Ms. JOHNSON of Texas. Mr. Speaker, I yield myself the balance of my time.

I simply urge the passage of H.R. 335, and I thank all the staff, as well, for the bipartisan support of this bill.

I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentlewoman from Texas (Ms. JOHNSON) that the House suspend the rules and pass the bill, H.R. 335, 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.

CYBERSECURITY VULNERABILITY REMEDIATION ACT

Ms. JACKSON LEE. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 3710) to amend the Homeland Security Act of 2002 to provide for the remediation of cybersecurity vulnerabilities, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 3710

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 ''Cybersecurity Vulnerability Remediation Act''.

SEC. 2. CYBERSECURITY VULNERABILITIES.

Section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659) is amended—

(1) in subsection (a)—

(A) in paragraph (5), by striking ''and'' after the semicolon at the end;

(B) by redesignating paragraph (6) as paragraph (7); and

(C) by inserting after paragraph (5) the following new paragraph:

''(6) the term 'cybersecurity vulnerability' has the meaning given the term 'security vulnerability' in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501); and''.

(2) in subsection (c)—

(A) in paragraph (5)—

(i) in subparagraph (A), by striking ''and'' after the semicolon at the end;

(ii) by redesignating subparagraph (B) as subparagraph (C);

(iii) by inserting after subparagraph (A) the following new subparagraph:

''(B) sharing mitigation protocols to counter cybersecurity vulnerabilities pursuant to subsection (n); and''; and

(iv) in subparagraph (C), as so redesignated, by inserting ''and mitigation protocols to counter cybersecurity vulnerabilities in accordance with subparagraph (B)'' before ''with Federal'';

(B) in paragraph (7)(C), by striking ''sharing'' and inserting ''share''; and

(C) in paragraph (9), by inserting ''mitigation protocols to counter cybersecurity vulnerabilities,'' after ''measures,'';

(3) in subsection (e)(1)(G), by striking the semicolon after ''and'' at the end; and

(4) by adding at the end the following new subsection:

''(n) PROTOCOLS TO COUNTER CYBERSECURITY VULNERABILITIES.—The Director may, as appropriate, identify, develop, and disseminate actionable protocols to mitigate cybersecurity vulnerabilities, including in circumstances in which such vulnerabilities exist because software or hardware is no longer supported by a vendor.''.

SEC. 3. REPORT ON CYBERSECURITY VULNERABILITIES.

(a) REPORT.—Not later than one year after the date of the enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on how the Agency carries out subsection (m) of section 2209 of the Homeland Security Act of 2002 to coordinate vulnerability disclosures, including disclosures of cybersecurity vulnerabilities (as such term is defined in such section), and subsection (n) of such section (as added by section 2) to disseminate actionable protocols to mitigate cybersecurity vulnerabilities, that includes the following:

(1) A description of the policies and procedures relating to the coordination of vulnerability disclosures.

(2) A description of the levels of activity in furtherance of such subsections (m) and (n) of such section 2209.

(3) Any plans to make further improvements to how information provided pursuant to such subsections can be shared (as such term is defined in such section 2209) between the Department and industry and other stakeholders.

(4) Any available information on the degree to which such information was acted upon by industry and other stakeholders.

(5) A description of how privacy and civil liberties are preserved in the collection, retention, use, and sharing of vulnerability disclosures.

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

SEC. 4. COMPETITION RELATING TO CYBERSECURITY VULNERABILITIES.

The Under Secretary for Science and Technology of the Department of Homeland Security, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency of the Department, may establish an incentive-based program that allows industry, individuals, academia, and others to compete in providing remediation solutions for cybersecurity vulnerabilities (as such term is defined in section 2209 of the Homeland Security Act of 2002, as amended by section 2).

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

The Chair recognizes the gentlewoman from Texas.

GENERAL LEAVE

Ms. JACKSON LEE. 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 Texas?

There was no objection.

