Mr. Speaker, I want to again thank Ms. KELLY for her leadership on this issue, as well as Chairman ROYCE and Ranking Member ENGEL for their work on this important piece of legislation.

I encourage my colleagues to support this bill.

Mr. BERA. Mr. Speaker, I yield myself the balance of my time.

I will close by again thanking Chairman ROYCE for bringing this legislation to the floor.

We have no greater duty on our committee than to protect Americans serving abroad. I am very pleased that we are making several essential fixes in our approach to embassy security in this legislation and authorizing the embassy security, construction, and maintenance at a robust level.

We live in a dangerous time, and the Trump administration's budget would put our diplomats at even greater risk than what they have already faced on a daily basis, so I am glad that the House is stepping in to do what is needed.

Finally, let me say again, while I am pleased this bill is moving forward, I don't believe the window has closed on getting a comprehensive State Department authorization bill to the President's desk, and I continue to stand ready to work with the chairman to do just that.

Mr. Speaker, I support the chairman's motion; I urge all Members to do the same.

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

Mr. ROYCE of California. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, America's embassies obviously are forward operating bases for our democracy, for our system. The brave men and women who serve at those posts represent our country on a daily basis and represent them often in a difficult and increasingly dangerous environment.

As we have tragically seen before, diplomatic posts overseas are often the first and easiest targets our enemies choose to attack. Importantly, this legislation will improve the security, the functionality, and the efficiency of our embassies and our consulates through enhanced oversight and better management of the construction of new diplomatic facilities.

So, again, I want to thank Chairman MIKE MCCAUL of Texas, and I want to thank Representative ROBIN KELLY, as well as Ranking Member ENGEL and the many members of the committee from both sides of the aisle who have worked extensively on this important piece of legislation.

Our embassies project American power. They do reflect our values. We owe it to our diplomats and the American people to build the best embassies possible.

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 California (Mr. ROYCE) that the House suspend the rules and pass the bill, H.R. 4969, 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 DETERRENCE AND RESPONSE ACT OF 2018

Mr. ROYCE of California. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 5576) to address state-sponsored cyber activities against the United States, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 5576

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 Deterrence and Response Act of 2018''.

SEC. 2. FINDINGS.

Congress finds the following:

(1) On February 13, 2018, the Director of National Intelligence stated in his testimony before the Senate Select Committee on Intelligence that ''Russia, China, Iran, and North Korea will pose the greatest cyber threats to the United States during the next year'' through the use of cyber operations as low-cost tools of statecraft, and assessed that these states would ''work to use cyber operations to achieve strategic objectives unless they face clear repercussions for their cyber operations''.

(2) The 2017 Worldwide Threat Assessment of the United States Intelligence Community stated that ''The potential for surprise in the cyber realm will increase in the next year and beyond as billions more digital devices are connected—with relatively little built-in security—and both nation states and malign actors become more emboldened and better equipped in the use of increasingly widespread cyber toolkits. The risk is growing that some adversaries will conduct cyber attacks—such as data deletion or localized and temporary disruptions of critical infrastructure—against the United States in a crisis short of war.''.

(3) On March 29, 2017, President Donald J. Trump deemed it necessary to continue the national emergency declared in Executive Order 13694 as ''Significant malicious cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States, continue to pose an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States.''.

(4) On January 5, 2017, former Director of National Intelligence, James Clapper, former Undersecretary of Defense for Intelligence, Marcel Lettre, and the Commander of the United States Cyber Command, Admiral Michael Rogers, submitted joint testimony to the Committee on Armed Services of the Senate that stated ''As of late 2016 more than 30 nations are developing offensive cyber attack capabilities'' and that ''Protecting critical infrastructure, such as crucial energy, financial, manufacturing, transportation, communication, and health systems, will become an increasingly complex national security challenge.''.

(5) There is significant evidence that hackers affiliated with foreign governments have conducted cyber operations targeting companies and critical infrastructure sectors in the United States as the Department of Justice and the Department of the Treasury have announced that—

(A) on March 15, 2018, five Russian entities and 19 Russian individuals were designated under the Countering America's Adversaries Through Sanctions Act, as well as pursuant to Executive Order 13694, for interference in the 2016 United States elections and other malicious cyber-enabled activities;

(B) on March 24, 2016, seven Iranians working for Iran's Revolutionary Guard Corps-affiliated entities were indicted for conducting distributed denial of service attacks against the financial sector in the United States from 2012 to 2013; and

(C) on May 19, 2014, five Chinese military hackers were charged for hacking United States companies in the nuclear power, metals, and solar products industries, and engaging in economic espionage.

(6) In May 2017, North Korea released ''WannaCry'' pseudo-ransomware, which posed a significant risk to the economy, national security, and the citizens of the United States and the world, as it resulted in the infection of over 300,000 computer systems in more than 150 countries, including in the healthcare sector of the United Kingdom, demonstrating the global reach and cost of cyber-enabled malicious activity.

(7) In June 2017, Russia carried out the most destructive cyber-enabled operation in history, releasing the NotPetya malware that caused billions of dollars' worth of damage within Ukraine and across Europe, Asia, and the Americas.

