security risks. The U.S. Government has particularly highlighted concerns about Kaspersky Lab. In September 2017, DHS issued a directive requiring Federal agencies to remove all Kaspersky products from their networks, given ties between certain Kaspersky officials and Russian intelligence.

The risks to the supply chain are all too real and must be mitigated. That is why I am proud to cosponsor H.R. 6430, a measure that acts upon the information provided to us by our intelligence community to help DHS better counter these mounting threats.

H.R. 6430 provides DHS with needed authority to exclude vendors who are bad actors from the information technology and communications supply chain. If enacted, H.R. 6430 will allow the Department to be proactive and effective in addressing these complex threats in the future.

Importantly, the bill includes robust oversight provisions to ensure that Congress receives notification and justification of any exercise of authority under this act. Notably, this measure is based on a similar authority provided to the Department of Defense in 2011 and incorporates language provided by the Office of Management and Budget.

H.R. 6430 provides the Secretary of Homeland Security with a much-needed tool to eliminate national security threats to our supply chain. Enactment of H.R. 6430 will help DHS secure information technology and telecommunications equipment and services that are so essential to keeping our Nation secure.

Mr. Speaker, I would like to compliment the gentleman from New York, who has significant experience in this area, for offering this legislation.

Mr. Speaker, I encourage my colleagues to support H.R. 6430, and I yield back the balance of my time.

Mr. KING of New York. Mr. Speaker, I yield myself the balance of my time.

Let me again thank the gentleman from Mississippi and the ranking member for his service on this bill and his service to the committee over the years.

Mr. Speaker, this legislation provides DHS vital authority to protect the Department from vendors who pose a risk. The bill includes important accountability measures to ensure that decisions are risk based, allows the vendor to provide feedback, and requires annual reviews any time the authority is used.

This is commonsense legislation that will provide important national security protections for the Department similar to what already exists for the Department of Defense and the intelligence community.

Mr. Speaker, I once again urge my colleagues to support H.R. 6430, the Securing the Homeland Security Supply Chain Act of 2018, and I yield back the balance of my time.

The SPEAKER pro tempore (Mr. HILL). The question is on the motion offered by the gentleman from New York (Mr. KING) that the House suspend the rules and pass the bill, H.R. 6430.

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

A motion to reconsider was laid on the table.

ADVANCING CYBERSECURITY DIAGNOSTICS AND MITIGATION ACT

Mr. RATCLIFFE. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 6443) to amend the Homeland Security Act of 2002 to authorize the Secretary of Homeland Security to establish a continuous diagnostics and mitigation program at the Department of Homeland Security, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 6443

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 ''Advancing Cybersecurity Diagnostics and Mitigation Act''.

SEC. 2. ESTABLISHMENT OF CONTINUOUS DIAGNOSTICS AND MITIGATION PROGRAM IN DEPARTMENT OF HOMELAND SECURITY.

(a) IN GENERAL.—Section 230 of the Homeland Security Act of 2002 (6 U.S.C. 151) is amended by adding at the end the following new subsection:

''(g) CONTINUOUS DIAGNOSTICS AND MITIGATION.—

''(1) PROGRAM.—

''(A) IN GENERAL.—The Secretary shall deploy, operate, and maintain a continuous diagnostics and mitigation program. Under such program, the Secretary shall—

''(i) develop and provide the capability to collect, analyze, and visualize information relating to security data and cybersecurity risks;

''(ii) make program capabilities available for use, with or without reimbursement;

''(iii) employ shared services, collective purchasing, blanket purchase agreements, and any other economic or procurement models the Secretary determines appropriate to maximize the costs savings associated with implementing an information system;

''(iv) assist entities in setting information security priorities and managing cybersecurity risks; and

''(v) develop policies and procedures for reporting systemic cybersecurity risks and potential incidents based upon data collected under such program.

''(B) REGULAR IMPROVEMENT.—The Secretary shall regularly deploy new technologies and modify existing technologies to the continuous diagnostics and mitigation program required under subparagraph (A), as appropriate, to improve the program.

''(2) ACTIVITIES.—In carrying out the continuous diagnostics and mitigation program under paragraph (1), the Secretary shall ensure, to the extent practicable, that—

''(A) timely, actionable, and relevant cybersecurity risk information, assessments, and analysis are provided in real time;

''(B) share the analysis and products developed under such program;

''(C) all information, assessments, analyses, and raw data under such program is made available to the national cybersecurity and communications integration center of the Department; and

''(D) provide regular reports on cybersecurity risks.''.