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

Mr. Speaker, I rise today in support of H.R. 3710, the Cybersecurity Vulnerability Remediation Act, and I thank Chairman BENNIE THOMPSON for his work in securing the Nation against terrorist threats, including cybersecurity vulnerabilities that target critical infrastructure, civilian agency networks, and private-sector cyber resources.

I also thank subcommittee Chairman RICHMOND and the Committee on Homeland Security staff for working with my staff and me on H.R. 3710.

I thank the ranking member of the full committee, Mr. ROGERS from Alabama, and the ranking member of the subcommittee.

Mr. Speaker, just a few weeks ago, we saw technology in the form of drones be utilized to attack, with explosives, refineries in Saudi Arabia. I think the basis of my legislation speaks to the point that it is crucial that this Congress and this Nation prepare itself for new forms of technology.

We have not had that incident here in the United States, but if we recall, in 9/11, no one could fathom using loaded airplanes, fully filled with the material, fuel, that could be utilized as a weapon to attack the World Trade Center, to kill the brave at the Pentagon and the brave in Pennsylvania.

H.R. 3710 is to speak to those vulnerabilities, in particular, cybersecurity vulnerability remediation, which directs the DHS to prioritize efforts to help network operators address known vulnerabilities.

It requires DHS' Cybersecurity and Infrastructure Security Agency to widely share mitigation protocols that counter cybersecurity vulnerabilities, authorizing the DHS Science and Technology Directorate to establish an incentive-based program to allow industry, individuals, agencies, and academia to compete in providing remediation solutions for the highest priority cybersecurity vulnerabilities.

We must be ever vigilant and diligent as we look to these new levels and subsets of technology. It requires the CISA to report to Congress on its efforts to share mitigation protocols and coordinate vulnerability disclosure with its partners.

H.R. 3710 authorizes, for the first time, the Cybersecurity and Infrastructure Security Agency to develop and distribute playbooks, in consultation with private-sector experts, to provide procedures and mitigation strategies for the most critical known vulnerabilities, especially those affecting software or hardware that is no longer supported by a vendor.

One of the statistics that we really know is that 80 percent—maybe even higher now—to 85 percent of the Nation's vulnerabilities—technology, infrastructure—is in the private sector. Those are the sites that our enemies would look eagerly to attack. The World Trade Center; in Saudi, the refineries; maybe some of our beautiful national monuments, outstanding sites here in Washington, D.C.; our national parks, these are the examples and the exhibits of the freedom of this Nation. Those are some government, some private sector.

Many know the terror that New York collectively faced, but there are other sites along the West Coast, in the Midwest, and in the Deep South that would also exhibit what the freedom of America is all about.

The playbooks that we would make available to Federal agencies, industry, and other stakeholders would help them prepare a network defense in the event of a cyberattack based upon vulnerability. I would like to think that we could prevent that attack.

A zero-day vulnerability is a software bug or exploit that has not been patched. Hackers can use these bugs and exploits based upon the vulnerability to steal data or damage networks before a patch can be developed to prevent a breach.

There are some vulnerabilities that cannot be patched. These require the resources provided by the playbook that will be provided in my bill.

H.R. 3710 authorizes the DHS Science and Technology Directorate, in consultation with CISA, to establish a competition program for industry, individuals, academia, and others to provide remediation solutions for cybersecurity vulnerabilities that are no longer supported.

The good news is that it seeks to have the consultation of Americans who have expertise and to be able to work with them to provide the remediation but also the playbook for prevention.

The vulnerabilities that will receive an entry in the playbook are serious and, if used by an adversary, can lead to significant costs and disruption of vital goods and services to the public. Just think of your water system, run mostly by local entities, or the electric grid, run mostly by the private sector.

In the 115th Congress, I introduced H.R. 3202, Cyber Vulnerability Disclosure Reporting Act, which addresses the Federal Government's sharing of cyber vulnerability disclosures to critical infrastructure owners and operators. H.R. 3710 goes further to address the remediation of identified cybersecurity threats by incentivizing work to patch or find solutions for cyber threats inherent in legacy systems.