(8) In May 2018, the Department of State, pursuant to section 3(b) of Executive Order 13800, prepared recommendations to the President on Deterring Adversaries and Better Protecting the American People From Cyber Threats, which stated ''With respect to activities below the threshold of the use of force, the United States should, working with likeminded partners when possible, adopt an approach of imposing swift, costly, and transparent consequences on foreign governments responsible for significant malicious cyber activities aimed at harming U.S. national interests.''.

SEC. 3. ACTIONS TO ADDRESS STATE-SPONSORED CYBER ACTIVITIES AGAINST THE UNITED STATES.

(a) DESIGNATION AS A CRITICAL CYBER THREAT ACTOR.—

(1) IN GENERAL.—The President, acting through the Secretary of State, and in coordination with other relevant Federal agency heads, shall designate as a critical cyber threat actor—

(A) each foreign person and each agency or instrumentality of a foreign state that the President determines to be knowingly responsible for or complicit in, or have engaged in, directly or indirectly, state-sponsored cyber activities that are reasonably likely to result in, or have contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that have the purpose or effect of—

(i) causing a significant disruption to the availability of a computer or network of computers;

(ii) harming, or otherwise significantly compromising the provision of service by, a computer or network of computers that support one or more entities in a critical infrastructure sector;

(iii) significantly compromising the provision of services by one or more entities in a critical infrastructure sector;

(iv) causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain;

(v) destabilizing the financial sector of the United States by tampering with, altering, or causing a misappropriation of data; or

(vi) interfering with or undermining election processes or institutions by tampering with, altering, or causing misappropriation of data;

(B) each foreign person that the President has determined to have knowingly, significantly, and materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, any activities described in subparagraph (A) by a foreign person or agency or instrumentality of a foreign state designated as a critical cyber threat actor under subparagraph (A); and

(C) each agency or instrumentality of a foreign state that the President has determined to have significantly and materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, any activities described in subparagraph (A) by a foreign person or agency or instrumentality of a foreign state designated as a critical cyber threat actor under subparagraph (A).

(2) PUBLICATION IN FEDERAL REGISTER.—

(A) IN GENERAL.—The President shall—

(i) publish in the Federal Register a list of each foreign person and each agency or instrumentality of a foreign state designated as a critical cyber threat actor under this subsection; and

(ii) regularly update such list not later than seven days after making any changes to such list, and publish in the Federal Register such updates.

(B) EXCEPTION.—

(i) IN GENERAL.—The President may withhold from publication in the Federal Register under subparagraph (A) the identification of any foreign person or agency or instrumentality of a foreign state designated as a critical cyber threat actor under this subsection if the President determines that withholding such identification—

(I) in the national interests of the United States; or

(II) is for an important law enforcement purpose.

(ii) TRANSMISSION.—If the President exercises the authority under this subparagraph to withhold from publication in the Federal Register the identification of a foreign person or agency or instrumentality of a foreign state designated as a critical cyber threat actor under this subsection, the President shall transmit to the appropriate congressional committees in classified form a report containing any such identification, together with the reasons for such exercise.

(b) NON-TRAVEL-RELATED SANCTIONS.—

(1) IN GENERAL.—The President shall impose one or more of the applicable sanctions described in paragraph (2) with respect to each foreign person and each agency or instrumentality of a foreign state designated as a critical cyber threat actor under subsection (a).

(2) SANCTIONS DESCRIBED.—The sanctions described in this paragraph are the following:

(A) The President may provide for the withdrawal, limitation, or suspension of nonhumanitarian United States development assistance under chapter 1 of part I of the Foreign Assistance Act of 1961.

(B) The President may provide for the withdrawal, limitation, or suspension of United States security assistance under part II of the Foreign Assistance Act of 1961.

(C) The President may direct the United States executive director to each international financial institution to use the voice and vote of the United States to oppose any loan from the international financial institution that would benefit the designated foreign person or the designated agency or instrumentality of a foreign state.

(D) The President may direct the Overseas Private Investment Corporation, or any other United States Government agency not to approve the issuance of any (or a specified number of) guarantees, insurance, extensions of credit, or participations in the extension of credit.

(E) The President may, pursuant to such regulations or guidelines as the President may prescribe, prohibit any United States person from investing in or purchasing significant amounts of equity or debt instruments of the designated foreign person.

(F) The President may, pursuant to procedures the President shall prescribe, which shall include the opportunity to appeal actions under this subparagraph, prohibit any United States agency or instrumentality from procuring, or entering into any contract for the procurement of, any goods, technology, or services, or classes of goods, technology, or services, from the designated foreign person or the designated agency or instrumentality of a foreign state.

(G) The President may order the heads of the appropriate United States agencies to not issue any (or a specified number of) specific licenses, and to not grant any other specific authority (or a specified number of authorities), to export any goods or technology to the designated foreign person or the designated agency or instrumentality of a foreign state under—

(i) the Export Administration Act of 1979 (as continued in effect pursuant the International Emergency Economic Powers Act);

(ii) the Arms Export Control Act;

(iii) the Atomic Energy Act of 1954; or

(iv) any other statute that requires the prior review and approval of the United States Government as a condition for the export or re-export of goods or services.

(H)(i) The President may exercise all of the powers granted to the President under the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (except that the requirements of section 202 of such Act (50 U.S.C. 1701) shall not apply) to the extent necessary to block and prohibit all transactions in property and interests in property of the designated foreign person if such property and interests in property are in the United States, come within the United States, or are or come within the possession or control of a United States person.

