the United States, our allies, and people in the Middle East face today, and that is ISIS. ISIS is a brutal, growing force, growing in its influence and ability to carry out successful terrorist attacks, but also growing in its ability to inspire others to take up attacks on their own.

ISIS has been so successful these days that they don't even have to order attacks here in America. Their success has inspired others to take up their own attacks. Until we are as coordinated as they are, they will continue to be successful. We saw, in Paris, that a number of the attackers were people who had traveled from Western Europe to Syria and then returned to carry out the horrific attacks we saw back in November.

But we can defeat ISIS. We have defeated evil as a country before, and this country works best when its leaders work to protect the American people in a bipartisan way, as we are seeing today.

There is no silver bullet we can fire to stop ISIS. Instead, ISIS' defeat will come at the hands of American leadership—American leadership in stitching together a coalition of countries willing and able to defeat ISIS—but also American leadership and its own intelligence community to protect us here at home.

Mr. Speaker, let me close by reiterating my strong support for the Tracking Foreign Fighters in Terrorist Safe Havens Act. The information that this will provide is an important step regarding foreign fighter training, and it will be of great importance as we continue to fight terrorism at home and abroad and secure our homeland.

Again, I thank the gentleman from New Jersey.

I yield back the balance of my time.

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

Once again, I join in thanking my colleague from California (Mr. SWALWELL). I think the approach we have had to this is exactly what we need in combating terrorism.

It is hard to imagine, even just a few years ago, that we would be facing this threat that we face today and this threat of terrorism that we have seen, this barbaric face in Paris and in San Bernardino, the fact that the enemy is evolving in so many different ways, and the fact that we have to be right 100 percent of the time and that they have so many different avenues that they can pursue.

This piece of legislation is another piece to the puzzle which will help our country and our agencies be able to figure things out. Our intelligence community works tirelessly with law enforcement to be able to figure out what the next challenge is.

I hope the people of America understand the expertise and professionalism that the intelligence community and law enforcement bring to the table to keep our country safe. I hope my colleagues understand how important this legislation is and everyone votes ''yes'' to support it.

I yield back the balance of my time.

The SPEAKER pro tempore (Mr. TIPTON). The question is on the motion offered by the gentleman from New Jersey (Mr. LOBIONDO) that the House suspend the rules and pass the bill, H.R. 4239, 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. LOBIONDO. 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 2015

Mrs. MILLER of Michigan. Mr. Speaker, I move to suspend the rules

and pass the bill (H.R. 3878) 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. 3878

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 2015''.

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 that term is defined in the second section 226 of the Homeland Security Act of 2002 (6 U.S.C. 148));

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

(3) seek to ensure participation of at least one information sharing and analysis organization (as that 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 the second section 226 of the Homeland Security Act of 2002 (6 U.S.C. 148);

(4) establish guidelines for voluntary reporting of maritime-related cybersecurity risks and incidents (as such terms are defined in the second section 226 of the Homeland Security Act of 2002 (6 U.S.C. 148)) to the Center (as that term is defined subsection (b) of the second section 226 of the Homeland Security Act of 2002 (6 U.S.C. 148)), 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 between relevant Federal agencies and State, local, and tribal governments and consistent with the responsibilities of the Center (as that term is defined subsection (b) of the second section 226 of the Homeland Security Act of 2002 (6 U.S.C. 148)); relevant public safety and emergency response agencies; relevant law enforcement and security organizations; maritime industry; port owners and operators; and 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 security plan and 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.

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 gentlewoman from Michigan (Mrs. MILLER) and the gentlewoman from California (Mrs. TORRES) each will control 20 minutes.

The Chair recognizes the gentlewoman from Michigan.

GENERAL LEAVE

Mrs. MILLER of Michigan. Mr. Speaker, I ask unanimous consent that all Members have 5 legislative days within which to revise and extend their remarks and include any extraneous materials on the bill under consideration.

The SPEAKER pro tempore. Is there objection to the request of the gentlewoman from Michigan?

There was no objection.