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

I hope that we will see our way forward in getting proactive and preventative as we move toward new levels of technology.

Mr. Speaker I rise today to speak in favor of H.R. 3710, the "Cybersecurity Vulnerability Remediation Act."

I thank Chairman BENNIE G. THOMPSON for his work in securing the nation against terrorist threats, including cybersecurity vulnerabilities that target critical infrastructure, civilian agency networks, and private sector cyber resources.

I thank Subcommittee Chairman RICHMOND and the Homeland Security Committee staff for working with me and my staff on H.R. 3710.

H.R. 3710, the "Cybersecurity Vulnerability Remediation Act" directs DHS to prioritize efforts to help network operators address known vulnerabilities by:

1. Requiring DHS's Cybersecurity and Infrastructure Security Agency (CISA) to widely share mitigation protocols to counter cybersecurity vulnerabilities;

2. Authorizing the DHS Science and Technology Directorate to establish an incentive-based program to allow industry, individuals, agencies, and academia to compete in providing remediation solutions for the highest priority cybersecurity vulnerabilities; and

3. Requiring CISA to report to Congress on its efforts to share mitigation protocols and coordinate vulnerability disclosures with its partners.

H.R. 3710, authorizes for the first time the Cybersecurity and Infrastructure Agency (CISA) to develop and distribute "playbooks," in consultation with private sector experts, to provide procedures and mitigation strategies for the most critical, known vulnerabilities, especially those affecting software or hardware that is no longer supported by a vendor.

The playbooks would be available to Federal agencies, industry, and other stakeholders to help them prepare network defense in the event of a cyber-attack based upon a vulnerability.

A zero-day vulnerability is a software bug or exploit that has not been patched.

Hackers can use these bugs and exploits based upon the vulnerability to steal data or damage networks before a patch can be developed to prevent a breach.

There are some vulnerabilities that cannot be patched and these require the resources provided by the Playbook that will be provided by this bill.

H.R. 3710 authorizes DHS Science and Technology Directorate (S&T), in consultation with CISA, to establish a competition program for industry, individuals, academia, and others to provide remediation solutions for cybersecurity vulnerabilities that are no longer supported.

The vulnerabilities that will receive entry into the Playbook are serious and if used by an advisory, can lead to significant cost and disruption of vital goods and services to the public.

In the 115th Congress, I introduced H.R. 3202, Cyber Vulnerability Disclosure Reporting Act, which addresses the federal government's sharing of cyber vulnerability disclosures to critical infrastructure owners and operators.

H.R. 3710 goes further to address the remediation of identified cybersecurity threats by incentivizing work to patch or find solutions for cyber threats inherent in legacy systems.

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

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

Most people do not know how long the federal government has used computing to carry out vital functions in service of the public.

The Federal government's first use of computing technology occurred in 1890 when an automated tabulation method was used to organize that year's census data encoded on punch cards.

Since that modest beginning in 1890, the Federal government has blazed a path for adoption of computing technology throughout the federal government, which established an unprecedented pace for innovation in the private sector that transformed our world from analogue to digital in 129 years.

One of the consequences of federal government's use of computing technology over the last 129 years are the challenges of operating legacy systems that use outdated software, which cannot be quickly upgraded to eliminate known cybersecurity vulnerabilities.

Federal government offices are vulnerable to cyberattacks, with the number of cyber incidents reported by federal agencies increasing more than 1,300 percent between 2006 and 2015.

In 2015, a hacker exploited access provided by a government agency contractor to break into government databases to gain access to 22 million security clearance files from the Office of Personnel Management.

In 2017, Federal agencies reported more than 35,000 cyber incidents, some of which targeted old operating systems that were no longer supported by a vendor.

According to the National Security Agency, it has not responded to a zero-day attack on government systems in the last four years, largely because hackers have found better success through basic attack methods.