(ii) The penalties provided for in subsections (b) and (c) of section 206 of the International Emergency Economic Powers Act (50 U.S.C. 1705) shall apply to a person that violates, attempts to violate, conspires to violate, or causes a violation of regulations prescribed under clause (i) to the same extent that such penalties apply to a person that commits an unlawful act described in subsection (a) of such section 206.

(I) The President may, pursuant to such regulations as the President may prescribe, prohibit any transfers of credit or payments between one or more financial institutions or by, through, or to any financial institution, to the extent that such transfers or payments are subject to the jurisdiction of the United States and involve any interest of the designated foreign person.

(c) TRAVEL-RELATED SANCTIONS.—

(1) ALIENS INELIGIBLE FOR VISAS, ADMISSION, OR PAROLE.—An alien who is designated as a critical cyber threat actor under subsection (a) is—

(A) inadmissible to the United States;

(B) ineligible to receive a visa or other documentation to enter the United States; and

(C) otherwise ineligible to be admitted or paroled into the United States or to receive any other benefit under the Immigration and Nationality Act (8 U.S.C. 1101 et seq.).

(2) CURRENT VISAS REVOKED.—The issuing consular officer, the Secretary of State, or the Secretary of Homeland Security (or a designee of either such Secretaries) shall revoke any visa or other entry documentation issued to the foreign person designated as a critical cyber threat actor under subsection (a) regardless of when issued. A revocation under this clause shall take effect immediately and shall automatically cancel any other valid visa or entry documentation that is in the possession of such foreign person.

(d) ADDITIONAL SANCTIONS WITH RESPECT TO FOREIGN STATES.—

(1) IN GENERAL.—The President may impose any of the sanctions described in paragraph (2) with respect to the government of each foreign state that the President has determined aided, abetted, or directed a foreign person or agency or instrumentality of a foreign state designated as a critical cyber threat actor under subsection (a).

(2) SANCTIONS DESCRIBED.—The sanctions referred to in paragraph (1) are the following:

(A) The President may provide for the withdrawal, limitation, or suspension of nonhumanitarian or non-trade-related assistance United States development assistance under chapter 1 of part I of the Foreign Assistance Act of 1961.

(B) The President may provide for the withdrawal, limitation, or suspension of United States security assistance under part II of the Foreign Assistance Act of 1961.

(C) The President may instruct the United States Executive Director to each appropriate international financial institution to oppose, and vote against the extension by such institution of any loan or financial assistance to the government of the foreign state.

(D) No item on the United States Munitions List (established pursuant to section 38 of the Arms Export Control Act (22 U.S.C. 2778)) or the Commerce Control List set forth in Supplement No. 1 to part 774 of title 15, Code of Federal Regulations, may be exported to the government of the foreign state.

(e) IMPLEMENTATION.—The President may exercise all authorities provided under sections 203 and 205 of the International Emergency Economic Powers Act (50 U.S.C. 1702 and 1704) to carry out this section.

(f) COORDINATION.—To the extent practicable—

(1) actions taken by the President pursuant to this section should be coordinated with United States allies and partners; and

(2) the Secretary of State should work with United States allies and partners, on a voluntary basis, to lead an international diplomatic initiative to—

(A) deter critical cyber threat actors and state-sponsored cyber activities; and

(B) provide mutual support to such allies and partners participating in such initiative to respond to such state-sponsored cyber activities.

(g) EXEMPTIONS, WAIVERS, AND REMOVALS OF SANCTIONS AND DESIGNATIONS.—

(1) MANDATORY EXEMPTIONS.—The following activities shall be exempt from sanctions under subsections (b), (c), and (d):

(A) Activities subject to the reporting requirements of title V of the National Security Act of 1947 (50 U.S.C. 413 et seq.), or to any authorized intelligence activities of the United States.

(B) Any transaction necessary to comply with United States obligations under the Agreement between the United Nations and

the United States of America regarding the Headquarters of the United Nations, signed June 26, 1947, and entered into force on November 21, 1947, or under the Vienna Convention on Consular Relations, signed April 24, 1963, and entered into force on March 19, 1967, or under other international obligations.

(2) WAIVER.—The President may waive the imposition of sanctions described in this section for a period of not more than one year, and may renew such waiver for additional periods of not more than one year, if the President transmits to the appropriate congressional committees a written determination that such waiver meets one or more of the following requirements:

(A) Such waiver is in the national interests of the United States.

(B) Such waiver will further the enforcement of this Act or is for an important law enforcement purpose.

(C) Such waiver is for an important humanitarian purpose.

(3) REMOVALS OF SANCTIONS AND DESIGNATIONS.—The President may prescribe rules and regulations for the removal of sanctions under subsections (b), (c), and (d) and the removal of designations under subsection (a) if the President determines that a foreign person, agency or instrumentality of a foreign state, or government of a foreign state subject to such sanctions or such designations, as the case may be, has verifiably ceased its participation in any of the conduct with respect to which such foreign person, agency or instrumentality of a foreign state, or government of a foreign state was subject to such sanctions or designation, as the case may be, under this section, and has given assurances that such foreign person, agency or instrumentality of a foreign state, or government of a foreign state, as the case may be, will no longer participate in such conduct.