Mrs. MILLER of Michigan. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I rise in support of H.R. 3878, and I urge its passage.

Since the terrorist attacks of 9/11, the U.S. Congress has appropriated $2.4 billion in port security grant funds to protect port facilities against potential terror attacks. As a nation, we have done a fairly good job of updating the physical security at ports, but the U.S. Government has been very slow to ensure that our ports are secure from cyber vulnerabilities.

For example, cybersecurity of our Nation's critical infrastructure has been on the Government Accountability Office's High Risk List since 2003, yet we have not fully engaged on cybersecurity efforts at the Nation's 360 seaports.

The threat of a cyber attack is real, and, when addressing the protection of maritime critical infrastructure, we must clearly define the roles and responsibilities for ensuring our Nation's ports are protected.

Under the Maritime Transportation Security Act of 2002, the Coast Guard is identified as the government agency responsible for ensuring the physical security at our Nation's port infrastructure. This bill makes it clear that the Coast Guard is also the primary agency responsible for ensuring the maritime sector is prepared to prevent and to respond to cybersecurity risk and vulnerability.

More than $1 trillion of goods—from cars, to oil, to corn, and everything in between—move through our Nation's seaports each and every year. Like many industries in America, port facilities and ship operators are increasingly moving cargo through our ports using automated industrial control systems.

While this automation certainly has a lot of benefits, such as reducing the time that it takes to stock our shelves and lowering the cost of doing business, it doesn't come without risks. These computer systems are controlling machinery at port facilities to move containers and fill tanks and onload and offload ships.

Terror groups, nation-states, criminal organizations, hackers, and even disgruntled employees could breach these systems, with potentially catastrophic results to the Nation's security and economy.

Breaches in the maritime domain are particularly concerning, not only from an economic standpoint, but because the dangerous cargos, such as liquefied natural gas and other dangerous cargos, that also pass through our Nation's seaports are at risk.

Just as we have hardened physical security at our Nation's ports, we need to do the same in virtual space to protect the systems critical to the maritime transportation system against malicious actors. This bill does just that, and it requires the Coast Guard to develop a comprehensive cyber risk assessment specific to the vulnerabilities of the maritime industry. It directs the Secretary of Homeland Security to encourage participation with information sharing to better streamline coordination at the national level.

H.R. 3878 is a bipartisan piece of legislation, introduced by my colleague from California (Mrs. TORRES), and I give her great credit for this piece of legislation, working with so many Members on this. It actually is the result of a hearing held by the Homeland Security Subcommittee that I chaired back in October on the subject of cybersecurity at our Nation's ports.

□ 1230

The bill clarifies the Department of Homeland Security's role in maritime cybersecurity as well as it ensures that port facilities work with the Coast Guard to identify cyber risks and vulnerabilities and share best practices across the industry. This is the first step, Mr. Speaker, in protecting our ports from cyber threats, and I certainly urge my colleagues to join this commonsense, bipartisan legislation.

Again, I want to thank the gentlewoman from California for her work on this issue.

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

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

Mr. Speaker, I rise in support of H.R. 3878, the Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act.

Mr. Speaker, I introduced H.R. 3878, the Strengthening Cybersecurity Information Sharing and Coordination in

Our Ports Act, to ensure the Department of Homeland Security takes a more proactive approach to address cybersecurity risks at our Nation's ports and to improve cybersecurity information sharing and coordination between public and private partners at maritime facilities.

The United States has approximately 360 commercial sea and river ports which use cyber technology to move over $1 trillion worth of cargo each year. The Ports of Los Angeles and Long Beach and other ports in California account for almost 40 percent of the cargo entering this country, and nearly 30 percent of the country's exports leave through California ports.

The Port of Los Angeles is the number one port by container volume and cargo value in the United States, seeing around $1.2 billion worth of cargo each day. Each year, the Port of Long Beach handles more than 6.8 million 20-foot container units in cargo value at $180 billion and is the second busiest port in the U.S. With so much economic activity happening at our Nation's ports, protecting the cyber networks they rely on is critical to our local and national economy.

This past October, the Subcommittee on Border and Maritime Security on which I serve held a hearing focused on the threat of cyber attacks at a port and how the Coast Guard is working with private and public partners to protect maritime critical infrastructure against such attacks. This is of particular interest to me because many of the goods that enter through the Ports of Long Beach and Los Angeles come directly to my district where the goods are redistributed throughout the Nation. The hearing was called in response to a June 2014 GAO report recommending the Department of Homeland Security take action to strengthen cybersecurity at our Nation's ports.

Mr. Speaker, the report found that maritime Sector Coordinating Councils are no longer active. These councils include port owners, operators, and related private industry associations. This means that today there is no one entity that coordinates information sharing between the ports, the private sector, and government stakeholders.

At the October subcommittee hearing, we received testimony that information sharing on cyber risks at ports should be stronger and that some ports lack the resources to prevent, identify, and respond to cyber attacks. To address these challenges, I introduced H.R. 3878, which will require the Secretary of Homeland Security and the Commandant of the U.S. Coast Guard to take several steps to enhance cybersecurity at our ports.

Specifically, it requires the Secretary of Homeland Security to establish guidelines for reporting cybersecurity risks, to develop and implement a maritime cybersecurity risk model, and to make recommendations on enhancing the sharing of cyber information. It also requires the Coast Guard to direct Area Maritime Security Committees to address cybersecurity risks. These measures will create an environment where DHS, the Coast Guard, ports, and stakeholders work together to enhance cybersecurity at our Nation's ports.

Mr. Speaker, I would like to thank Chairman MCCAUL and Subcommittee Chairwoman MILLER for their cooperation and the bipartisan nature of the staff discussions on this bill. Mr. Speaker, I urge my colleagues to support H.R. 3878.

I reserve the balance of my time.

Mrs. MILLER of Michigan. Mr. Speaker, I yield such time as he may consume to the distinguished gentleman from New York (Mr. DONOVAN).

Mr. DONOVAN. Mr. Speaker, I rise today in support of H.R. 3878, the Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2015.

This bill by my friend Representative TORRES contains an amendment I offered at committee, which makes an important change to the Maritime Transportation Security Act of 2002.

More than $1.3 trillion worth of cargo travels through U.S. ports each year, making them a truly critical part of our Nation's infrastructure. Any disruption or slowdown of activity could have a tremendous impact on the entire economy, costing billions of dollars every day.

Ensuring the security of our maritime infrastructure is a complex task and one that falls primarily on the United States Coast Guard. However, while the Coast Guard has the history and the expertise to provide physical security, its mission of ensuring that our maritime infrastructure is safe from cyber threats is still evolving.

Currently, the Maritime Transportation Security Act of 2002 requires vessels and port facilities to conduct vulnerability assessments and develop security plans for physical security, access controls, procedural security measures, and communication systems. My amendment in committee added cybersecurity to that list. This addition will make it crystal clear that the Coast Guard has the specific authority to require maritime vessels and facilities to incorporate cybersecurity into their assessments and plans.

The need for this change and the underlying legislation was highlighted during a hearing before the Border and Maritime Security Subcommittee on the topic of cybersecurity at our Nation's ports. In that hearing, we heard how a range of actors—from narcotics traffickers to terrorist organizations, and even nation-states—could exploit cyber vulnerabilities at our ports for the purpose of smuggling illicit materials or causing severe economic disruption. Mr. Speaker, this legislation will ensure that we are better prepared to respond to the growing cyber threat to our Nation's maritime infrastructure.

I thank Representative TORRES for offering this legislation and for accepting my amendment at committee.

Mr. Speaker, I urge my colleagues to support the bill.

Mrs. TORRES. Mr. Speaker, I yield 3 minutes to the gentleman from California (Mr. LOWENTHAL).

(Mr. LOWENTHAL asked and was given permission to revise and extend his remarks.)

Mr. LOWENTHAL. I thank the gentlewoman for yielding.

Mr. Speaker, I rise in support of H.R. 3878, the Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2015.

Mr. Speaker, in southern California, I represent the Port of Long Beach, which is one of the busiest seaports in the country, is set to handle more than 7 million containers this year, and accounts for nearly 20 percent of all the loaded containers moving throughout our Nation. It is a critical link for trade between our country and Asia and is a linchpin for our national security and our national economy. In other words, the security of the Port of Long Beach is not to be treated lightly.

I am not a stranger to the critical nature of the port, but we are now learning about emerging port-specific cyber threats. This body recently took the first steps to fight off the growing threats to our Nation's cybersecurity with a number of bills and hearings on this topic. I am glad that out of those hearings, our attention now turns to the cybersecurity of our critical infrastructure, including the hundreds of cargo ports in this country.

As a result of H.R. 3878, we would see working groups forming at our ports and coming together to address port-specific cybersecurity vulnerabilities. These findings would be shared with appropriate stakeholders, including Federal and local governments, port authorities, terminal operators, as well as law enforcement, in an effort to enhance cybersecurity situational awareness at the ports.

Mr. Speaker, I am confident that these working groups will continue to find innovative solutions in response to this emerging threat. Within the working groups, I hope that they will codify key definitions and classification mechanisms and that they will come out of these discussions to ensure the effectiveness of the group.

In closing, Mr. Speaker, I urge my colleagues to support this important bill.

Mrs. MILLER of Michigan. Mr. Speaker, I reserve the balance of my time.

Mrs. TORRES. Mr. Speaker, I yield 3 minutes to the gentlewoman from California (Ms. HAHN).

Ms. HAHN. I thank my colleague, Congresswoman TORRES, for introducing this very important bill.

Mr. Speaker, as co-chair and co-founder of the Congressional PORTS Caucus and also as a representative of the busiest port complex in the Nation,

I have long advocated for much-needed cybersecurity at our Nation's ports.

In 2013, a report by the Brookings Institution found that there is a serious cybersecurity gap at many of our Nation's ports, putting them at risk for an attack. A significant cyber attack at one of our major ports could bring commerce in an entire region to a halt and send shock waves throughout the national and global economies.

This is a problem that needs to be addressed, but unfortunately, we do not have a clear picture of where cybersecurity vulnerabilities exist at our ports.

Earlier this year, the House passed my amendment to instruct the Department of Homeland Security to identify gaps in cybersecurity at the Nation's 10 most at-risk ports and then to make recommendations for how we can address these problems. I am pleased that that amendment has been included in the omnibus that we will be voting on later this week.

Mr. Speaker, the bill we are talking about today expands on this progress and is a great vehicle to identify cybersecurity problems at our Nation's ports. I would like to commend my colleague Congresswoman TORRES for bringing this important issue to the floor.

Mr. Speaker, I urge all my colleagues to vote ''yes'' on this bill.

Mrs. MILLER of Michigan. Mr. Speaker, I have no further speakers. If the gentlewoman from California is prepared to close, I will then close for our side.

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

Mr. Speaker, H.R. 3878 will enhance our understanding of cyber risks at our ports and the countermeasures needed to mitigate them.

With the increased levels of technology at maritime facilities, all public and private port stakeholders must share information and coordinate efforts to make sure that our Nation's ports are protected from cyber attacks.

Again, I appreciate the bipartisan cooperation on this legislation.

Mr. Speaker, I encourage my colleagues to support H.R. 3878.

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

Mrs. MILLER of Michigan. Mr. Speaker, I simply, once again, urge my colleagues to support H.R. 3878. It is a very good bill, and it is a very important bill—again, in a bipartisan way—for the security of our ports and the homeland security of our Nation as well.

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

Ms. JACKSON LEE. Mr. Speaker, I speak in support of H.R. 3878, the Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act.

I thank Chairman MCCAUL and Ranking Member THOMPSON for their bipartisan work and stewardship of the Committee on Homeland Security's work, which includes H.R. 3878.

Congresswoman TORRES should be commended for her hard work that led to the introduction of the Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act.

H.R. 3878, requires the Department of Homeland Security (DHS) to seek to enhance cybersecurity situational awareness and information sharing between maritime security stakeholders, the maritime industry, port owners and operators, which include maritime terminal owners and operators.

This bill requires DHS to:

consult with the Coast Guard to enhance participation by the Maritime Information Sharing and Analysis Center in the National Cybersecurity and Communications Integration Center; and

request that the National Maritime Security Advisory Committee report and make recommendations to DHS on methods to enhance cybersecurity and information sharing between stakeholders.

The bill also assures DHS leadership in port security by requiring the agency's maritime security risk assessments to include cybersecurity risks to ports and the maritime border of the United States.

Ports serve as America's gateway to the global economy. The nation's economic prosperity rests on the ability of containerized and bulk cargo arriving unimpeded at U.S. ports to support the rapid delivery system that underpins the manufacturing and retail sectors.

My service in the House of Representatives has focused on making sure that our nation is secure and prosperous.

A central component of national security is the ability of our International Ports to move goods into and out of the country.

The Port of Houston is critical infrastructure:

According to the Department of Commerce in 2012, Texas exports totaled $265 billion.

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 impact.

In 2014, the Port of Houston was ranked among U.S. ports as the 1st in foreign tonnage; largest Texas port with 46 percent 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; and 2nd ranked U.S. port in terms of total foreign cargo value.

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

A Maritime Cyber-RISKS report published in 2014 outlined examples of cybersecurity vulnerabilities that are specific to ports.

The Cyberattacks examined included:

Theft of money by deceiving a company into transferring large amounts of funds to a bank account owned by criminals;

In 2013, the FBI issued a warning to maritime companies warning them of a fraud committed against several companies using a man-in-the-middle cyberattack that resulted in $1.65 million in losses.

In this attack an impersonation occurs when the email address of a trusted party is co-opted or taken over by an unknown 3rd party.

The trusted 3rd party makes a request to change banking information that should be used to provide payment for legitimate services provided an established business relationship.

The legitimate business is not aware of the request to change bank payment information.

When the payment is sent, thieves receive it and quickly close the account so that the funds cannot be retrieved.

Another malicious attack that does not involve theft of funds can occur if the location of cargo information is deleted by a cyber-attacker.

According to CyberKeel this type of attack happened to a shipping company in 2011.

In this attack data related to rates, loading, cargo number, date and place were corrupted.

This cyberattack meant that no one at the port could identify where containers were, whether they loaded, nor identify which containers were on ships.

Cyberattack that targeted technology used by companies who are taking receipt of cargo at port locations.

The Firmware software code on handheld scanning technology that reads barcodes on containers was corrupted by malware.

When the scanners were plugged into the company's network the corrupted code started a series of automated cyberattacks that searched the company's network for financial information.

After finding the information, a connection was established with a computer in China.

Cyberattack at the Port of Antwerp was run by a drug smuggling ring.

In this attack the cyber criminals were able to gain control of the port terminal system that allowed them to release containers to their own trucks without the knowledge of port authorities.

This attack is particularly chilling when considering our efforts to protect against weapons of mass destruction in the form of biological, nuclear and chemical weapons from being brought into the country undetected.

This type of attack also has implications for persons entering the country undetected.

The same attack carried out against port worker automated identification systems would open the door on a host of domestic security issues.

Our nation has thousands of miles of coastlines, lakes, and rivers and hundreds of ports that provide opportunities for legitimate travel, trade, and recreation.

At the same time, these waterways offer opportunities for terrorists and their instruments, and drug smugglers to enter our country.

Cybersecurity at ports must be national priority, for this reason, I ask my colleagues to join me in voting in favor of H.R. 3878.

The SPEAKER pro tempore (Mr. DONOVAN). The question is on the motion offered by the gentlewoman from Michigan (Mrs. MILLER) that the House suspend the rules and pass the bill, H.R. 3878, 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.

RECESS

The SPEAKER pro tempore. Pursuant to clause 12(a) of rule I, the Chair