of S. 2030 are not intended to delay the change to the 190-watt limiter requirement.

Mr. Speaker, I believe ceiling fan lighting kit manufacturers have acted in good faith in the run-up to the change in the standard and that they should not be penalized for producing light kits without the 190-watt limiting device.

In my view, DOE should take whatever steps are necessary to revise its rules to allow these otherwise compliant kits to be sold and should take no enforcement actions against manufacturers solely because a kit fails to include the 190-watt limiting device.

That doesn't mean the Department should stop all enforcement to ensure compliance with standards for these kits, but it should specifically forgo action against companies for failing to include a limiting device.

Mr. Speaker, I ask if the chairman shares my view.

Mr. UPTON. Will the gentleman yield?

Mr. MCNERNEY. I yield to the gentleman from Michigan.

Mr. UPTON. Mr. Speaker, I thank the gentleman for yielding.

Yes, I do share that view. This bill directs the Secretary of Energy to make technical and conforming changes to any implementing regulation so as to carry out the provisions in this bill.

In carrying out this requirement, DOE should make clear to the regulated community that the specific inclusion of a watt-limiting device is no longer needed for a kit to be deemed to meet the 190-watt-or-less consumption requirement.

I further want to associate myself with the gentleman's comments regarding enforcement. The Secretary should take whatever steps are necessary to ensure that no enforcement action is taken against any manufacturer solely because a kit fails to include the 190-watt limiting device.

To the extent he can, the Secretary should make clear in a public manner that DOE will not enforce against these manufacturers with regard to this particular matter so that no producer holds back their product for the market out of fear of violation.

Mr. MCNERNEY. Mr. Speaker, reclaiming my time, I want to thank the chairman for his indulgence in this important clarification of legislative intent.

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

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

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

Mr. Speaker, I again want to thank the chairman and commend my colleagues in both Chambers, specifically Mr. HUDSON and Mr. BUTTERFIELD, for working on this bill. The legislation enjoys support from both sides of the aisle on this committee; and, in fact, the House version of the bill, H.R. 3477, passed both the Energy Subcommittee and the full Energy and Commerce Committee by a voice vote with almost no debate. Similarly, the Senate companion, which is before us now, passed that body by unanimous consent. I hope that we can do the same today and swiftly send this to the President's desk for his signature.

Mr. Speaker, I urge my colleagues to join me in supporting the passage of S. 2030.

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 Michigan (Mr. UPTON) that the House suspend the rules and pass the bill, S. 2030.

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.

□ 1600

DHS CYBER INCIDENT RESPONSE TEAMS ACT OF 2018

Mr. MCCAUL. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 5074) to authorize cyber incident response teams at 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. 5074

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 ''DHS Cyber Incident Response Teams Act of 2018''.

SEC. 2. DEPARTMENT OF HOMELAND SECURITY CYBER INCIDENT RESPONSE TEAMS.

(a) IN GENERAL.—Section 227 of the Homeland Security Act of 2002 (6 U.S.C. 148) is amended—

(1) in subsection (d)(1)(B)(iv), by inserting '', including cybersecurity specialists'' after ''entities'';

(2) by redesignating subsections (f) through (m) as subsections (g) through (n), respectively; and

(3) by inserting after subsection (e) the following new subsection (f):

''(f) CYBER INCIDENT RESPONSE TEAMS.—

''(1) IN GENERAL.—The Center shall maintain cyber hunt and incident response teams for the purpose of providing, as appropriate and upon request, assistance, including the following:

''(A) Assistance to asset owners and operators in restoring services following a cyber incident.

''(B) The identification of cybersecurity risk and unauthorized cyber activity.

''(C) Mitigation strategies to prevent, deter, and protect against cybersecurity risks.

''(D) Recommendations to asset owners and operators for improving overall network and control systems security to lower cybersecurity risks, and other recommendations, as appropriate.

''(E) Such other capabilities as the Under Secretary appointed under section 103(a)(1)(H) determines appropriate.

''(2) CYBERSECURITY SPECIALISTS.—The Secretary may include cybersecurity specialists from the private sector on cyber hunt and incident response teams.

''(3) ASSOCIATED METRICS.—The Center shall continually assess and evaluate the cyber incident response teams and their operations using robust metrics.

''(4) SUBMITTAL OF INFORMATION TO CONGRESS.—Upon the conclusion of each of the first four fiscal years ending after the date of the enactment of this subsection, the Center shall submit to the Committee on Homeland Security of the House of Representatives and the Homeland Security and Governmental Affairs Committee of the Senate, information on the metrics used for evaluation and assessment of the cyber incident response teams and operations pursuant to paragraph (3), including the resources and staffing of such cyber incident response teams. Such information shall include each of the following for the period covered by the report:

''(A) The total number of incident response requests received.

''(B) The number of incident response tickets opened.

''(C) All interagency staffing of incident response teams.

''(D) The interagency collaborations established to support incident response teams.''; and

(4) in subsection (g), as redesignated by paragraph (2)—

(A) in paragraph (1), by inserting '', or any team or activity of the Center,'' after ''Center''; and

(B) in paragraph (2), by inserting '', or any team or activity of the Center,'' after ''Center''.

(b) NO ADDITIONAL FUNDS AUTHORIZED.—No additional funds are authorized to be appropriated to carry out the requirements of this Act and the amendments made by this Act. Such requirements shall be carried out using amounts otherwise authorized to be appropriated.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Texas (Mr. MCCAUL) and the gentleman from Mississippi (Mr. THOMPSON) each will control 20 minutes.

The Chair recognizes the gentleman from Texas.

GENERAL LEAVE

Mr. MCCAUL. Mr. Speaker, I ask unanimous consent that all Members have 5 legislative days within which to revise and extend their remarks and include any extraneous material on the bill under consideration.

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

There was no objection.

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

Mr. Speaker, I rise today in strong support of the DHS Cyber Incident Response Teams Act.

Before I discuss the bill, however, I would like to say a few words about the recent bombings in my hometown of Austin. In the past month, there have been a total of four bombings that have killed two people and injured four others. These are heinous, hateful acts on innocent Americans, and they will not be tolerated.

I know the people of Austin very well, and they will not be intimidated. I urge everyone back home to take caution and heed the warnings of local law enforcement. We will find whoever is responsible for these bombings and bring them to justice.

Mr. Speaker, I would like to now address the bill I have introduced and the threats confronting our cybersecurity.

As technology advances, more and more people are relying on their computers, iPads, and smartphones for both personal and professional use. In short, Mr. Speaker, everyone is a target.

But our enemies do not just attack individuals and their devices. They also put America's critical infrastructure sectors in their crosshairs, endangering all aspects of civilian life. These sectors include our financial services, healthcare systems, dams, and our energy production, among others. All of them play a vital role in making America work, and each one is vulnerable to an attack.

Last week, the FBI and DHS reported that Russian hackers had engineered a series of cyber attacks against American and European nuclear power plants and electric systems. Crippling or shutting down our power plants would have catastrophic effects.

We also know that Russia tried to undermine the credibility of our democratic system in the 2016 elections and are likely to try again in 2018. Strengthening our cyber election security needs to be a bipartisan priority.

Russia is not the only perpetrator of these kinds of attacks. Between 2011 and 2013, Iranian hackers attacked dozens of U.S. banks and even tried to shut down a dam in New York.

In 2015, we learned that Chinese hackers gained access to the private information of 80 million members and employees of Anthem healthcare. The Chinese also stole 22 million security clearances, including my own, from OPM. This attack allowed them to obtain highly sensitive personal data, including fingerprints and Social Security numbers. These continual onslaughts are part of a greater cyber war being carried out against the United States, even as I stand here and speak.

Unfortunately, it doesn't stop there. Our adversaries have weaponized technology and are using it to engage in espionage and to steal our intellectual property. This costs our economy hundreds of billions of dollars each year. In fact, former NSA Director, General Keith Alexander, described this theft as the ''greatest transfer of wealth in history.''

We must do more to stop these attacks. That is why I have prioritized the cybersecurity mission of DHS as chairman of the Homeland Security Committee. Through CISA, the previous bill which passed the House in December, we are elevating and making operational the Department's cybersecurity and infrastructure protection missions.

As part of the landmark DHS reauthorization, which passed the House in July, the Department will be required to provide volunteer assistance to State and local election officials upon request. These were important bipartisan steps, but we need to do more.

The legislation before us today codifies and enhances the cyber incident response times at DHS. These teams shall provide, upon request, assistance to asset owners and operators following cyber incidents, including with election infrastructure.

These teams may also include cybersecurity specialists from the private sector to provide outside expertise, which is a new, innovative breakthrough. By fostering this new collaboration between government and private sector, we can harness our talent and maximize our efforts to stay one step ahead of our enemies.

This innovative approach serves as a force multiplier to enhance our cybersecurity workforce. Being able to utilize a great number of experts will strengthen our efforts to protect our cyber networks. My bill provides DHS with that necessary capability.

The American people deserve to know that we are making every effort to strengthen our cybersecurity. This bill helps us achieve that goal, and I urge my colleagues to support it.

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

Mr. THOMPSON of Mississippi. Mr. Speaker, I yield myself such time as I may consume.

I rise in support of H.R. 5074, the DHS Cyber Incident Response Teams Act of 2018.

Mr. Speaker, at the outset, let me again support the chairman's comments about Austin, Texas. We talked a little bit about it last week in a hearing and, since that hearing, another incident has occurred. Terrorism, whether it is domestic or whatever, has no place in this country. I look forward to the capture of the person or persons who are committing these heinous acts in Austin, as well as providing whatever resources might go toward any future apprehensions.

Mr. Speaker, last week, the Department of Homeland Security issued a technical alert with the FBI on the Russian Government's efforts to use cyber tools to target our critical infrastructure—including our energy, water, aviation, and commercial facilities, critical infrastructure sectors.

DHS and the FBI released the alert amidst ongoing discussions about the urgent need to better secure our election infrastructure against Russian targeting and as the sophisticated cyber capabilities of Iran, North Korea, China, and nonstate actors continue to evolve. H.R. 5074, the DHS Cyber Incident Response Teams Act of 2018, would codify DHS' Hunt and Incident Response Teams into law.

The Department deploys Hunt and Incident Response Teams to owners and operators of critical infrastructure, upon request and free of charge after a cybersecurity incident. These DHS teams provide intrusion analysis, identify malicious actors, analyze malicious tools, and provide mitigation assistance strategies. They are DHS' ''boots on the ground'' in cyber incident response and, as such, play an integral role in improving the cybersecurity posture of critical infrastructure owners and operators.

I urge my colleagues to support this measure.

Mr. Speaker, the President's decision last week to finally issue sanctions in response to meddling in the 2016 election was long overdue. Though it was a positive move, I believe it will do little to deter the Russian Government from using cyber tools to target our critical infrastructure.

The Trump administration has yet to put any meaningful strategy in place to address ongoing efforts by the Russian Government—or any other bad actor, for that matter—to undermine the stability of the U.S. economy and government infrastructure in cyberspace. We must ensure that organizations have access to high-quality cyber incident response capabilities. H.R. 5074 would do just that, and I urge my colleagues to support it.

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

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

Mr. Speaker, this is a hugely important issue. I think cyber often gets overlooked when we look at kinetic threats of nuclear missiles coming out of North Korea, which is obviously a huge threat to the United States and its allies. But in cyberspace, we are at war, as well, with countries like Russia and China and Iran and North Korea, the Russian meddling in the elections. We can't sit idly by and let that happen again in 2018.

I think this is, as Mr. THOMPSON stated, a very bipartisan issue that we need to work together on against our foreign adversaries that every day are trying to undermine us, stealing intellectual property, espionage, or bringing down things in a cyber warfare attack. It is not the future of warfare; it is warfare here and now.

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

Ms. JACKSON LEE. Mr. Speaker, I rise in strong support of H.R. 5074, the DHS Cyber Incident Response Teams Act of 2018.

The ''DHS Cyber Incident Response Teams Act of 2018,'' codifies DHS' National Cybersecurity and Communications Coordination Center (NCCIC) hunt and incident response teams which the Department currently deploys to provide intrusion analysis, identify malicious actors, analyze malicious tools, and provide mitigation assistance to entities requesting assistance after a cybersecurity incident.

The DHS' Hunt and Incident Response Teams play an integral role in improving the cybersecurity posture of critical infrastructure owners and operators, from energy and nuclear power firms to state and local governments administering elections.

The bill requires the NCCIC to submit information to Congress regarding metrics for the teams, at the conclusion of the first four years after enactment.

In 2016, Russian actors targeted U.S. election infrastructure, hackers escalated efforts to

breach the domestic energy sector, and WannaCry and NotPetya ransomware wreaked havoc on public and private infrastructure around the world.

According to Symantec, a leading provider of cybersecurity solutions, said that ''The world of cyber espionage experienced a notable shift towards more overt activity, designed to destabilize and disrupt targeted organizations and countries.''

These threats to cyber security are not new.

In June 2015, it was reported that the Office of Personnel Management lost personal information on 21.5 million current and former federal employees and their families.

In 2017, the following were reported attacks and breaches:

WannaCry ransomware that infected millions of networks worldwide; and the

Equifax hack exposed millions of American's credit information to cyber-thieves;

Our nation's critical infrastructure and civilian government agencies depend on the cybersecurity talent and resources that the Department of Homeland Security can provide on the frontline to defend against attacks.

As cyber threats continue to evolve and become more sophisticated, so must U.S. efforts to confront them.

The Department of Homeland Security plays a central role in the federal government's cybersecurity apparatus and in coordinating federal efforts to secure critical infrastructure.

DHS is charged with coordinating agency efforts to secure the (dot).gov Domain, while also serving as the hub for cybersecurity information sharing between and among the private sector and federal government.

Earlier this Congress, I introduced H.R. 3202, the Cyber Vulnerability Disclosure Reporting Act, which was passed by the full House and is now in the Senate.

H.R. 3202 requires the Secretary of Homeland Security to submit a report on the policies and procedures developed for coordinating cyber vulnerability disclosures.

The report will include an annex with information on instances in which cyber security vulnerability disclosure policies and procedures were used to disclose details on identified weaknesses in computing systems that or digital devices at risk.

The report will provide information on the degree to which the information provided by DHS was used by industry and other stakeholders.

The reason that I worked to bring this bill before the committee is the problem often referred to as a ''Zero Day Event,'' which describes the situation that network security professionals may find themselves when a previously unknown error in computing code is exploited by a cybercriminal or terrorist.

As with other threats that this nation has faced and overcome, we must create the resources and the institutional responses to protect our nation against cyber threats while preserving our liberties and freedoms.

We cannot accomplish this task without the full cooperation and support of the private sector, computing research community and academia.

This level of engagement requires the trust and confidence of the American people that this new cyber threat center will be used for the purpose it was created and that the collaboration of others in this effort to better protect computing networks will be used only for protection and defense.

There are people with skills and those with the potential to develop skills that would be of benefit to our nation's efforts to develop an effective cybersecurity defense and deterrence posture.

It is my hope that as we move forward the Committee on Homeland Security will continue in a bipartisan manner to seek out the best ways to bring the brightest and most qualified people into the government as cybersecurity professionals.

With this policy objective in mind, I look forward to working with the Committee on H.R. 1981, the Cyber Security Education and Federal Workforce Enhancement Act.

I urge my Colleagues in the House to join me in voting for H.R. 5074.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Texas (Mr. MCCAUL) that the House suspend the rules and pass the bill, H.R. 5074, 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.

□ 1615

AIR CARGO SECURITY IMPROVEMENT ACT OF 2018

Mr. ESTES of Kansas. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 4176) to strengthen air cargo 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. 4176

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 ''Air Cargo Security Improvement Act of 2018''.

SEC. 2. ESTABLISHMENT OF AIR CARGO SECURITY DIVISION.

(a) IN GENERAL.—Subchapter II of chapter 449 of title 49, United States Code, is amended by adding at the end the following new section:

''§ 44947. Air cargo security division

''(a) ESTABLISHMENT.—Not later than 90 days after the date of the enactment of this section, the Administrator of the Transportation Security Administration shall establish an air cargo security division to carry out all policy and engagement with air cargo security stakeholders.

''(b) LEADERSHIP; STAFFING.—The air cargo security division established pursuant to subsection (a) shall be headed by an individual in the executive service within the Transportation Security Administration and be staffed by not fewer than four full-time equivalents, including the head of the division.

''(c) STAFFING.—The Administrator of the Transportation Security Administration shall staff the air cargo security division with existing Transportation Security Administration personnel.''.

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 449 of title 49, United States Code, is amended by inserting after the item related to section 44946 the following new item:

''44947. Air cargo security division.''.

SEC. 3. FEASIBILITY STUDY AND PILOT PROGRAM FOR EMERGING TECHNOLOGIES.

(a) STUDY.—Not later than 120 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration, in coordination with the Under Secretary for Science and Technology of the Department of Homeland Security, shall submit to Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a feasibility study regarding expanding the use of computed tomography technology for the screening of air cargo transported on passenger aircraft operated by an air carrier or foreign air carrier in air transportation, interstate air transportation, or interstate air commerce. Such study shall consider the following:

(1) Opportunities to leverage computed tomography systems used for screening passengers and baggage.

(2) Costs and benefits of using computed tomography technology for screening air cargo.

(3) An analysis of emerging computed tomography systems that may have potential to enhance the screening of air cargo, including systems that may address aperture challenges associated with screening certain categories of air cargo.

(4) An analysis of emerging screening technologies, in addition to computed tomography, that may be used to enhance the screening of air cargo.

(b) PILOT PROGRAM.—Not later than 120 days after submission of the feasibility study required under subsection (a), the Administrator of the Transportation Security Administration shall initiate a two-year pilot program to achieve enhanced air cargo security screening outcomes through the use of new or emerging screening technologies, such as computed tomography technology, as identified through such study.

(c) UPDATES.—Not later than 60 days after the initiation of the pilot program under subsection (b) and every six months thereafter for two years, the Administrator of the Transportation Security Administration shall brief the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate on the progress of implementation of such pilot program.

(d) DEFINITIONS.—In this section:

(1) AIR CARRIER.—The term ''air carrier'' has the meaning given such term in section 40102 of title 49, United States Code.

(2) AIR TRANSPORTATION.—The term ''air transportation'' has the meaning given such term in section 40102 of title 49, United States Code.

(3) FOREIGN AIR CARRIER.—The term ''foreign air carrier'' has the meaning given such term in section 40102 of title 49, United States Code.

(4) INTERSTATE AIR COMMERCE.—The term ''interstate air commerce'' has the meaning given such term in section 40102 of title 49, United States Code.

(5) INTERSTATE AIR TRANSPORTATION.—The term ''interstate air transportation'' has the meaning given such term in section 40102 of title 49, United States Code.

SEC. 4. AIR CARGO REGULATION REVIEW.

(a) REVIEW.—Not later than 150 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report on actions to improve the Certified Cargo Screening Program as established by the Administrator in September 2009. The report shall—