(4) EXCEPTION TO COMPLY WITH UNITED NATIONS HEADQUARTERS AGREEMENT.—Sanctions under subsection (c) shall not apply to a foreign person if admitting such foreign person into the United States is necessary to permit the United States to comply with the Agreement regarding the Headquarters of the United Nations, signed at Lake Success June 26, 1947, and entered into force November 21, 1947, between the United Nations and the United States, or other applicable international obligations.

(h) RULE OF CONSTRUCTION.—Nothing in this section may be construed to limit the authority of the President under the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) or any other provision of law to impose sanctions to address critical cyber threat actors and malicious state-sponsored cyber activities.

(i) DEFINITIONS.—In this section:

(1) ADMITTED; ALIEN.—The terms ''admitted'' and ''alien'' have the meanings given such terms in section 101 of the Immigration and Nationality Act (8 U.S.C. 1101).

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

(A) the Committee on Foreign Affairs, the Committee on Financial Services, the Committee on the Judiciary, the Committee on Oversight and Government Reform, and the Committee on Homeland Security of the House of Representatives; and

(B) the Committee on Foreign Relations, the Committee on Banking, Housing, and Urban Affairs, the Committee on the Judiciary, and the Committee on Homeland Security and Governmental Affairs of the Senate.

(3) AGENCY OR INSTRUMENTALITY OF A FOREIGN STATE.—The term ''agency or instrumentality of a foreign state'' has the meaning given such term in section 1603(b) of title 28, United States Code.

(4) CRITICAL INFRASTRUCTURE SECTOR.—The term ''critical infrastructure sector'' means any of the designated critical infrastructure sectors identified in the Presidential Policy Directive entitled ''Critical Infrastructure Security and Resilience'', numbered 21, and dated February 12, 2013.

(5) FOREIGN PERSON.—The term ''foreign person'' means a person that is not a United States person.

(6) FOREIGN STATE.—The term ''foreign state'' has the meaning given such term in section 1603(a) of title 28, United States Code.

(7) KNOWINGLY.—The term ''knowingly'', with respect to conduct, a circumstance, or a result, means that a person has actual knowledge, or should have known, of the conduct, the circumstance, or the result.

(8) MISAPPROPRIATION.—The term ''misappropriation'' means taking or obtaining by improper means, without permission or consent, or under false pretenses.

(9) STATE-SPONSORED CYBER ACTIVITIES.—The term ''state-sponsored cyber activities'' means any malicious cyber-enabled activities that—

(A) are carried out by a government of a foreign state or an agency or instrumentality of a foreign state; or

(B) are carried out by a foreign person that is aided, abetted, or directed by a government of a foreign state or an agency or instrumentality of a foreign state.

(10) UNITED STATES PERSON.—The term ''United States person'' means—

(A) a United States citizen or an alien lawfully admitted for permanent residence to the United States; or

(B) an entity organized under the laws of the United States or of any jurisdiction within the United States, including a foreign branch of such an entity.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from California (Mr. ROYCE) and the gentleman from New York (Mr. ENGEL) each will control 20 minutes.

The Chair recognizes the gentleman from California.

GENERAL LEAVE

Mr. ROYCE of California. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days in which to revise and extend their remarks and to include any extraneous material.

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

There was no objection.

Mr. ROYCE of California. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, in recent years, foreign adversaries have developed sophisticated cyber capabilities that can disrupt our network, that can threaten our critical infrastructure, and that harm our economy and undermine our elections.

Malicious cyber activity topped the Director of National Intelligence's list of worldwide threats in 2018—topped it—ahead of terrorism and weapons of mass destruction; and in testimony before this Congress, Director Coats stated: ''Frankly, the United States is under attack.''

A report by the White House Council of Economic Advisers estimates that malicious cyber activity cost the U.S. economy between $57 billion and over $100 billion in 2016 alone. But it is not just the economic cost of cyber incidents that we should worry about. There are real physical costs to these online attacks as well.

Last year's WannaCry cyberattack by the North Korea regime compromised the U.K.'s healthcare sector, if you will recall. In 2016, Russian cyber actors attempted to interfere in our election—an assault on our very democracy—and these attacks by Russia continue today. Despite the gravity of this threat, the U.S. continues to lack a unified framework to deter and respond to state-sponsored cyber activities.

I applaud Representative YOHO and Ranking Member ENGEL for introducing the Cyber Deterrence and Response Act, which establishes a framework for deterring and responding to state-sponsored malicious cyber activity against this country.

Consistent with the State Department's recommendation to the President on deterrence in cyberspace, this bill will ensure swift, powerful, and transparent consequences against bad actors online.

Specifically, this bill requires the President to designate as a critical cyber threat actor each foreign person or each foreign agency of a foreign state that the President determines is responsible for state-sponsored cyber activities that pose a significant threat to the national security, foreign policy, economic health, or financial stability of the United States. In effect, this would codify America's longstanding unofficial policy of naming and shaming bad actors in cyberspace.

Further, this bill would require the President to impose sanctions from a menu of options against any critical cyber threat actor.

Finally, the bill calls on the President to coordinate designations and sanctions with our allies and partners to maximize their effectiveness. The Secretary of State is to lead an international diplomatic initiative to deter state-sponsored cyber activities and promote mutual support to our allies and partners to respond to malicious cyber incidents.