(b) CONTINUOUS DIAGNOSTICS AND MITIGATION STRATEGY.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall develop a comprehensive continuous diagnostics and mitigation strategy to carry out the continuous diagnostics and mitigation program required under subsection (g) of section 230 of such Act, as added by subsection (a).

(2) SCOPE.—The strategy required under paragraph (1) shall include the following:

(A) A description of the continuous diagnostics and mitigation program, including efforts by the Secretary of Homeland Security to assist with the deployment of program tools, capabilities, and services, from the inception of the program referred to in paragraph (1) to the date of the enactment of this Act.

(B) A description of the coordination required to deploy, install, and maintain the tools, capabilities, and services that the Secretary of Homeland Security determines to be necessary to satisfy the requirements of such program.

(C) A description of any obstacles facing the deployment, installation, and maintenance of tools, capabilities, and services under such program.

(D) Recommendations and guidelines to help maintain and continuously upgrade tools, capabilities, and services provided under such program.

(E) Recommendations for using the data collected by such program for creating a common framework for data analytics, visualization of enterprise-wide risks, and real-time reporting.

(F) Recommendations for future efforts and activities, including for the rollout of new tools, capabilities and services, proposed timelines for delivery, and whether to continue the use of phased rollout plans, related to securing networks, devices, data, and information technology assets through the use of such program.

(3) FORM.—The strategy required under subparagraph (A) shall be submitted in an unclassified form, but may contain a classified annex.

(c) REPORT.—Not later than 90 days after the development of the strategy required under subsection (b), the Secretary of Homeland Security shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representative a report on cybersecurity risk posture based on the data collected through the continuous diagnostics and mitigation program under subsection (g) of section 230 of the Homeland Security Act of 2002, as added by subsection (a).

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

The Chair recognizes the gentleman from Texas.

GENERAL LEAVE

Mr. RATCLIFFE. Mr. Speaker, I ask unanimous consent that all Members have 5 legislative days in which to revise and extend their remarks and include any 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. RATCLIFFE. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, earlier this year, the Office of Management and Budget and the Department of Homeland Security

released a report on the cybersecurity risks faced by Federal agencies. Among the findings of that report was that almost 75 percent of our Federal agencies are vulnerable to cyber threats, in large part due to their inability to understand cybersecurity risks and, therefore, to properly prioritize resources.

Mr. Speaker, it is statistics like this that should make the state of our Nation's cyber readiness and resilience deeply troubling to all of us. And it is one of the main reasons that DHS' Continuous Diagnostics and Mitigation, or CDM, program has been one of my top priorities during my time as chairman of the Cybersecurity and Infrastructure Protection Subcommittee. That is because CDM has the potential to provide solutions to this problem by dramatically increasing visibility across Federal networks, thereby dramatically improving the ability of DHS, OMB, and agency security officers to better understand the technology assets being utilized across their agencies.

Mr. Speaker, at the end of the day, looking across all networks and systems the Federal Government owns and operates, it comes down to fingers on government keyboards, whether they be laptops, desktops, tablets, servers, or in data centers.

□ 1715

We need to know what we have before we can try to defend it.

That is why the CDM program is so crucial to the cybersecurity posture of our Federal Government. Through its phased rollout, CDM requires DHS to provide agencies with the capabilities to collect the cybersecurity risk information necessary to make better decisions. It not only allows the ability to combat our enemies in cyberspace, but also to help Federal CIOs manage information technology.

The security data that CDM capabilities and tools collect will help Federal CIOs and DHS make smarter choices about where taxpayer dollars are going and to understand some of the most basic questions a cybersecurity expert faces, including what devices are on the network.

Mr. Speaker, H.R. 6443 is necessary to codify the CDM program at DHS and ensure that these authorities will exist to allow the continued progress of this essential cybersecurity program.

Making sure that Federal agencies have access to the tools and capabilities they need to defend their networks and getting DHS the data to understand cybersecurity risks and vulnerabilities, and to coordinate our Federal network defenses, are paramount concerns in this technological age.

My goal, and the goal of the bipartisan group of cosponsors supporting H.R. 6443, is to help boost the long-term success of the CDM program.

This bill also ensures that this program keeps pace with the cutting-edge capabilities being developed in the private sector, thereby avoiding the type of vendor lock that has previously been a problem. In that way, this bill ensures that we will be modernizing and updating our systems before they become legacy technologies unsupported by vendors and at even greater risk of being exploited by our digital adversaries.

