and Europe to observe international aviation security efforts firsthand, my colleagues and I returned home determined to bolster the Department of Homeland Security's efforts to build capacity among foreign partners.

When it comes to aviation security, we are only as secure as our weakest link. Unfortunately, through our oversight on the Homeland Security Committee's Subcommittee on Transportation and Protective Security, we have grown increasingly concerned that existing standards are simply not sufficient to keep up with the changing threats to aviation.

This legislation will ensure that DHS and TSA are aggressively committed to eliminating security vulnerabilities and inconsistencies at overseas airports with direct flights to the United States.

I wish to thank Congressman ESTES for participating in the important delegation we undertook which led to this legislation, as well as his commitment and leadership to security America's transportation systems on my Subcommittee.

I urge my colleagues to support the bill.

Mr. MCCAUL. Mr. Speaker, I include in the RECORD the cost estimate from the Congressional Budget Office regarding H.R. 4559. The cost estimate was not available at the time of the filing of the Committee report.

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, January 9, 2018.

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

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 4559, the Global Aviation System Security Reform Act of 2017.

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

Sincerely,

KEITH HALL.

Enclosure.

H.R. 4559—GLOBAL AVIATION SYSTEM SECURITY REFORM ACT OF 2017

As ordered reported by the House Committee on Homeland Security on December 13, 2017

H.R. 4559 would direct the Transportation Security Administration (TSA), in consultation with other federal agencies, to review security-related standards across the global aviation system. The bill would require TSA to identify best practices for:

Enhancing security by collaborating with foreign partners involved in aviation security,

Identifying foreign entities that have not yet implemented international standards,

Improving processes for issuing security-related directives to air carriers, and

Assessing cyber-related threats to screening equipment.

Using information from TSA, CBO estimates that meeting the bill's requirements would increase the agency's costs by less than $500,000 in 2018; such spending would be subject to appropriation. Enacting H.R. 4559 would not affect direct spending or revenues; therefore, pay-as-you-go procedures do not apply.

CBO estimates that enacting H.R. 4559 would not increase net direct spending or on-budget deficits in any of the four consecutive 10-year periods beginning in 2028.

H.R. 4559 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act.

The CBO staff contact for this estimate is Megan Carroll. The estimate was approved by H. Samuel Papenfuss, Deputy Assistant Director for Budget Analysis.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Kansas (Mr. ESTES) that the House suspend the rules and pass the bill, H.R. 4559, 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.

CYBER VULNERABILITY DISCLOSURE REPORTING ACT

Mr. ESTES of Kansas. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 3202) to require the Secretary of Homeland Security to submit a report on cyber vulnerability disclosures, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 3202

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 ''Cyber Vulnerability Disclosure Reporting Act''.

SEC. 2. REPORT ON CYBER VULNERABILITIES.

(a) REPORT.—Not later than 240 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report that contains a description of the policies and procedures developed for coordinating cyber vulnerability disclosures, in accordance with section 227(m) of the Homeland Security Act of 2002 (6 U.S.C. 148(m)). To the extent possible, such report shall include an annex with information on instances in which such policies and procedures were used to disclose cyber vulnerabilities in the year prior to the date such report is required and, where available, information on the degree to which such information was acted upon by industry and other stakeholders. Such report may also contain a description of how the Secretary is working with other Federal entities and critical infrastructure owners and operators to prevent, detect, and mitigate cyber vulnerabilities.

(b) FORM.—The report required under subsection (b) shall be submitted in unclassified form but may contain a classified annex.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Kansas (Mr. ESTES) and the gentlewoman from Texas (Ms. JACKSON LEE) each will control 20 minutes.

The Chair recognizes the gentleman from Kansas.

GENERAL LEAVE

Mr. ESTES of Kansas. 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 material on the bill under consideration.

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

There was no objection.

Mr. ESTES of Kansas. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I rise in support of H.R. 3202, the Cyber Vulnerability Disclosure Reporting Act.

It is hard to find an electronic device today that doesn't connect to the internet. From smartphones to alarm clocks, everything is part of the Internet of Things. Americans can do everything, from personal banking to unlocking the front door, with the palm of their hands.

As the world has become increasingly interconnected, vulnerabilities in computer code underlying these devices and the applications they run can often expose the average American to exploitation by hackers, criminals, and even bad actors from nation states.

As more and more critical and personal information is being stored on the internet and more industrial systems are being operated autonomously, it is vital that we are able to plug the holes in vulnerable technology.

It seems like every day we read about another data breach that could have been prevented if only the company had known about a vulnerability in the product or network, occurrences such as the WannCry ransomware that affected hundreds of thousands of computers in more than 150 countries, and the recently reported meltdown that could affect millions of personal computers throughout the world. That is why, in this world of ever-increasing intrusions, we must do our best to make sure our computer systems are as invulnerable to attack as possible.

The Department of Homeland Security was given the authority by the Cybersecurity Act of 2015 to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats.

The Homeland Security Act of 2002 allows the Secretary to coordinate with industry to develop departmental policies and procedures for coordinating the disclosure of cyber vulnerabilities as described in the Vulnerabilities Equities Policy and Process published by the White House on November 15, 2016. This disclosure is important, as it highlights vulnerabilities and allows the public and private sector to work to prevent and mitigate cyber threats.

H.R. 3202, the Cyber Vulnerability Disclosure Reporting Act, is an important tool, in that it requires the Secretary of Homeland Security to submit a report to Congress on their policies and procedures for disclosing vulnerabilities.

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

Ms. JACKSON LEE. Mr. Speaker, I yield myself such time as I may consume, and I thank the manager for his kind words.

Mr. Speaker, I rise in support of H.R. 3202, the Cyber Vulnerability Disclosure Reporting Act. I very much want

to thank the committee for bringing the Jackson Lee bill to the floor and the work that we did on it in committee.

I wish to speak specifically to the work that is done on the Homeland Security Committee as I discuss this legislation. I think it is very important to take note of the fact that the ranking member works very hard to generate very positive legislation and that we have been able to see a large number of bills, some that I have been able to sponsor, come to the floor of the House.

Mr. Speaker, therefore, I thank the chairman, Mr. MCCAUL, and the ranking member for making the Homeland Security Committee so productive in generating important legislation to ensure the security of this Nation. I thank them for their leadership in putting the security of our Nation's cyber assets first, whether they are computing resources used in voting technology, or industrial control systems that support the delivery of electricity, oil and gas, or management of transportation systems that are vital to our Nation's economic health.

Mr. Speaker, I was chairman of the Transportation Security and Infrastructure Protection Subcommittee some few sessions ago. This was when infrastructure was included in the transportation and security domain. I can tell you that, even then, we began to acknowledge the crucialness of protecting the cyber system and how far-reaching cyber systems can go, as far away as water systems, to bridges, to dams, and in between, and to note that a lot of our cyber system, 80 percent of it was in the private sector, probably more at this point.

H.R. 3202, the Cyber Vulnerability Disclosure Reporting Act, which I introduced, 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 cybersecurity 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.

The report may also contain a description of how the Secretary of Homeland Security is working with other Federal entities and critical infrastructure owners and operators to prevent, detect, and mitigate cyber vulnerabilities.

It is important to restate that our cyber system is largely in the private sector. It does not alleviate or eliminate the role that the Federal Government should play. This legislation squarely places with the Federal Government the responsibilities of dealing with those critical infrastructure owners and operators to prevent, detect, and mitigate cyber vulnerabilities.

The reason that I have worked to bring this bill before the full House for consideration is a problem often referred to as a zero-day event. A zero-day event describes a situation that network security professionals may find themselves in when a previously unknown error or flaw in computing code is exploited by a cybercriminal or terrorist.

The term ''zero-day event'' simply means that there is zero time to prepare a defense against a cyber attack. That is not the place that we would like to find ourselves.

When a defect in software is discovered, their network engineers and software companies can work to develop a patch to fix the problem before it can be exploited by those who may seek to do us harm.

We have evidence that the cyber world is a good world, but it can be a dangerous world and impact the life and quality and democracy and freedom of Americans. We want to be prepared and never have to face, in this most powerful country in the world, something called a zero-day event.

H.R. 3202 seeks a report on the ongoing Department of Homeland Security's policies and procedures for coordinating cyber vulnerability disclosures, such as zero-day events, with private sector partners. Because vulnerabilities can be used by adversaries, it is important that this sensitive information be managed securely so details are not routinely made available, neither to the public nor to Congress.

H.R. 3202 provides the Congress with the opportunity to understand the process and procedures used by the Department of Homeland Security and the benefit these disclosures may have for private sector entities participating in programs in support of cybersecurity.

Mr. Speaker, I thank Lillie Coney of my district and Jean de Pruneda, a fellow on the Committee on Homeland Security, for their work on this important legislation.

I urge Members of the House to vote in favor of H.R. 3202, the Cyber Vulnerability Disclosure Reporting Act.

Mr. Speaker, I want to emphasize again a point that I made earlier. Because vulnerabilities can be used by adversaries, it is important that this sensitive information be managed securely so details are not routinely made available, neither to the public nor to Congress.

It is important to take note of the fact that the work we have to do is ongoing and continuing.

H.R. 3202 will give this body important information on our government-wide efforts to secure civilian agency networks and the collaborative ongoing work to provide information to private sector partners on computing vulnerabilities. There is no security in keeping zero-day events secure from disclosure and not working on solutions.

Cybersecurity is found in finding the zero-day events, creating solutions to defend against them, and sharing the solutions broadly so that they can be deployed. Once solutions are in place, the zero-day event should be disclosed to the public so that scholars and researchers can learn from the experience.

In essence, what we are saying is that we want to make sure that we are in the driver's seat, that we know the vulnerabilities, that we can confront the zero-day events, and that we can do that, meaning the Federal Government, in working with the private sector to ensure that we do protect this Nation.

Before I close, since we are dealing with Homeland Security Committee issues, I think it is important to take note of the fact of the crucialness and the importance of having a DACA fix and working together, as we have been doing, to ensure that the thousands and thousands of young people located across the Nation, who came here through no fault of their own, have a serious pathway of protection, in particular, the 140,000 that are in the State of Texas.

If we can stand here as bipartisan Members, I know that we can continue to work on that crucial and important issue, which I stand with those young people to ensure to get that done.

Mr. Speaker, I include in the RECORD an article by Morgan Chalfant, ''Lawmakers approve 'cyber vulnerability' bill,'' written in The Hill.

[From the Hill, July 26, 2017]

LAWMAKERS APPROVE 'CYBER VULNERABILITY' BILL

(By Morgan Chalfant)

A House panel advanced legislation on Wednesday requiring the Department of Homeland Security (DHS) to give lawmakers more information on how it discloses cyber vulnerabilities to the private sector.

The legislation was sponsored by Rep. Sheila Jackson Lee (D-Texas) and received broad support from members of the House Homeland Security Committee, including Chairman Michael McCaul (R-Texas).

The bill would require Homeland Security Secretary John Kelly to send a report to relevant congressional committees describing policies and procedures used by the DHS to coordinate the disclosure of what are called ''zero days''—cyber vulnerabilities that are unknown to a product's manufacturer and for which no patch exists.

The federal government decides whether to disclose zero days to the private sector through the vulnerabilities equities process (VEP), which was first acknowledged by the Obama administration in 2014 but is still shrouded in secrecy. While the government is said to err on the side of disclosure, the VEP has proven controversial because so little is known about it.

The process has attracted increased scrutiny in the wake of the outbreak of the ''Wanna Cry'' ransomware, which is believed to be based on a hacking tool developed by the National Security Agency.

Lawmakers in both chambers have sought to boost transparency of the VEP.

On Wednesday, Jackson Lee touted the legislation as providing an opportunity for Congress to better understand the process by which the DHS shares threat information

with private companies and how that information benefits the private sector.

''Because vulnerabilities can be used by adversaries, it is important that the sensitive information is managed securely and the details are guarded against premature disclosure,'' Jackson Lee said during a committee markup.

''There's no security in keeping zero day events secure and not working on solutions,'' she said. ''The protection is in finding the zero day events, creating solutions, sharing the solutions broadly, then disclosing the vulnerabilities to the public.''

The report mandated by the legislation would include an annex of information on specific instances when the DHS disclosed vulnerabilities to private sector companies in the previous year and information on how industry acted on the information. It could also contain information about how the DHS is working with other federal agencies and departments, as well as owners of critical infrastructure, to mitigate the threat of these vulnerabilities.

Kelly would be required to submit the report, which would be unclassified but could have a classified annex, within 240 days of the enactment of the legislation.

The committee approved the legislation in a voice vote with no amendments, sending it to the full House for a vote.

Ms. JACKSON LEE. Mr. Speaker, I encourage my colleagues to support H.R. 3202, and I thank my manager as well.

Mr. Speaker, I rise to speak in support of H.R. 3202, the Cyber Vulnerabilities Disclosure Reporting Act.

I thank Chairman MCCAUL and Ranking Member THOMPSON for their leadership on putting the security of our nation's cyber assets first whether they are computing resources used in voting technology or industrial control systems that support the delivery of electricity, oil and gas, or management of transportation systems all are vital to our nation.

H.R. 3202, the Cyber Vulnerability Disclosure Reporting Act, which I introduced, 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 that 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.

The report may also contain a description of how the Secretary of Homeland Security is working with other Federal entities and critical infrastructure owners and operators to prevent, detect, and mitigate cyber vulnerabilities.

The reason that I worked to bring this bill before the Full House for consideration is the problem often referred to as a ''Zero Day Event.''

Zero Day Events are vulnerabilities in software or firmware that have gone undetected or undisclosed, but if exploited by terrorists could cause great harm to computer networks, data, or complex computing dependent systems.

Our nation's electric power grid; industrial control systems that operate bridges, dams, water treatment facilities or food processing plants are all vulnerable to the potential harm that could be caused if a weakness in software or firmware goes undetected.

Critical infrastructure must be secured against terrorist attacks that may use Zero Day Event vulnerabilities to attack critical infrastructure or civilian government agency computing assets.

Zero Day Events discovered in commercial software applications such as the ''Heartbleed'' and OpenSSL cryptographic software library vulnerability.

Proactive and coordinated efforts are necessary to strengthen and maintain secure critical infrastructure including assets that are vital to public confidence in the cyber nation's safety.

This bill supports the ongoing work of the Department of Homeland Security in security civilian agency and coordinating with private sector computing network owners and operators.

The nation's critical infrastructure is diverse, complex, and interdependent.

The overwhelming majority of critical infrastructure is privately owned or managed.

Critical Infrastructure owners and operators are uniquely positioned to manage risk to their operations and assets.

What is needed is a better understanding of how vulnerability discoveries lead to better protection for computing networks.

Zero Day Events require a coordinated approach to assignment of responsibility for developing patches or solutions, and a means of effectively distributing the solution without alerting potential terrorist or cyber criminals.

H.R. 3202 provides the Congress with the opportunity to understand the process and procedures used by the Department of Homeland Security and the benefit these disclosures may have for private sector entities participating in programs in support of cybersecurity.

I thank Lillie Coney of my staff and Jean de Pruneda a Fellow on the Committee on Homeland Security for their work on this important legislation.

I ask my colleagues to vote for H.R. 3202.

Mr. Speaker, I rise in support of 3202, The ''Cyber Disclosure Reporting Act.''

I thank Chairman MCCAUL and Ranking Member THOMPSON for their leadership on putting the security of our nation's cyber assets first whether they are computing resources used in voting technology or industrial control systems that support the delivery of electricity, oil and gas, or management of transportation systems that are vital to our nation economic health.

H.R. 3202, the Cyber Vulnerability Disclosure Reporting Act, which I introduced, 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 that 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.

The report may also contain a description of how the Secretary of Homeland Security is working with other Federal entities and critical infrastructure owners and operators to prevent, detect, and mitigate cyber vulnerabilities.

The reason that I worked to bring this bill before the Full House for consideration is the problem often referred to as a ''Zero Day Event.''

A Zero Day Event describes the situation that network security professionals may find themselves when a previously unknown error or flaw in computing code is exploited by a cybercriminal or terrorist.

The term ''Zero Day Event'' simply means that there is zero time to prepare a defense against a cyberattack.

When a defect in software is discovered then network engineers and software companies can work to develop a ''patch'' to fix the problem before it can be exploited by those who may seek to do harm.

H.R. 3202 seeks a report on the ongoing Department of Homeland Security's policies and procedures for coordinating cyber vulnerability disclosures such as Zero Day Events with private sector partners.

Because vulnerabilities can be used by adversaries it is important that this sensitive information be managed securely so details are not routinely made available neither to the public nor to Congress.

H.R. 3202 provides the Congress with the opportunity to understand the process and procedures used by the Department of Homeland Security and the benefit these disclosures may have for private sector entities participating in programs in support of cybersecurity.

I thank Lillie Coney of my staff and Jean de Pruneda a Fellow on the Committee on Homeland Security for their work on this important legislation.

I urge members of the House to vote in favor of H.R. 3202, the Cyber Vulnerabilities Disclosure Act.

Mr. Speaker, H.R. 3202 will give this body important information on our government wide efforts to secure civilian agency networks and the collaborative ongoing work to provide information to private sector partners on computing vulnerabilities.

There's no security in keeping zero day events secure from disclosure and not working on solutions.

Cyber security is found in finding the zero day events, creating solutions to defend against them, and sharing the solutions broadly so that they can be deployed.

Once solutions are in place the Zero Day Event should be disclosed to the public so that scholars and researchers can learn from the experience.

With that, I encourage my colleagues to support H.R. 3202.

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

Mr. ESTES of Kansas. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I once again urge my colleagues to support this bill. With an ever-increasing reliance on technology today, we need to make sure that it is secure and safe for us to use and that the vulnerabilities are addressed so that we can maintain a safe and secure environment.

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 Kansas (Mr. ESTES) that the House suspend the rules and pass the bill, H.R. 3202.

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.

□ 1345

DHS INTERAGENCY COUNTERTERRORISM TASK FORCE ACT OF 2017

Mr. RUTHERFORD. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 4555) to authorize the participation in overseas interagency counterterrorism task forces of personnel of 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. 4555

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 ''DHS Interagency Counterterrorism Task Force Act of 2017''.

SEC. 2. OVERSEAS INTERAGENCY COUNTERTERRORISM TASK FORCE PARTICIPATION.

Section 102 of the Homeland Security Act of 2002 (6 U.S.C. 112) is amended by adding at the end the following new subsection:

''(h) COORDINATION WITH OTHER FEDERAL DEPARTMENTS AND AGENCIES OVERSEAS.—

''(1) IN GENERAL.—The Secretary is authorized to assign Department personnel to participate in overseas interagency counterterrorism task forces to—

''(A) facilitate the sharing of counterterrorism information, and

''(B) combat the threat of terrorism and associated risks to the United States stemming from overseas sources of conflict or terrorism,

as determined by the Secretary.

''(2) PERSONNEL.—In carrying out this subsection, the Secretary may assign personnel from any component of the Department the Secretary determines necessary to participate in the overseas counterterrorism task forces referred to in paragraph (1).''.

SEC. 3. ANNUAL REPORTS.

Not later than 18 months after the date of the enactment of this Act and annually thereafter for three years, the Secretary of Homeland Security shall report to the Committee on Homeland Security, the Committee on Foreign Affairs, the Permanent Select Committee on Intelligence, and the Committee on Armed Services of the House of Representatives and the Committee on Homeland Security and Governmental Affairs, the Committee on Foreign Relations, Select Committee on Intelligence, and the Committee on Armed Services of the Senate on activities carried out pursuant to subsection (h) of section 102 of the Homeland Security Act of 2002 (6 U.S.C. 112), as added by section 2 of this Act.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Florida (Mr. RUTHERFORD) and the gentlewoman from Texas (Ms. JACKSON LEE) each will control 20 minutes.

The Chair recognizes the gentleman from Florida.

GENERAL LEAVE

Mr RUTHERFORD. 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 material on the bill under consideration.

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

There was no objection.

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

Mr. Speaker, as terrorists and foreign fighters in Iraq and Syria seek to return home or travel to other regions in the wake of the defeat of ISIS on the battlefield, cooperation among U.S. military, national security, and law enforcement agencies is vital.

When these fighters move from the Middle East to the West or other regions, information collection and tracking becomes extremely difficult, especially when ensuring that all relevant Federal agencies have access to the same critical information. An enhanced, whole-of-government effort to share information and intelligence related to these fighters and their movements would improve security of the homeland.

In order to achieve this, H.R. 4555 authorizes the Department of Homeland Security Secretary to assign DHS personnel to overseas interagency counterterrorism task forces to facilitate the sharing of counterterrorism information and combat threats stemming from overseas sources of conflict or terrorism. This will enable DHS to build on existing initiatives to colocate DHS personnel with other Federal departments and agencies that play a crucial role in the fight against terrorism.

For example, assigning DHS personnel to the Department of Defense locations would facilitate better collection and sharing of information recovered from those conflict zones, which significantly improves our ability to interdict terrorists before they enter our country.

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

Ms. JACKSON LEE. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I rise in support of H.R. 4555, the DHS Interagency Counterterrorism Task Force Act of 2017.

Mr. Speaker, H.R. 4555 authorizes DHS personnel to participate in overseas interagency counterterrorism task forces. Since the attacks of September 11 and the demise of central al-Qaida, there has been an upsurge in the number of foreign terrorist organizations. The terrorist threat picture demands that DHS work to ''push our borders out'' and deal with terrorist threats overseas. As such, it is important that DHS deploy DHS personnel overseas to engage in counterterrorism information sharing with international partners.

Our close partnerships with countries around the world, especially in Europe, are essential to preventing returning foreign fighters from attacking the U.S. homeland. However, we remain concerned that terrorist organizations, in particular, ISIS, al-Qaida, and their affiliates, continue to plot attacks against the U.S. homeland and our interests abroad.

Authorizing the participation of DHS personnel in overseas interagency counterterrorism task forces will facilitate better counterterrorism information sharing, which will help protect the homeland and U.S. interests abroad. As such, I support this legislation.

Mr. Speaker, in closing, H.R. 4555 authorizes the participation of DHS personnel in overseas interagency counterterrorism task forces. This measure seeks to help safeguard our homeland by fostering DHS overseas partnerships and facilitating counterterrorism information sharing.

I want to thank the gentleman from Florida (Mr. RUTHERFORD) for sponsoring this legislation and for working with me on my amendment, which added reporting language on the activities authorized by this measure.

This is an important step forward and, again, I might emphasize, the work that is being done between the ranking member, Mr. THOMPSON, and the full committee chair, Mr. MCCAUL, in bringing our committee together in producing a myriad of constructive legislation all geared to our task, because, when all is said and done, we are the Homeland Security Committee within the Homeland Security Department, created in the aftermath of the most heinous, horrific tragedy in the history of the United States of recent recollection that was not an incident of war.

Therefore, I think the American people, and I know the American people are owed our diligence and are owed our commitment and are owed our studiousness. I am very pleased to say that, on this committee, the production of legislation that comes to the floor, all is geared to securing the homeland.

Mr. Speaker, I urge passage of H.R. 4555.

Mr. Speaker, I rise in support of H.R. 4555, the "DHS Interagency Counterterrorism Task Force Act of 2017."

H.R. 4555 authorizes DHS personnel to participate in overseas interagency counterterrorism task forces.

Since the attacks of September 11th and the demise of central al Qaeda, there has been an upsurge in the number of foreign terrorist organizations.

The terrorist threat picture demands that DHS work to "push our borders out" and deal with terrorist threats overseas.

As such, it is important that DHS deploy DHS personnel overseas to engage in counter-terrorism information sharing with international partners.

Our close partnerships with countries around the world, especially in Europe, are essential to preventing returning foreign fighters from attacking the U.S. homeland.