This legislation will put countries like Iran, North Korea, and Russia on notice that the United States is prepared to impose tough consequences for cyber attacks.

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

HOUSE OF REPRESENTATIVES,
COMMITTEE ON FINANCIAL SERVICES,
Washington, DC, July 20, 2018.

Hon. ED ROYCE,
Chairman, Committee on Foreign Affairs, Washington, DC.

DEAR CHAIRMAN ROYCE: I am writing concerning H.R. 5576, the Cyber Deterrence and Response Act of 2018.

As a result of your having consulted with the Committee on Financial Services concerning provisions in the bill that fall within our Rule X jurisdiction, I agree to forgo action on the bill so that it may proceed expeditiously to the House Floor. The Committee

on Financial Services takes this action with our mutual understanding that, by foregoing consideration of H.R. 5576, at this time, we do not waive any jurisdiction over the subject matter contained in this or similar legislation, and that our Committee will be appropriately consulted and involved as this or similar legislation moves forward so that we may address any remaining issues that fall within our Rule X jurisdiction. Our Committee also reserves the right to seek appointment of an appropriate number of conferees to any House-Senate conference involving this or similar legislation, and requests your support for any such request.

Finally, I would appreciate your response to this letter confirming this understanding with respect to H.R. 5576 and would ask that a copy of our exchange of letters on this matter be included in the Congressional Record during floor consideration thereof.

Sincerely,

JEB HENSARLING,
Chairman.

HOUSE OF REPRESENTATIVES,
COMMITTEE ON FOREIGN AFFAIRS,
Washington, DC, July 20, 2018.

Hon. JEB HENSARLING,
Chairman, Committee on Financial Services, Washington, DC.

DEAR CHAIRMAN HENSARLING: Thank you for consulting with the Foreign Affairs Committee and agreeing to be discharged from further consideration of H.R. 5576, the Cyber Deterrence and Response Act of 2018, so that the bill may proceed expeditiously to the House floor.

I agree that your forgoing further action on this measure does not in any way diminish or alter the jurisdiction of your committee, or prejudice its jurisdictional prerogatives on this resolution or similar legislation in the future. I would support your effort to seek appointment of an appropriate number of conferees from your committee to any House-Senate conference on this legislation.

I will seek to place our letters on H.R. 5576 into the Congressional Record during floor consideration of the bill. I appreciate your cooperation regarding this legislation and look forward to continuing to work together as this measure moves through the legislative process.

Sincerely,

EDWARD R. ROYCE,
Chairman.

HOUSE OF REPRESENTATIVES, COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, DC, July 20, 2018.

Hon. EDWARD R. ROYCE,
Chairman, Committee on Foreign Affairs, House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: Thank you for your letter regarding H.R. 5576, the Cyber Deterrence and Response Act of 2018. As you know, certain provisions of the bill fall within the jurisdiction of Committee on Oversight and Government Reform.

Based on your consultation with the Committee on Oversight and Government Reform and so the bill may proceed expeditiously to the House Floor, I agree to discharging the Committee on Oversight and Government Reform from further consideration of H.R. 5576. I agree that forgoing formal consideration of the bill will not prejudice the Committee on Oversight and Government Reform with respect to any future jurisdictional claim, and I appreciate your agreement to support appointment of members of the Committee on Oversight and Government Reform as conferees in any House-Senate conference on this or related legislation. In addition, I request the Committee be consulted and involved as the bill or similar legislation moves forward so we may address any remaining issues within our jurisdiction.

Finally, I request you include your letter and this response in the bill report filed by the Committee on Foreign Affairs, as well as in the Congressional Record during consideration of the bill on the floor.

Sincerely,

TREY GOWDY.

HOUSE OF REPRESENTATIVES,
COMMITTEE ON FOREIGN AFFAIRS,
Washington, DC, July 20, 2018.

Hon. TREY GOWDY,
Chairman, Committee on Oversight and Government Reform, Washington, DC.

DEAR CHAIRMAN GOWDY: Thank you for consulting with the Foreign Affairs Committee and agreeing to be discharged from further consideration of H.R. 5576, the Cyber Deterrence and Response Act of 2018, so that the bill may proceed expeditiously to the House floor.

I agree that your forgoing further action on this measure does not in any way diminish or alter the jurisdiction of your committee, or prejudice its jurisdictional prerogatives on this resolution or similar legislation in the future. I would support your effort to seek appointment of an appropriate number of conferees from your committee to any House-Senate conference on this legislation.

I will seek to place our letters on H.R. 5576 into the Congressional Record during floor consideration of the bill. I appreciate your cooperation regarding this legislation and look forward to continuing to work together as it moves through the legislative process.

Sincerely,

EDWARD R. ROYCE,
Chairman.

HOUSE OF REPRESENTATIVES,
COMMITTEE ON FOREIGN AFFAIRS,
Washington, DC, July 20, 2018.

Hon. BOB GOODLATTE,
Chairman, Committee on the Judiciary, Washington, DC.

DEAR CHAIRMAN GOODLATTE: Thank you for consulting with the Foreign Affairs Committee and agreeing to be discharged from further consideration of H.R. 5576, the Cyber Deterrence and Response Act of 2018, so that the bill may proceed expeditiously to the House floor.