It is DHS' CDM program that will help Federal agencies and the whole of the Federal Government to understand the threats they face and the risks that these vulnerabilities pose in real time. Authorizing the CDM program will further DHS' role in the cybersecurity mission throughout our government and will continue to strengthen and elevate this important program.

Mr. Speaker, I urge my colleagues to support this bill, and I reserve the balance of my time.

Mr. THOMPSON of Mississippi. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I rise in support of H.R. 6443, the Advanced Cybersecurity Continuous Diagnostics and Mitigation Act.

Mr. Speaker, H.R. 6443 would codify the existing Continuous Diagnostics and Mitigation, or CDM, program within the Department of Homeland Security's National Protection and Programs Directorate, NPPD.

CDM is an important part of our national approach to securing Federal networks. Through CDM, DHS works with Federal agencies to identify, purchase, and integrate cybersecurity tools and services to help defend their networks against cyber attacks.

By taking advantage of bulk pricing, CDM allows agencies to purchase security services at a discounted rate and, in turn, devote more of their limited resources to carrying out their missions. Another benefit of the program is that it enables DHS to track threats to agency networks, giving the Department a more holistic view of the threat landscape.

Still, given the enormous challenges associated with protecting such a massive and diverse set of networks, it is not surprising that DHS has, at times, struggled.

For instance, in rolling out CDM, DHS officials mapped four phases of implementation where, in the first phase, agencies would identify all the assets and devices on their networks.

At the time, DHS projected that the last phase, which is focused on protecting the data that agencies store, would begin being tackled in 2017. Unfortunately, the CDM deployment schedule has been plagued with across-the-board delays, starting with the implementation of phase 1, which took years. As a result of these delays, the data housed on agency networks—what the bad guys are really after—remains less secure than might otherwise have been.

H.R. 6443 would address CDM's challenges in a few ways, for example, by asking DHS to reconsider its phased approach to implementation and examine opportunities to streamline adoption of CDM technologies.

This bill would also require DHS to develop a comprehensive strategy that addresses deployment challenges, areas where greater coordination is needed, and recommendations for continuous improvement.

Finally, H.R. 6443 adds specificity to DHS' responsibilities under CDM and includes robust reporting requirements to inform congressional oversight.

Every year, Federal networks get hit by tens of thousands of attempted intrusions, many of them sophisticated, state-sponsored attacks. We have seen time and again the cost and damage that can flow from a high-profile Federal breach. As such, we need CDM to work.

Mr. Speaker, I yield 2 minutes to the gentleman from Rhode Island (Mr. LANGEVIN).

Mr. LANGEVIN. Mr. Speaker, I thank the gentleman for yielding, and I want to recognize and thank the gentleman from Texas for his leadership on this issue as well as for his leadership as chairman of the Subcommittee on Cybersecurity and Infrastructure Protection.

As the cofounder and co-chair of the Congressional Cybersecurity Caucus, which I have co-led for a decade with my good friend Chairman MCCAUL, I firmly believe that cybersecurity is the national and economic security issue of the 21st century. I believe it is, therefore, incumbent upon us as Members of Congress to enable the government to take the steps needed to protect our systems and to provide some course correction when necessary.

This bill does both, authorizing the Continuous Diagnostics and Mitigation, or CDM, program and requiring a strategy from the Department of Homeland Security to guide its future growth. CDM represents a core component of the Department's efforts to better secure the dot-gov domain. In particular, by giving agencies a better view into their networks, systems, and data, it helps provide an understanding of cybersecurity status in real time.

It also feeds back data to DHS, so that cybersecurity specialists at the National Protection and Programs Directorate can better assist agencies in closing vulnerabilities and responding to incidents.

Conceptually, CDM makes a lot of sense, but it has not been without challenges in implementation. Originally designed with a phased model that focused on incorporating new sets of tools at each milestone, it has fallen behind schedule, and many agencies have expressed skepticism about the program's utility.

I believe in CDM, and I believe that the congressional direction provided by Mr. RATCLIFFE's bill will help dispel some of these doubts. I also believe that the strategy can further help refocus the program on the present and future needs of Federal networks. So I am pleased that, during the committee

consideration, my amendment requiring a re-examination of the phasing plan was adopted.

