West Berlin at the Brandenburg Gate in 1963: ''Ich bien ein Berliner.''

Mr. Speaker, the principle of collective defense is the core of NATO's founding treaty and the NATO alliance has been the backbone of American national security and foreign policy for nearly 70 years.

The strength and solidarity of this western alliance kept Western Europe whole, prosperous, and free and paved the way for the collapse of the Soviet Union and the liberation of the nations of Eastern and Central Europe, many of which have now been integrated into NATO.

The Constitution of the United States grants Congress the sole power to declare war, but Article 5 does not increase the chance of war.

Rather, NATO is a bulwark against the outbreak of war because it deters aggression by any adversary.

As a result, NATO is the most successful military alliance in world history, successfully deterring the outbreak of a third world war, seeing the Cold War to a victorious conclusion, and protecting the principle of territorial integrity.

This is why I strongly support H.R. 676, which reaffirms the commitment of the Congress to Article 5 of the North Atlantic Treaty.

The legislation also expresses support for the agreement reached at the 2014 NATO Wales Summit calling upon each NATO member nation to allocate at least two percent of its gross domestic product to defense by 2024.

The legislation also expresses congressional support for robust United States funding for the European Deterrence Initiative, which increases the ability of the United States and its allies to deter and defend against Russian aggression.

Finally, H.R. 676 provides that no funds are authorized to be appropriated, obligated, or expended to take any action to withdraw the United States from the North Atlantic Treaty signed on April 14, 1949, in Washington, D.C., between the United States of America and the other 15 founding members of the North Atlantic Treaty 16 Organization.

I urge all Members to join me in affirming the commitment of the United States to the North Atlantic Treaty, which has kept the peace on the European continent for nearly 70 years and continues to serve as a bulwark and deterrent to Russian aggression and its long-held strategic objective of splitting the Western Alliance that has done more than any other collective enterprise in history to preserve and maintain international peace.

Mr. KINZINGER. Mr. Speaker, I rise today in support of H.R. 676, the NATO Support Act.

For almost 70 years, the North Atlantic Treaty Organization has formed the cornerstone of national security policy for the postwar world order. Through this alliance, we have successfully defeated communism, halted genocide in the Balkans, defended against threats from terrorism in Afghanistan, and maintained cohesion with our like-minded democratic partners. By forming these relationships, we have successfully defended our values and principles in the face of repression and tyranny. While we no longer face the same existential threat posed by the Soviet Union, NATO's resolve and stability has helped maintain peace in a world drowning with strongmen. That is why I stand in support this bipartisan legislation.

H.R. 676 codifies Congressional support of the North Atlantic Treaty Organization, while calling on our allies to modernize their capabilities and meet the Wales Defense Investment Pledge. Five years ago, NATO members agreed to reverse their declining defense budgets and balance the responsibilities that come with our partnership. While it was an ambitious goal, we have already seen many of our partners increase their commitments to our mutual security by meeting the agreed upon threshold of spending 2 percent of GDP on defense.

As part of our commitment, we must continue to support the European Deterrence Initiative, by maintaining a robust U.S. presence throughout the European theater. Most importantly, this legislation would ensure that no matter which way the political winds blow no administration could use funds to withdraw from this treaty without the consent of the coequal branch of government in Congress.

NATO is not some outdated relic from past conflicts. We are living in a world where repression is on the rise, and human freedom is increasingly in jeopardy. What our partnership stands for, what NATO defends—it gives hope to the repressed. That is why I urge my colleagues in joining me in passing this legislation.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from New York (Mr. ENGEL) that the House suspend the rules and pass the bill, H.R. 676.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds being in the affirmative, the ayes have it.

Mr. ENGEL. Mr. Speaker, on that I demand the yeas and nays.

The yeas and nays were ordered.

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX, further proceedings on this motion will be postponed.

HACK YOUR STATE DEPARTMENT ACT

Mr. ENGEL. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 328) 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.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 328

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 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 contracts to entities, 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 VDP, including information relating to the following:

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

(6) 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 contracts to entities, 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 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 complements 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 gentleman from New York (Mr. ENGEL) and the gentleman from Texas (Mr. MCCAUL) each will control 20 minutes.