I agree that your forgoing further action on this measure does not in any way diminish or alter the jurisdiction of your committee, or prejudice its jurisdictional prerogatives on this bill or similar legislation in the future. I would support your effort to seek appointment of an appropriate number of conferees from your committee to any House-Senate conference on this legislation.

I will seek to place our letters on this measure into the Congressional Record during floor consideration of the bill. I appreciate your cooperation regarding this legislation and look forward to continuing to work together as it moves through the legislative process.

Sincerely,

EDWARD R. ROYCE,
Chairman.

□ 1400

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

Mr. Speaker, I rise in strong support of H.R. 5576, the Cyber Deterrence and Response Act of 2018. I am proud to be an original cosponsor of this legislation authored by Congressman YOHO, who did great work with this bill, along with Chairman ROYCE and other members of our committee.

Mr. Speaker, every day, America faces cyber threats from around the world. Countries, including Russia, China, Iran, and North Korea, have attacked our companies, our infrastructure, our government, and even the very heart of our democracy, our elections.

The Cyber Deterrence and Response Act is a step in responding to these threats. This bill requires the President to impose sanctions on those who participate in a state-sponsored cyber attack against the United States.

These far-reaching sanctions could be targeted to individuals, entities, and states themselves that perpetrate these attacks. These include attacks against critical infrastructure, public and private computer networks, and any sector that would jeopardize America's national security, foreign policy, economic health, or financial stability.

This is a bipartisan, good bill, and I urge all Members to support it. But let me be clear: This bill does not do nearly enough to respond to Putin's attack on our democracy. We must continue to do this, but this is an important step and a very good step, and is indicative of the bipartisan cooperation that we have in the Foreign Affairs Committee, which is very, very important when we are dealing with foreign affairs.

Our adversaries need to know that we are united, and that is what a bill like this does. So I congratulate Mr. YOHO for his hard work on this bill. It is a welcome effort to enhance our response to cyber attacks, but it is a Band-Aid on a bullet wound, if we don't do anything else.

We need to keep doing these kinds of things. Those countries that would wish us ill, we have to let them know that we are not going to just stand idly by and be a target.

In 2016, our Nation was attacked. The very core of our democratic process was hit by Russian cyber forces, and our government has been woefully negligent to adequately respond.

I thank Republican leadership for bringing this bill forward, but we really need to address the critical issue of our vulnerability to these cyber attacks. If we do that, they will bring forward one of the many other stronger bills on this matter as well, for example, my bill that I introduced with Mr. CONNOLLY, the SECURE Our Democracy Act; or the Secure America from Russian Interference Act, which includes my bill; and more than a dozen others. These bills constitute a strong, decisive response that matches the gravity of the threat we face.

These bills would require the President to impose sanctions on those who attacked our elections in 2016 and would do much, much more to shore up our election system. For over a year, I have been pushing and pleading that the bill moves forward. I hope it will move forward as well.

We need to go on record now and say whether we will do everything in our power to stop another attack on American democracy, or whether we will

just step to the side with rhetoric and let it happen again. That is, again, why I am so happy to support this bill, because it shows that we are working together.

But the point I want to make in collaboration with that is that we still have much more work to do. I know the committee, in a couple of weeks, is going to hold a very important hearing on Russia, and I think it is very important that we do that.

Mr. Speaker, I again urge my colleagues to support this very good piece of legislation, and I reserve the balance of my time.

Mr. ROYCE of California. Mr. Speaker, I yield 4 minutes to the gentleman from Florida (Mr. YOHO), the chairman of the Foreign Affairs Subcommittee on Asia and the Pacific, and the author of this bill.

Mr. YOHO. Mr. Speaker, I rise in support of H.R. 5576, the Cyber Deterrence and Response Act. I thank Chairman ROYCE and Ranking Member ENGEL and his staff for helping usher this bill through the Foreign Affairs Committee.

The threats of cyber attacks on our country and the American people are growing in their sophistication and frequency by the minute. Targeted attacks against the Federal Government, private businesses, and individual Americans continue to pose escalating threats to our Nation.

Foreign adversaries like Iran, North Korea, Russia, and China have developed sophisticated cyber capabilities that can disrupt our networks, threaten our critical infrastructure, harm our economy, and undermine our elections.

As Members of Congress, we must work to deter and respond to these state-sponsored cyber attacks against the United States.

This is why I stand here today to urge support for H.R. 5576, the Cyber Deterrence and Response Act. This legislation codifies and enhances the substance of the cyber executive orders that are currently the foundation of the United States cyber policy.

This bill will enhance cybersecurity by defining state-sponsored attacks and establishing strong penalties for would-be attackers. It will deter bad players from attacking the U.S. Government and our businesses.

H.R. 5576 establishes a three-step process for the U.S. strategy to respond to cyber threats.

The first step will require the President to identify and designate individuals and groups who are responsible for and are complicit in state-sponsored cyber attacks as critical cyber threat actors.

This name-and-shame tactic will expose current hackers and deter future threats, making U.S. sanctions more consistent with other successful sanction procedures, like the SDN, which is a Specially Designated National list. The administration would then be tasked with imposing appropriate actions and sanctions on the designated actors.

A third step would include imposing additional sanctions against the foreign governments that are behind these attacks. In this way, like our State Sponsors of Terrorism list and the Trafficking in Persons watch list, my legislation goes to the governments that are at the root of the threat, not stopping at the agents that carry out the attacks.