H.R. 3710 will provide much needed structure around a federal government wide effort to address cybersecurity vulnerabilities in federal civilian agency networks.

I ask my colleagues to join me in voting for H.R. 3710.

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

□ 1345

Mr. GREEN of Tennessee. Mr. Speaker, I yield myself such time as I may consume.

I rise today in support of H.R. 3710, the Cybersecurity Vulnerability Remediation Act. This bill enables CISA to develop important mitigation protocols for vulnerabilities existing in outdated software and hardware through collaboration with public- and private-sector entities.

This important legislation, introduced by Ms. JACKSON LEE of Texas, helps ensure that we maintain security in our networks.

I support this legislation, and I urge my colleagues to join me in doing so.

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

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

Mr. Speaker, let me further explain what this bill does.

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

Most people do not know how long the Federal Government has used computing to carry out vital functions in service of the public. The Federal Government's first use of computing technology occurred as long ago as 1890,

when an automated tabulation method was used to organize that year's Census data encoded on punch cards.

Let me remind our colleagues that we are about to venture on to Census now. Imagine a cyberattack on that process.

Since a modest beginning in 1890, the Federal Government has blazed a path for adoption of computing technology throughout the Federal Government, which established an unprecedented pace for innovation in the private sector that transformed our world from analog to digital in 129 years.

One of the consequences of the Federal Government's use of computing technology over the last 129 years is the challenges of operating legacy systems that use outdated software, which cannot be quickly upgraded to eliminate known cybersecurity vulnerabilities.

Federal Government offices are vulnerable to cyberattacks, with the number of cyber incidents reported by Federal agencies increasing more than 1,300 percent between 2006 and 2015.

In 2015, a hacker exploited access by a government agency contractor to break into the government databases to gain access to 22 million security clearance files from the Office of Personnel Management.

In 2017, Federal agencies reported more than 35,000 cyber incidents, some of which targeted old operating systems that were no longer supported by a vendor.

According to the National Security Agency, it has not responded to a zero-day attack on government systems in the last 4 years because hackers have found better success through basic attack methods.

I would hope my colleagues would consider recognizing that we must be in front of these potential attacks and not behind them.

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

Mr. GREEN of Tennessee. Mr. Speaker, I urge adoption to the bill, and I yield back the balance of my time.

Ms. JACKSON LEE. Mr. Speaker, I want to thank the minority for its support of this legislation and ask my colleagues to support it.

As I do so, Mr. Speaker, I include in the RECORD an article, ''DHS Flags Cybersecurity Vulnerabilities in Philips Patient Monitors: The Department of Homeland Security has issued an advisory about cybersecurity vulnerabilities in the wireless local area network modules of Philips IntelliVue portable patient monitors.''

[Sept. 13, 2019]

DHS FLAGS CYBERSECURITY VULNERABILITIES IN PHILIPS PATIENT MONITORS

THE DEPARTMENT OF HOMELAND SECURITY HAS ISSUED AN ADVISORY ABOUT CYBERSECURITY VULNERABILITIES IN THE WIRELESS LOCAL AREA NETWORK MODULES OF PHILIPS INTELLIVUE PORTABLE PATIENT MONITORS

(By Fred Donovan)

The Department of Homeland Security has issued (https://www.us-cert.gov/ics/advisories/icsma-19-255-01) an advisory about cybersecurity vulnerabilities in the wireless local area network (WLAN) modules of certain Philips IntelliVue portable patient monitors.

DHS's Industrial Control Systems Cyber Emergency Response Team (ICS–CERT) warned that an attacker could corrupt the IntelliVue WLAN firmware and alter the data flow over to the patient monitor, causing an inoperative condition alert at the device and central station.

The vulnerable patient monitors are IntelliVue MP monitors MP20–MP90, MP5/5SC, MP2/X2, and MX800/700/600.

The vulnerabilities include use of hard-coded password and download of code without integrity check.