The Chair recognizes the gentleman from New York.

GENERAL LEAVE

Mr. ENGEL. Mr. Speaker, I ask unanimous consent that all Members have 5 legislative days in which to revise and extend their remarks and include extraneous material on H.R. 328, the Hack Your State Department Act.

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

There was no objection.

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

Mr. Speaker, let me start by thanking Representative LIEU, a valued member of the Committee on Foreign Affairs, for his hard work on this bill and on everything else.

This important legislation passed the House in the last Congress with strong bipartisan support, and I certainly support passing it again.

Mr. Speaker, it is critical that we modernize our government to better deal with 21st century challenges. The State Department is under the constant threat of cyberattack from foreign actors bent on stealing our secrets, disrupting our foreign policy, and undermining our security.

Mr. LIEU's bill will help shore up the State Department against this sort of intrusion.

First, 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, the 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 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 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 am very glad to support this bill, and I reserve the balance of my time.

Mr. MCCAUL. Mr. Speaker, I yield myself as much time as I may consume.

Mr. Speaker, I rise in support of the Hack Your State Department Act, which will help address lingering cybersecurity gaps at the Department of State.

The massive breach of the State Department's unclassified computer network in 2014 exposed grave weaknesses.

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.

Last September, the Department revealed that it recently suffered a breach of its unclassified email system, which exposed the personal information of some of its employees.

The Department needs cost-effective solutions to these IT security challenges.

Today's legislation directs the Secretary of State to develop and implement a vulnerability disclosure process that will allow threat researchers from the private sector to identify and report cybersecurity flaws.

Currently, there is no legal avenue that allows them to do so. This bill fixes that problem.

The bill will establish a ''bug bounty'' pilot program to reward ethical hackers for discovering and reporting vulnerabilities at the Department.

These programs have been used successfully by the Defense Department and numerous private companies to improve their cyber defenses at minimal cost. In fact, I remember introducing a similar bill for the Department of Homeland Security.

As a national security agency, the State Department must do more to secure its networks. The Hack Your State Department Act is a small but important step towards cost-effective solutions.

Mr. Speaker, I want to thank the author, Mr. LIEU, for putting his computer science background to work here in the Congress, and he understands, I believe, the nature of the threats that we face in the cyber realm and the importance of a strong cybersecurity partnership between the public and the private sectors.

Mr. Speaker, I urge support, and I reserve the balance of my time.

Mr. ENGEL. Mr. Speaker, I yield 4 minutes to the gentleman from California (Mr. TED LIEU), the author of this bill and a very honored member of the Foreign Affairs Committee.

Mr. TED LIEU of California. Mr. Speaker, I thank Ranking Member

MCCAUL for his support of this legislation and I thank Chairman ENGEL for his leadership of the House Foreign Affairs Committee.

Mr. Speaker, I rise in support of my legislation, H.R. 328, which will strengthen cybersecurity at the State Department. This legislation is known as the Hack Your State Department Act. It is introduced with my colleague, TED YOHO of Florida, and has received strong bipartisan support, and that is because there is no such thing as Republican cybersecurity or Democratic cybersecurity; it is just cybersecurity, and we are behind.

American institutions are under constant attack from criminals, from foreign intelligence services, and from everyday hackers. That is why last term, I was very honored to have introduced legislation known as the Hack DHS Act, along with Senators MAGGIE HASSAN, ROB PORTMAN, KAMALA HARRIS, and Congressman SCOTT TAYLOR. That legislation was signed into law last month.

This legislation focuses on the State Department. It is something that we need to do, because we know that the State Department over the years 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.

Last year, the State Department suffered another breach of its email system, exposing the personal information of a number of its employees.

As a recovering computer science major, I recognize there are improvement tools at our disposal to improve cybersecurity that the State Department has not yet adopted, and one such tool is exactly what this bill will do.