As chairman of the House Foreign Affairs Subcommittee on Asia and the Pacific, I understand the importance of protecting our Nation from malicious cyber attackers. Some of the worst offenders fall inside my jurisdiction. It is vital that we improve our ability to thwart these potential devastating cyber attacks.

Understand this: An attack on just one government agency or any individual business is an attack on all Americans. To adequately protect our national security from advancing threats, we must put politics aside and put our country first.

The Cyber Deterrence and Response Act will do just that, and I encourage all my colleagues to support this bill.

Mr. ENGEL. Mr. Speaker, I yield 3 minutes to the gentleman from Rhode Island (Mr. LANGEVIN), an original cosponsor of this legislation and a strong leader on cyber policy in Congress.

Mr. LANGEVIN. Mr. Speaker, I thank the gentleman for yielding, and I would like to begin by thanking my colleague, the gentleman from Florida (Mr. YOHO), for his leadership on this very important issue. I am very proud to have helped shape this strong bill, and I appreciate the gentleman's bipartisan collaboration.

Mr. Speaker, the international community has reached consensus on many norms of responsible state behavior in cyberspace. One key agreement reached by the joint 2015 Group of Governmental Experts is that responsible states do not use cyber means to damage or impair the operation of critical infrastructure that provides services to the public. Yet states regularly flaunt these international rules of the road.

The North Koreans spread the WannaCry pseudo-ransomware last May. The Russians have targeted the electric grid in Ukraine and were behind NotPetya, the most devastating cyber incident in history. Closest to home, Russia launched an assault on our elections with the goal of undermining citizens' faith in our democracy.

President Obama recognized that protecting the Nation's cyberspace has three components: improving our defenses to prevent hackers from getting in; increasing resilience to minimize the damage when they do get in; and imposing costs on states that act against our national interest.

His executive orders, particularly 13694 and 13757, focused on this last point, holding nations accountable through sanctions when they or their agents target our critical infrastructure. Mr. YOHO's bill codifies large portions of these executive orders, and it goes further by requiring the President to both designate critical cyber threats and to sanction them.

I strongly support the underlying policy and the enhancements made by my friend from Florida.

Mr. Speaker, I think we also need to go further. The September 2015 Obama-Xi accord on Chinese economic espionage, which remains one of the most successful examples of cyber deterrence, relied on the threat of sanctions targeting the beneficiaries of China's spying, not just PLA members. We must continue to work together in a bipartisan fashion to maximize the efficacy of sanctions, which are intended not to punish but to shape behavior.

Most importantly, though, I hope the President takes more aggressive actions to protect American interests in cyberspace. I criticized President Obama's response to Russia's election interference as too little, too late, and, unfortunately, President Trump has been reticent to act against Russia.

The norms we talk about are norms of behavior, and I remain deeply concerned that our absence of action in response to malign state activity is developing into a norm in and of itself. Actions, as they say, speak louder than words.

However, all told, Mr. Speaker, this bill is an important first step in recognizing that cyber threats are the new weapon of choice for states that seek to sow discord and engage in conflict below the level of the threshold of war.

I again thank Congressman YOHO for introducing the bill and Chairman ROYCE and Ranking Member ENGEL for supporting it. I strongly support H.R. 5576, and I urge my colleagues to do the same.

Mr. ROYCE of California. Mr. Speaker, I yield 2 minutes to the gentleman from Pennsylvania (Mr. FITZPATRICK). He is a member of the Committee on Foreign Affairs. He is a cosponsor of this legislation. He has formerly worked for the FBI on cyber issues, and we very much appreciate his expertise in this area.

Mr. FITZPATRICK. Mr. Speaker, I rise today in strong support of H.R. 5576, the Cyber Deterrence and Response Act of 2018.

Mr. Speaker, our adversaries continually engage in sophisticated cyber attacks designed to disrupt our critical infrastructure, harm our economy, and undermine our elections. As has been said time and time again, our Nation's electoral process is sacred, and it must be protected at all costs from interference from all hostile foreign actors.

In February, the Director of National Intelligence stated that Russia, China, Iran, and North Korea will pose the greatest cyber threats to the United States during the course of the next year.

We have seen continued hostility from state actors like Russia to undermine our democratic institutions and

trigger instability in Europe by weakening key partners like Ukraine and Georgia.

Mr. Speaker, I saw this firsthand during my time as an FBI agent working both here domestically and overseas. We must make it clear to these hostile states that they will face harsh consequences for their cyber attacks.

That is exactly what this bipartisan bill accomplishes. The Cyber Deterrence and Response Act establishes a clear framework to deter and respond to state-sponsored cyber threats. It provides harsh sanctions through suspension of developmental assistance and credit allotment to nations engaged in malicious state-sponsored cyber activities against our United States.

We must hold these foreign actors accountable while strengthening the integrity of our intelligence community. I commend my colleague from Florida (Mr. YOHO) for introducing this bill, along with Chairman ROYCE and Ranking Member ENGEL for bringing this vital matter to the floor. I urge my colleagues, Democrat and Republican alike, to support this critical legislation that is necessary to protect our national security.

Mr. ENGEL. Mr. Speaker, I reserve the balance of my time to close.

Mr. ROYCE of California. Mr. Speaker, I yield 2 minutes to the gentleman from Utah (Mr. CURTIS). He is a member of the Committee on Foreign Affairs and a cosponsor of this legislation as well.

Mr. CURTIS. Mr. Speaker, I am pleased to join my friend and colleague, Mr. YOHO, on the floor today with others to speak in support of this bipartisan bill, H.R. 5576, the Cyber Deterrence and Response Act. I would also like to give a special thanks to Foreign Affairs Committee Chairman ROYCE and Ranking Member ENGEL for their support of the bill and moving it through the committee process.

Mr. Speaker, more than 30 nations are currently developing offensive cyber attack capabilities. Earlier this year, the Director of National Intelligence testified before Congress that Russia, China, Iran, and North Korea posed the greatest cyber threats to the United States. He continued and said work to use cyber operations to achieve strategic objectives will continue ''unless they face clear repercussions for their cyber operations.''

This bill puts in place those clear repercussions for nations that have and seek to continue to use cyber attacks against the U.S. Specifically, the legislation authorizes the President, acting through the Secretary of State, to designate, where appropriate, foreign persons or agencies as critical cyber threats.

The bill also authorizes both travel and financial sanctions of individuals and agencies designated as critical cyber threats, and the legislation requires Congress to be briefed periodically on state-sponsored cyber activities against the United States.

This bill will help us better protect America's critical infrastructure, national security, healthcare, energy, financial, transportation, and communication systems from hostile state-sponsored cyber attacks.

Additionally, the legislation is important to help us better protect American companies and manufacturers from hackers and cyber intruders.

□ 1415

And maybe most importantly, H.R. 5576 will provide more tools for the U.S. to deter state-sponsored efforts to attack our democratic institutions and electoral systems.

I urge my colleagues to support me in voting in support of the Cyber Deterrence and Response Act of 2018.

Mr. ENGEL. Mr. Speaker, I am prepared to close. I yield myself such time as I may consume.

In closing, I urge all my colleagues once again to support this measure. The scope of the cyber threat that we are facing is immense. This is a good bill, and moves us in the right direction, and I urge all our colleagues to support it.

I want to thank Chairman ROYCE. As usual, I want to thank Chairman ROYCE and Congressman YOHO for their friendship and their hard work on this critical issue.

I yield back the balance of my time.

Mr. ROYCE of California. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, in closing, I would really like to thank our colleagues here, especially Representative TED YOHO, the chairman of the Subcommittee on Asia and the Pacific, and the ranking member of the Foreign Affairs Committee, Mr. ELIOT ENGEL of New York.

I also want to thank the Financial Services Committee that worked with us on this legislation. We want to thank, in addition, the Judiciary Committee. We had the Oversight and Government Reform Committee that worked with us as well in support of this bill.

I think, as Mr. YOHO would share with you, the bill is truly a bipartisan endeavor that has been improved by contributions from multiple committees, government agencies, and the business community. And with the passage of this bill, Congress sends a strong message to our adversaries, that cyberattacks against the United States and against our allies will not be tolerated.

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 California (Mr. ROYCE) that the House suspend the rules and pass the bill, H.R. 5576, 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.

GLOBAL ELECTORAL EXCHANGE ACT

Mr. ROYCE of California. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 5274) to promote international exchanges on best election practices, cultivate more secure democratic institutions around the world, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 5274

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 ''Global Electoral Exchange Act''.

SEC. 2. SENSE OF CONGRESS.

It is the sense of Congress that—

(1) recent elections globally have illustrated the urgent need for the promotion and exchange of international best election practices, particularly in the areas of cybersecurity, results transmission, transparency of electoral data, election dispute resolution, and the elimination of discriminatory registration practices and other electoral irregularities;

(2) the advancement of democracy worldwide promotes American interests, as stable democracies provide new market opportunities, improve global health outcomes, and promote economic freedom and regional security;

(3) credible elections are the cornerstone of a healthy democracy and enable all persons to exercise their basic human right to have a say in how they are governed;

(4) inclusive elections strengthen the credibility and stability of democracies more broadly, as democratic institutions flourish when representative of all groups of society;

(5) at the heart of a strong election cycle is the professionalism of the election management body and an empowered civil society; and

(6) the development of local expertise via peer-to-peer learning and exchanges promotes the independence of such bodies from internal and external influence.

SEC. 3. GLOBAL ELECTORAL EXCHANGE.

(a) GLOBAL ELECTORAL EXCHANGE.—The Secretary of State is authorized to establish and administer a Global Electoral Exchange Program to promote the utilization of sound election administration practices around the world.

(b) PURPOSE.—The purpose of the Global Electoral Exchange Program described in subsection (a) shall include the promotion and exchange of international best election practices, including in the areas of—

(1) cybersecurity;

(2) results transmission;

(3) transparency of electoral data;

(4) election dispute resolution;

(5) the elimination of discriminatory registration practices and electoral irregularities;

(6) equitable access to polling places, voter education information, and voting mechanisms (including by persons with disabilities); and

(7) other sound election administration practices.

(c) EXCHANGE OF ELECTORAL AUTHORITIES.—

(1) IN GENERAL.—The Secretary of State may, in consultation, as appropriate, with the United States Agency for International Development, make grants to any United States-based organization described in section 501(c)(3) of the Internal Revenue Code of