The use of a hard-coded password makes it easier for an attacker to guess the password and login via FTP and upload malicious firmware. In addition, the ''product downloads source code or an executable from a remote location and executes the code without sufficiently verifying the origin and integrity of the code,'' warned the advisory.

Shawn Loveric of Finite State reported the vulnerabilities to Philips.

In a product security advisory (https://www.usa.philips.com/healthcare/about/customer-support/product-security), Philips recommended that users of the affected IntelliVue patient monitors update to the WLAN Module Version C wireless module with current firmware.

Philips said it will also issue a software patch for WLAN Version A that will be available by the end of 2019, while WLAN Version B is obsolete.

''Wireless network access should be controlled by authentication and authorization (e.g. WPA2), which are supported by Philips. Additional mitigations include implementing a firewall rule on the customer wireless network, and further controls on physical access to the system,'' Philips advised.

Philips said it had received no reports of patient harm. Its analysis judged that it is unlikely that the cybersecurity vulnerability would impact clinical use, due to mitigating controls in place. To date, Philips has received no complaints involving clinical use that it has been able to associate with the vulnerability or evidence of patient identifiers compromised.

DHS's Cybersecurity and Infrastructure Security Agency recommended users of the vulnerable Philips devices take defensive measures to minimize the risk of exploitation of these vulnerabilities. Users should restrict system access to authorized personnel and follow a least privilege approach, apply defense-in-depth strategies, and disable unnecessary accounts and services.

Ms. JACKSON LEE. With that in mind, this is a real-life example of what can happen if we are not first in front.

Mr. Speaker, I hope that my colleagues will join me in voting for H.R. 3710, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentlewoman from Texas (Ms. JACKSON LEE) that the House suspend the rules and pass the bill, H.R. 3710.

The question was taken; and (two-thirds being in the affirmative) the rules were suspended and the bill was passed.

A motion to reconsider was laid on the table.

UNIFYING DHS INTELLIGENCE ENTERPRISE ACT

Ms. JACKSON LEE. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 2589) to amend the Homeland Security Act of 2002 to establish a homeland intelligence doctrine for the Department of Homeland Security, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 2589

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 ''Unifying DHS Intelligence Enterprise Act''.

SEC. 2. HOMELAND INTELLIGENCE DOCTRINE.

(a) IN GENERAL.—Subtitle A of title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.) is amended by adding at the end the following new section:

''SEC. 210H. HOMELAND INTELLIGENCE DOCTRINE.

''(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this section, the Secretary, acting through the Chief Intelligence Officer of the Department, in coordination with intelligence components of the Department, the Office of the General Counsel, the Privacy Office, and the Office for Civil Rights and Civil Liberties, shall develop and disseminate written Department-wide guidance for the processing, analysis, production, and dissemination of homeland security information (as such term is defined in section 892) and terrorism information (as such term is defined in section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485)).

''(b) CONTENTS.—The guidance required under subsection (a) shall, at a minimum, include the following:

''(1) A description of guiding principles and purposes of the Department's intelligence enterprise.

''(2) A summary of the roles, responsibilities, and programs of each intelligence component of the Department in the processing, analysis, production, or dissemination of homeland security information and terrorism information, including relevant authorities and restrictions applicable to each such intelligence component.

''(3) Guidance for the processing, analysis, and production of such information.

''(4) Guidance for the dissemination of such information, including within the Department, among and between Federal departments and agencies, among and between State, local, Tribal, and territorial governments, including law enforcement, and with foreign partners and the private sector, consistent with the protection of privacy, civil rights, and civil liberties.

''(5) A description of how the dissemination to the intelligence community (as such term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4))) and Federal law enforcement of such information assists such entities in carrying out their respective missions.

''(c) FORM.—The guidance required under subsection (a) shall be submitted in unclassified form, but may include a classified annex.

''(d) ANNUAL REVIEW.—For each of the five fiscal years beginning with the first fiscal year that begins after the date of the enactment of this section, the Secretary shall conduct a review of the guidance required under subsection (a) and, as appropriate, revise such guidance.''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting