across the aisle on national security issues.

Let me say, I never hesitate to say how proud I am of the Foreign Affairs Committee and Chairman ED ROYCE and the leadership of the committee on both sides of the aisle for what we think as being the most bipartisan committee in Congress. It is important when we are talking about foreign policy that America speak with one voice, and it is important when we talk about foreign policy that politics stops at the water's edge.

This bill is a very important bill. It is a great example of what we can produce when we work across the aisle, and I am glad we are getting it across the finish line before we wrap up our work this month.

Mr. Speaker, I urge a ''yes'' vote, and I yield back the balance of my time.

Ms. ROS-LEHTINEN. Mr. Speaker, I echo Mr. ENGEL's remarks that, under the leadership of Chairman ROYCE and Ranking Member ENGEL, our Foreign Affairs Committee is one of the most bipartisan committees of the House.

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

The SPEAKER pro tempore. The question is on the motion offered by the gentlewoman from Florida (Ms. ROS-LEHTINEN) that the House suspend the rules and pass the bill, S. 1595, 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.

HACK YOUR STATE DEPARTMENT ACT

Ms. ROS-LEHTINEN. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 5433) to require the Secretary of State to design and establish a Vulnerability Disclosure Process (VDP) to improve Department of State cybersecurity and a bug bounty program to identify and report vulnerabilities of internet-facing information technology of the Department of State, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 5433

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 ''Hack Your State Department Act''.

SEC. 2. DEFINITIONS.

In this Act:

(1) BUG BOUNTY PROGRAM.—The term ''bug bounty program'' means a program under which an approved individual, organization, or company is temporarily authorized to identify and report vulnerabilities of internet-facing information technology of the Department in exchange for compensation.

(2) DEPARTMENT.—The term ''Department'' means the Department of State.

(3) INFORMATION TECHNOLOGY.—The term ''information technology'' has the meaning given such term in section 11101 of title 40, United States Code.

(4) SECRETARY.—The term ''Secretary'' means the Secretary of State.

SEC. 3. DEPARTMENT OF STATE VULNERABILITY DISCLOSURE PROCESS.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary shall design, establish, and make publicly known a Vulnerability Disclosure Process (VDP) to improve Department cybersecurity by—

(1) providing security researchers with clear guidelines for—

(A) conducting vulnerability discovery activities directed at Department information technology; and

(B) submitting discovered security vulnerabilities to the Department; and

(2) creating Department procedures and infrastructure to receive and fix discovered vulnerabilities.

(b) REQUIREMENTS.—In establishing the VDP pursuant to paragraph (1), the Secretary shall—

(1) identify which Department information technology should be included in the process;

(2) determine whether the process should differentiate among and specify the types of security vulnerabilities that may be targeted;

(3) provide a readily available means of reporting discovered security vulnerabilities and the form in which such vulnerabilities should be reported;

(4) identify which Department offices and positions will be responsible for receiving, prioritizing, and addressing security vulnerability disclosure reports;

(5) consult with the Attorney General regarding how to ensure that approved individuals, organizations, and companies that comply with the requirements of the process are protected from prosecution under section 1030 of title 18, United States Code, and similar provisions of law for specific activities authorized under the process;

(6) consult with the relevant offices at the Department of Defense that were responsible for launching the 2016 Vulnerability Disclosure Program, ''Hack the Pentagon'', and subsequent Department of Defense bug bounty programs;

(7) engage qualified interested persons, including nongovernmental sector representatives, about the structure of the process as constructive and to the extent practicable; and

(8) award a contract to an entity, as necessary, to manage the process and implement the remediation of discovered security vulnerabilities.

(c) ANNUAL REPORTS.—Not later than 180 days after the establishment of the VDP under subsection (a) and annually thereafter for the next six years, the Secretary of State shall submit to the Committee on Foreign Affairs of the House of Representatives and the Committee on Foreign Relations of the Senate a report on the following with respect to the VDP:

(1) The number and severity, in accordance with the National Vulnerabilities Database of the National Institute of Standards and Technology, of security vulnerabilities reported.

(2) The number of previously unidentified security vulnerabilities remediated as a result.

(3) The current number of outstanding previously unidentified security vulnerabilities and Department of State remediation plans.

(4) The average length of time between the reporting of security vulnerabilities and remediation of such vulnerabilities.

(5) An estimate of the total cost savings of discovering and addressing security vulnerabilities submitted through the VDP.

(6) The resources, surge staffing, roles, and responsibilities within the Department used to implement the VDP and complete security vulnerability remediation.

(7) Any other information the Secretary determines relevant.

SEC. 4. DEPARTMENT OF STATE BUG BOUNTY PILOT PROGRAM.

(a) ESTABLISHMENT OF PILOT PROGRAM.—

(1) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Secretary shall establish a bug bounty pilot program to minimize security vulnerabilities of internet-facing information technology of the Department.

(2) REQUIREMENTS.—In establishing the pilot program described in paragraph (1), the Secretary shall—

(A) provide compensation for reports of previously unidentified security vulnerabilities within the websites, applications, and other internet-facing information technology of the Department that are accessible to the public;

(B) award a contract to an entity, as necessary, to manage such pilot program and for executing the remediation of security vulnerabilities identified pursuant to subparagraph (A);

(C) identify which Department information technology should be included in such pilot program;

(D) consult with the Attorney General on how to ensure that approved individuals, organizations, or companies that comply with the requirements of such pilot program are protected from prosecution under section 1030 of title 18, United States Code, and similar provisions of law for specific activities authorized under such pilot program;

(E) consult with the relevant offices at the Department of Defense that were responsible for launching the 2016 ''Hack the Pentagon'' pilot program and subsequent Department of Defense bug bounty programs;

(F) develop a process by which an approved individual, organization, or company can register with the entity referred to in subparagraph (B), submit to a background check as determined by the Department, and receive a determination as to eligibility for participation in such pilot program;

(G) engage qualified interested persons, including nongovernmental sector representatives, about the structure of such pilot program as constructive and to the extent practicable; and

(H) consult with relevant United States Government officials to ensure that such pilot program compliments persistent network and vulnerability scans of the Department of State's internet-accessible systems, such as the scans conducted pursuant to Binding Operational Directive BOD-15-01.

(3) DURATION.—The pilot program established under paragraph (1) should be short-term in duration and not last longer than one year.

(b) REPORT.—Not later than 180 days after the date on which the bug bounty pilot program under subsection (a) is completed, the Secretary shall submit to the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives a report on such pilot program, including information relating to—

(1) the number of approved individuals, organizations, or companies involved in such pilot program, broken down by the number of approved individuals, organizations, or companies that—

(A) registered;

(B) were approved;

(C) submitted security vulnerabilities; and

(D) received compensation;

(2) the number and severity, in accordance with the National Vulnerabilities Database of the National Institute of Standards and

Technology, of security vulnerabilities reported as part of such pilot program;

(3) the number of previously unidentified security vulnerabilities remediated as a result of such pilot program;

(4) the current number of outstanding previously unidentified security vulnerabilities and Department remediation plans;

(5) the average length of time between the reporting of security vulnerabilities and remediation of such vulnerabilities;

(6) the types of compensation provided under such pilot program; and

(7) the lessons learned from such pilot program.

The SPEAKER pro tempore. Pursuant to the rule, the gentlewoman from Florida (Ms. ROS-LEHTINEN) and the gentleman from New York (Mr. ENGEL) each will control 20 minutes.

The Chair recognizes the gentlewoman from Florida.

GENERAL LEAVE

Ms. ROS-LEHTINEN. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days to revise and extend their remarks and to include extraneous material on this measure.

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

There was no objection.

Ms. ROS-LEHTINEN. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, a massive breach of the State Department's unclassified computer network in 2014 exposed grave weaknesses in its information technology systems. And in the years since that attack, problems have continued to mount.

The Department's cybersecurity response program received a D rating, the lowest of any agency, on its Federal Information Security Management Act report card in 2017. And just this month, the Department revealed that it recently suffered a breach of its unclassified email system, which exposed the personal information of some of its employees.

Mr. Speaker, more must be done to ensure cost-effective solutions to the Department's information technology security challenges.

The Hack Your State Department Act, authored by my Foreign Affairs Committee colleagues TED LIEU and TED YOHO, will help address cybersecurity gaps at the Department. This bill will crowdsource solutions and offer a layered approach to information technology security, consistent with the 2017 Report to the President on Federal IT Modernization.

This bill achieves this in two ways:

First, the bill establishes a vulnerability disclosure process to give security researchers clear guidelines for discovering and reporting cybersecurity vulnerabilities. This is considered a best practice in the private sector and, frankly, should be done in all government agencies.

Second, this bill would establish a bounty pilot program at the Department to reward ethical hackers for discovering and reporting vulnerabilities. Numerous private-sector companies and the Department of Defense have used programs like this to improve their cyber defenses at minimal cost.

The Department said that its Hack the Pentagon program ''demonstrated the power of engaging the hacker community to help address cybersecurity challenges of the Department of Defense.''

In its first pilot, hackers identified over 130 unique vulnerabilities, exceeding the Defense Department's expectations so much that it announced plans to expand the program to all of its more than 700 websites.

Both the vulnerability disclosure process and the bounty pilot program are designed to complement persistent network scans currently done by the Department of Homeland Security and other cybersecurity activities undertaken by the Department of State.

As a national security Department, the State Department must do more to secure its networks. The Hack Your State Department Act is a small but important step to bring cost-effective solutions commonly used in the private sector to bear in support of this goal.

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

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

Mr. Speaker, I rise in support of this measure.

Mr. Speaker, I thank Representative LIEU of southern California, a very valued member of the Committee on Foreign Affairs, for his hard work on this bill.

It is important, Mr. Speaker, that we modernize our agencies across government to better deal with 21st century challenges.

The State Department is under constant threat of cyberattacks from foreign actors bent on stealing our secrets, disrupting our foreign policy, and undermining our security.

Just 8 days ago, it was reported that the State Department's email system was breached. This time, whoever was behind the attack got ahold of private information about State Department personnel. Who knows what they will get their hands on next time.

Mr. LIEU's bill will help shore up the State Department against this sort of intrusion. First of all, it requires the Secretary of State to get out ahead of this problem. Instead of waiting for the next attack to happen, this bill would mandate a plan for researchers to actively seek out and report vulnerabilities.

Secondly, this bill launches a new initiative, a so-called bug bounty program. This seeks to tap the expertise of everyday Americans by rewarding citizens who uncover and report security risks in the Department's computer system. It will also allow security researchers and friendly hackers to find the cracks in the system so that the Department can patch them.

This effort is modeled after a very successful program at the Defense Department, which got off the ground in 2016. Since then, 1,400 people have registered to participate, and they have found roughly 140 vulnerabilities.

Our Federal agencies should learn from one another. It is just common sense to put this tested practice to work at the State Department and elsewhere.

Mr. Speaker, I commend Mr. LIEU. I am glad to support this bill, and I reserve the balance of my time.

Ms. ROS-LEHTINEN. Mr. Speaker, I reserve the balance of my time.

Mr. ENGEL. Mr. Speaker, it is my pleasure to yield 5 minutes to the gentleman from California (Mr. TED LIEU), the author of the bill.

Mr. TED LIEU of California. Mr. Speaker, I thank Representative ENGEL for yielding.

Mr. Speaker, I rise today in support of my legislation, H.R. 5433, the Hack Your State Department Act, that I coauthored with my friend, TED YOHO of Florida.

Over the years, the State Department has faced mounting cybersecurity threats from both criminal enterprises and state-sponsored hackers. In 2014, for instance, the Department was infiltrated by Russian hackers and had to temporarily shut down its email system.

Just last week, the State Department suffered another cybersecurity breach that exposed the personal information of a number of its employees.

As an agency with a critical national security role, we must do more to protect the State Department's cybersecurity. If there is any doubt that diplomatic cables cannot be sent to Washington securely or if sensitive diplomatic subjects are revealed, it jeopardizes the whole operation.

As a recovering computer science major, I recognize that there are proven tools at our disposal to improve cybersecurity that the Department has yet to adopt. One such tool is to enlist the help of America's top security researchers to find weaknesses in our cybersecurity. This legislation will bring that tool to the State Department after it has been proven successful in both the private sector, as well as at the Pentagon.

My legislation will do two things. The first step of this bill is to establish what is called a vulnerability disclosure process, which sets clear rules of the road so that, when people outside the Department discover vulnerabilities on Department systems, they can report it in a safe, secure, and legal manner with the confidence that the Department will actually fix the problems.

□ 2245

We cannot afford to allow vulnerabilities discovered in the wild remain known to hackers but unknown to the Department. This should be an easy fix.

The second step is to actually pay vetted white-hat hackers to find vulnerabilities. The Department of Defense proved the success of their bug

bounty program back in 2016. Over a 24-day period, the Pentagon learned of and fixed over 138 vulnerabilities in its systems.

A 2017 report to the President on Federal IT modernization stated: ''Agencies must take a layered approach to penetration testing. . . . At a bare minimum, agencies should establish vulnerability disclosure policies. . . . Agencies should also identify programs that are appropriate to place under public bug bounty programs such as those run by the Department of Defense or GSA.''

Today, with H.R. 5433, the House of Representatives is taking these recommendations to heart and helping to improve cybersecurity at the Department of State.

Mr. Speaker, I would like to thank Representative YOHO for partnering with me on this important legislation. I would like to thank Chairman ROYCE, Ranking Member ENGEL, and their staff for moving this bill through our committee.

Ms. ROS-LEHTINEN. I continue to reserve the balance of my time, Mr. Speaker.

Mr. ENGEL. Mr. Speaker, I am prepared to close.

In closing, I want to again thank Mr. LIEU and Chairman ROYCE.

It seems to me, Mr. Speaker, that we have been caught flatfooted before a range of new threats, including cyber attacks. Our agencies have not done enough to root out vulnerabilities, and, frankly, Congress hasn't done enough either to make sure our agencies across the government have the tools they need to tackle these challenges.

I hope going forward we will be able to take a comprehensive look at cyber threats and make sure the State Department, and all our departments and agencies, are up to the task.

For now, this bill is a good step in the right direction. It replicates an approach that has worked well over the last few years.

Mr. Speaker, I urge all Members to support it, and I yield back the balance of my time.

Ms. ROS-LEHTINEN. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, in closing, I would like to thank my colleagues—TED LIEU, a hardworking member of our Foreign Affairs Committee, and TED YOHO, chairman of the Subcommittee on Asia and the Pacific—for crafting this bipartisan legislation.

By unleashing the expertise of patriotic hackers, this bill will help the State Department identify and patch vulnerabilities on its computer systems.

The Hack Your State Department Act takes an innovative approach to improving network security at a Department that is in such desperate need of new solutions and improved capabilities.

Mr. Speaker, I urge passage of this bipartisan bill, and I yield back the balance of my time.

Ms. JACKSON LEE. Mr. Speaker, I rise today in support of H.R. 5433, the ''Hack Your State Department Act''.

This act would direct the State Department to establish what is known in the cybersecurity community as a 'bug bounty' program.

Bug bounty programs, also known as Vulnerability Disclosure Programs, are comprehensive efforts by an organization to lay out the method by which members of the public may report any security vulnerabilities to an entity.

They also lay out which of their resources are covered by this policy, and how any identified vulnerabilities will be addressed.

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, including the State Department, must evolve to keep pace with improved standards and policies.

Without an honest effort to seek awareness of the security of the State Department network, users, and devices, we will continue to be increasingly vulnerable.

To that end, H.R. 5433 recognizes the importance of a dynamic approach that will help secure federal networks and data, beginning with the State Department, as well as provide improved information on vulnerabilities and security practices across the various agencies.

Without codifying this concrete measure to improve awareness of federal network security at the State Department, this important agency will remain vulnerable.

We have seen an unfortunate loss of cybersecurity talent at the State Department this year.

Further, even 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 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.

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. 5433, the ''Hack Your State Department Act''.

The SPEAKER pro tempore. The question is on the motion offered by the gentlewoman from Florida (Ms. ROS-LEHTINEN) that the House suspend the rules and pass the bill, H.R. 5433, 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.

HONORING WENDY GRANT

(Ms. ROS-LEHTINEN asked and was given permission to address the House for 1 minute and to revise and extend her remarks.)

Ms. ROS-LEHTINEN. Mr. Speaker, Wendy Grant was a south Florida philanthropist who dedicated her all-too-brief life to serving others. Hers was a legacy of service to our community. She was also a well-respected aide to both Senator Connie Mack when he served here in D.C. and our Governor of Florida, Jeb Bush.

Here is a picture of lovely Wendy Grant. It says: A life lived for the greater good.

That was Wendy Grant.

Wendy was also a zealous advocate for children through her work with the St. Jude Children's Hospital, and she raised funds for its noble mission year after year.

Anyone who knew Wendy loved Wendy. She was famous for her birthday emails recognizing each of her friend's birthdays and updating us all on everyone's lives.

Remedios Diaz-Oliver, Lilliam Machado, and I were about to bestow upon Wendy the title of Honorary Cuban American, because she loved our history and our traditions. We will present the certificate when we honor her life next week at her church for her service.

Wendy Grant was a south Florida person to the hilt. She was warm; she was caring; and she was loyal. We will all miss Wendy Grant dearly.

Godspeed, my friend.

MOMENT OF SILENCE FOR DEPUTY ROBERT KUNZE

(Mr. ESTES of Kansas asked and was given permission to address the House for 1 minute and to revise and extend his remarks.)

Mr. ESTES of Kansas. Mr. Speaker, I rise to honor the life and service of Sedgwick County Sheriff's Deputy Robert Kunze III.