While I appreciate the thought underlying the original phasing approach, I believe that we make more progress if the planned phase 3 and phase 4 are constructed in parallel rather than serially.

This is a good bill, and I urge my colleagues to support its passage. However, I must take this opportunity to mention this bill's major omission. It does not address the incentive structure at other agencies to actually adopt CDM offerings. During hearings and roundtables on the program, we often heard from government stakeholders that internal dynamics at DHS' sister agencies were actually the biggest obstacle to the program's success.

The SPEAKER pro tempore (Mr. HIGGINS of Louisiana). The time of the gentleman has expired.

Mr. THOMPSON of Mississippi. Mr. Speaker, I yield an additional 1 minute to the gentleman from Rhode Island.

Mr. LANGEVIN. Mr. Speaker, I thank the gentleman for yielding.

This is, to be sure, outside the purview of the Committee on Homeland Security, and I believe the bill before us will materially improve the program.

One other thing, I urge my colleagues to consider the wisdom of having so many committees involved with cybersecurity jurisdiction, often to the detriment of making real progress. Right now, there are some 30 committees and subcommittees that have jurisdiction over cyber, and it is very difficult to get things done. So I also urge my colleagues to look at the Executive Cyberspace Coordination Act, which would put a Senate-confirmed director of cybersecurity at the White House to help better coordinate interagency processes. Dealing with these jurisdictional problems would substantially improve our cybersecurity posture and would allow CDM to fully live up to its potential.

With that, I would like to again thank Ranking Member THOMPSON and Chairmen MCCAUL and RATCLIFFE for continuing their focus on cybersecurity. I strongly urge support for H.R. 6443. I commend Chairman RATCLIFFE for introducing the bill, and I certainly hope all Members will support it and DHS' ongoing cybersecurity efforts.

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

Mr. THOMPSON of Mississippi. Mr. Speaker, I have no further speakers on this bill, and I yield myself the balance of my time.

Mr. Speaker, H.R. 6443 seeks to improve DHS' capacity to carry out one of its more important homeland security missions: the protection of Federal agency networks.

Over the past decade, we have seen the number of cyber attacks against Federal agencies rise by more than 1,000 percent. Last year alone, the Office of Management and Budget reported that Federal agencies experienced more than 35,000 cybersecurity incidents. A challenge of this magnitude cannot be undertaken by each agency on its own. They need help.

That is where the CDM program comes in. By authorizing CDM in law, DHS and its agency partners can confidently move forward to bolster Federal network security. By requiring the Department to revisit its implementation plans and work to finally resolve its longstanding CDM challenges, H.R. 6443 puts the program on an even more secure footing.

Mr. Speaker, I urge my colleagues to support this bipartisan legislation, and I yield back the balance of my time.

Mr. RATCLIFFE. Mr. Speaker, I would like to thank my friends across the aisle, Ranking Member THOMPSON and Congressman LANGEVIN, for their support of this bill. I would like to thank the ranking member of the Cybersecurity and Infrastructure Protection Subcommittee, Mr. RICHMOND, for cosponsoring this bill.

Mr. Speaker, this is, very simply, commonsense legislation that will strengthen our Nation's cybersecurity posture and thereby strengthen our Nation's national security.

Mr. Speaker, once again, I urge my colleagues to support H.R. 6443, and I yield back the balance of my time.

Ms. JACKSON LEE. Mr. Speaker, I rise today in support of H.R. 6443, the ''Advancing Cybersecurity Diagnostics and Mitigation Act'' which codifies the Continuous Diagnostics and Mitigation (CDM) Program administered by the Department of Homeland Security.

At a time when the computer networks of our government are under constant attack, and have suffered serious breaches in recent years, we must take action to ensure that the information of our citizens and the ability of federal agencies to carry out their duties are resilient.

As a long-time advocate of a government that works efficiently for the people, it is clear that current information security practices of federal agencies are neither sufficient nor consistent.

Without an honest effort to even get to obtain a view of the security state of federal networks, users, and devices, we will continue to be increasingly vulnerable.

To that end, H.R. 6443 recognizes the importance of a dynamic approach that will help secure federal networks and data, as well as provide improved information on vulnerabilities and security practices across the various agencies.

In particular, this measure codifies the Continuous Diagnostics and Mitigation (CDM) Program to which:

1. Deploys DHS sensors which perform ongoing scans for vulnerabilities and known flaws; and

2. Feed the collected data to an enterprise dashboard to provide increased insight into the information security posture of federal agencies.

Without codifying this concrete measure to fortify federal networks and devices, federal agencies will remain vulnerable.

While codifying the DHS CDM Program will harden the security posture of the federal government, we are still suffering from a shortage of workers with the requisite skills in this area.

To address this, I have introduced the Cyber Security Education and Federal Workforce Enhancement Act (H.R. 1981), which would address our cyber workforce shortage by establishing an Office of Cybersecurity Education and Awareness within DHS which will focus on:

1. Recruiting information assurance, cybersecurity, and computer security professionals;

2. Providing grants, training programs, and other support for kindergarten through grade 12, secondary, and post-secondary computer security education programs;

3. Supporting guest lecturer programs in which professional computer security experts lecture computer science students at institutions of higher education;

4. Identifying youth training programs for students to work in part-time or summer positions at federal agencies; and

5. Developing programs to support underrepresented minorities in computer security fields with programs at minority-serving institutions, including Historically Black Colleges and Universities, Hispanic-serving institutions, Native American colleges, Asian-American institutions, and rural colleges and universities.

Mr. Speaker, government agencies and the private sector alike continue to struggle to identify the motivations and methods behind a cyber-attack and, in many cases, lack timely information on tactics and techniques hackers are using.

Despite this, the White House has eliminated the position of Cybersecurity Coordinator from the National Security Council.

This occurred even after Federal Risk Determination Reports found that communication of threat information within agencies is also inconsistent, with only 59 percent of agencies reporting a capability to share threat information to all employees within an enterprise so they have the knowledge necessary to block attacks.

Federal agencies are not taking advantage of all available information such as threat intelligence, incident data, and network traffic flow to improve situational awareness regarding systems at risk and to prioritize investments.

For this reason, earlier this Congress, I introduced H.R. 3202, the ''Cyber Vulnerability Disclosure Reporting Act'', which was passed by the full House and is now in the Senate.

H.R. 3202 requires the Secretary of Homeland Security to submit a report on the policies and procedures developed for coordinating cyber vulnerability disclosures.

The report will include an annex with information on instances in which cyber security vulnerability disclosure policies and procedures were used to disclose details on identified weaknesses in computing systems or digital devices at risk.

The report will provide information on the degree to which the information provided by DHS was used by industry and other stakeholders.

I would also like to recognize the University of Houston, which has been recognized by the Department of Homeland Security and the National Security Agency as a Center of Academic Excellence for the programs in cybersecurity and cyber defense.

In closing, Mr. Speaker, I urge all members to join me in voting to pass H.R. 6433, the ''Advancing Cybersecurity Diagnostics and Mitigation Act''.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Texas (Mr. RATCLIFFE) that the House suspend the rules and pass the bill, H.R. 6443, 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.

MARITIME BORDER SECURITY REVIEW ACT

Mr. KATKO. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 5869) to require the Secretary of Homeland Security to conduct a maritime border threat analysis, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 5869

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 ''Maritime Border Security Review Act''.

SEC. 2. DEFINITIONS.

In this Act:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Committee on Homeland Security of the House of Representatives;

(B) the Committee on Transportation and Infrastructure of the House of Representatives;

(C) the Committee on Homeland Security and Government Affairs of the Senate; and

(D) the Committee on Commerce, Science, and Transportation of the Senate.

(2) MARITIME BORDER.—The term ''maritime border'' means—

(A) the transit zone; and

(B) the borders and territorial waters of Puerto Rico and the United States Virgin Islands.

(3) TRANSIT ZONE.—The term ''transit zone'' has the meaning given such term in section 1092(a)(8) of the National Defense Authorization Act for Fiscal Year 2017 (6 U.S.C. 223(a)(8)).

SEC. 3. MARITIME BORDER THREAT ANALYSIS.

(a) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Secretary of Homeland Security shall submit to the appropriate congressional committees a maritime border threat analysis that includes an identification and description of the following:

(1) Current and potential terrorism and criminal threats posed by individuals and groups seeking to—

(A) enter the United States through the maritime border; or

(B) exploit border vulnerabilities on the maritime border.

(2) Improvements needed at United States sea ports to—

(A) prevent terrorists and instruments of terror from entering the United States; and

(B) reduce criminal activity, as measured by the total flow of illegal goods and illicit drugs, related to the maritime border.

(3) Improvements needed with respect to the maritime border to—

(A) prevent terrorists and instruments of terror from entering the United States; and

(B) reduce criminal activity related to the maritime border.

(4) Vulnerabilities in law, policy, cooperation between State, territorial, and local law enforcement, or international agreements that hinder effective and efficient border security, counterterrorism, anti-human trafficking efforts, and the flow of legitimate trade with respect to the maritime border.

(5) Metrics and performance parameters used by the Department of Homeland Security to evaluate maritime security effectiveness, as appropriate.

(b) ANALYSIS REQUIREMENTS.—In preparing the threat analysis required under subsection (a), the Secretary of Homeland Security shall consider and examine the following:

(1) Technology needs and challenges.

(2) Personnel needs and challenges.

(3) The role of State, territorial, and local law enforcement in general border security activities.

(4) The need for cooperation among Federal, State, territorial, local, and appropriate international law enforcement entities relating to border security.

(5) The geographic challenges of the maritime border.

(6) The impact and consequences of Hurricanes Harvey, Irma, Maria, and Nate on general border security activities with respect to the maritime border.

(c) CLASSIFIED THREAT ANALYSIS.—To the extent possible, the Secretary of Homeland Security shall submit the threat analysis required under subsection (a) in unclassified form. The Secretary may submit a portion of the threat analysis in classified form if the Secretary determines that such form is appropriate for such portion.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from New York (Mr. KATKO) and the gentleman from Mississippi (Mr. THOMPSON) each will control 20 minutes.

The Chair recognizes the gentleman from New York.

□ 1730

GENERAL LEAVE

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

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

There was no objection.

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

Mr. Speaker, I rise today in support of H.R. 5869, the Maritime Border Security Review Act, sponsored by the gentlewoman from Puerto Rico (Miss GONZÁLEZ-COLÓN), my friend and colleague.

With increasing focus on the threats at the southwest border, we must be mindful that our adversaries can and will adapt as they seek to gain entry into our homeland. As illicit pathways are squeezed on the southwest border, the Nation's maritime border is a likely alternative route for our adversaries to utilize.

The brave men and women of the United States Coast Guard are responsible for patrolling our Nation's maritime border, conducting counter-drug and migrant interdiction operations, as well as search and rescue missions to ensure the safety and legitimacy of travel and trade in the maritime environment.

The Coast Guard also interdicts and often rescues migrants who are attempting to reach the United States not only from the Caribbean and Latin American region but, as recent cases have indicated, from countries outside the Western Hemisphere, including China, India, Pakistan, and Jordan.

Cocaine is one of the most highly trafficked drugs throughout the maritime border, especially in the transit zone, a 7-million-square-mile area that includes the sea corridors of the western Atlantic Ocean, the Caribbean Sea, the Gulf of Mexico, and the eastern Pacific Ocean. I know that firsthand from the time I spent for 2 years in the mid-nineties prosecuting international drug organizations in San Juan, Puerto Rico.

The Coast Guard interdicts thousands of pounds of cocaine every year; though, according to the DHS Office of Inspector General, only about 8.2 percent of the total cocaine flow through the transit zone was interdicted in fiscal year 2017.

Unfortunately, we currently do not have the resources to turn back or interdict all the threats in the maritime environment. To make matters worse, the devastating effects of the 2017 hurricane season diminished local law enforcement operational capabilities and resources available to combat maritime-based threats in the U.S. territories, putting further strain on our Federal law enforcement agents and officers.

Many of the hurricane-affected areas are still not back to pre-hurricane conditions. Under this environment, by the time a threat reaches our coastal waters, it is too easy to slip into the country and often too late, from a law enforcement standpoint, to intercept that threat.

H.R. 5869 requires the Secretary of Homeland Security to conduct a threat analysis of the greater U.S. maritime border, to include the territorial waters of Puerto Rico and the United States Virgin Islands as well as the transit zone. The bill requires the examination of terrorist and criminal threats posed by individuals and groups seeking to enter the U.S. through the maritime border.

The bill also requires the Secretary to identify vulnerabilities in law, policy, and cooperation between State, territorial, and local law enforcement, and it asks the Secretary to review the impact of the geographic challenges of the maritime border and of Hurricanes Harvey, Irma, Maria, and Nate on general border security activities related to the maritime border.

The Maritime Border Security Review Act is a necessary and timely piece of legislation, and I want to thank the gentlewoman from Puerto Rico for introducing it.

Mr. Speaker, I urge all Members to join me in supporting H.R. 5869, and I reserve the balance of my time.