□ 1730

This bill does primarily two things. The first is to establish what is called a vulnerability disclosure process, which sets clear rules of the road so, 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 State Department will actually fix the problems. 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 the bug bounty program back in 2016. Over a 24-day period, the Pentagon learned of and fixed over 138 vulnerabilities in its systems. The DHS is now also going to start this very same program. Hopefully, the State Department will be able to do this, as well, when this legislation is signed into law.

Let me conclude by saying that, today, with H.R. 328, the House of Representatives is taking these recommendations to heart and helping to improve cybersecurity at the Department of State.

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

In closing, I want to again thank the author, Mr. LIEU, and his primary sponsor, Mr. YOHO, for this creative effort to harness private-sector know-how to improve cyber defenses at the Department of State.

As the gentleman, Mr. LIEU, indicated, I moved this very same legislation when I was chairman of the Homeland Security Committee for the Department of Homeland Security, and I believe it is working very effectively. The Department of Defense has done the same thing. Now it is time for the Department of State to take on this challenge as well.

Mr. Speaker, I support this bill, and I yield back the balance of my time.

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

Mr. Speaker, I again want to thank Mr. LIEU for this important piece of legislation.

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

As we head into the 116th Congress, I will be leading the Foreign Affairs Committee in focusing on this. We will be taking a comprehensive look at cyber threats to make sure the State Department and all our departments and agencies are properly equipped to handle this challenge. For now, this bill is an important step in the right direction.

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

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from New York (Mr. ENGEL) that the House suspend the rules and pass the bill, H.R. 328.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds being in the affirmative, the ayes have it.

Mr. ENGEL. Mr. Speaker, on that I demand the yeas and nays.

The yeas and nays were ordered.

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX, further proceedings on this motion will be postponed.

RESIGNATION FROM THE HOUSE OF REPRESENTATIVES

The SPEAKER pro tempore laid before the House the following resignation from the House of Representatives:

CONGRESS OF THE UNITED STATES,
HOUSE OF REPRESENTATIVES,
Washington, DC, January 17, 2019.

Hon. NANCY PELOSI,
Speaker of the House of Representatives, Washington, DC.

SPEAKER PELOSI: I write to you to tender my resignation from the U.S. House of Representatives, 12th District of Pennsylvania, effective 12:01 a.m. Wednesday January 23, 2019.

Sincerely,

TOM MARINO,
Member of Congress.

CONGRESS OF THE UNITED STATES,
HOUSE OF REPRESENTATIVES,
Washington, DC, January 17, 2019.

Hon. TOM WOLF,
Governor,
Harrisburg, PA.

GOVERNOR WOLF: I write to you to tender my resignation from the U.S. House of Representatives, 12th District of Pennsylvania, effective 12:01 a.m. Wednesday January 23, 2019.

Sincerely,

TOM MARINO,
Member of Congress.

RECESS

The SPEAKER pro tempore. Pursuant to clause 12(a) of rule I, the Chair declares the House in recess until approximately 6:30 p.m. today.

Accordingly (at 5 o'clock and 33 minutes p.m.), the House stood in recess.

□ 1830

AFTER RECESS

The recess having expired, the House was called to order by the Speaker pro tempore (Mr. CUELLAR) at 6 o'clock and 30 minutes p.m.

ANNOUNCEMENT BY THE SPEAKER PRO TEMPORE

The SPEAKER pro tempore. Proceedings will resume on questions previously postponed.

Votes will be taken in the following order:

Motion to suspend the rules and pass H.R. 676;

Motion to suspend the rules and pass H.R. 328; and

Agreeing to the Speaker's approval of the Journal, if ordered.

The first electronic vote will be conducted as a 15-minute vote. Pursuant to clause 9 of rule XX, remaining electronic votes will be conducted as 5-minute votes.

NATO SUPPORT ACT

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX, the unfinished business is the vote on the motion to suspend the rules and pass the bill (H.R. 676), to reiterate the support of the Congress of the United States for the North Atlantic Treaty Organization, and for other purposes, on which the yeas and nays were ordered.

The Clerk read the title of the bill.

The SPEAKER pro tempore. The question is on the motion offered by