

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.