In order to meet the needs of those on the front line of homeland security activities from Customs and Border Protection and the Transportation Security to local first responders, the Science and Technology Directorate must rapidly develop and deliver innovative solutions that advance DHS' mission.

I am convinced that the whole matter of cyber technology are the new frontier of terrorism and that this Department must be, as it has been, very well prepared with human personnel being on the front lines of the first responders, and must give them extra tools through S&T to help to further the mission of the security of this Nation. It is a complex and difficult mission.

H.R. 3578 puts S&T on a pathway to making smarter and quicker R&D investment in technology and tools that help our first responders do their jobs better and more effectively.

With that, I ask my colleagues to support H.R. 3578, and I thank the proponent of this legislation.

I yield back the balance of my time.

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

I thank the gentlewoman for her support and leadership in connection with this bill. I would also like to thank Chairman MCCAUL and Ranking Member THOMPSON for their leadership in moving this important bill forward.

Mr. Speaker, threats in technologies are always changing. This bill will help DHS S&T find strategic and focused technology options and innovative solutions to address homeland security capability gaps and threats to our homeland.

I, once again, urge all of my colleagues to support H.R. 3578, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Texas (Mr. RATCLIFFE) that the House suspend the rules and pass the bill, H.R. 3578, as amended.

The question was taken.

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

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

The yeas and nays were ordered.

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

□ 1600

STATE AND LOCAL CYBER PROTECTION ACT OF 2015

Mr. HURD of Texas. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 3869) to amend the Homeland Security Act of 2002 to require State and local coordination on cybersecurity with the national cybersecurity and communications integration center, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 3869

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 ''State and Local Cyber Protection Act of 2015''.

SEC. 2. STATE AND LOCAL COORDINATION ON CYBERSECURITY WITH THE NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.

(a) IN GENERAL.—The second section 226 of the Homeland Security Act of 2002 (6 U.S.C. 148; relating to the national cybersecurity and communications integration center) is amended by adding at the end the following new subsection:

''(g) STATE AND LOCAL COORDINATION ON CYBERSECURITY.—

''(1) IN GENERAL.—The Center shall, to the extent practicable—

''(A) assist State and local governments, upon request, in identifying information system vulnerabilities;

''(B) assist State and local governments, upon request, in identifying information security protections commensurate with cybersecurity risks and the magnitude of the potential harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(i) information collected or maintained by or on behalf of a State or local government; or

''(ii) information systems used or operated by an agency or by a contractor of a State or local government or other organization on behalf of a State or local government;

''(C) in consultation with State and local governments, provide and periodically update via a web portal tools, products, resources, policies, guidelines, and procedures related to information security;

''(D) work with senior State and local government officials, including State and local Chief Information Officers, through national associations to coordinate a nationwide effort to ensure effective implementation of tools, products, resources, policies, guidelines, and procedures related to information security to secure and ensure the resiliency of State and local information systems;

''(E) provide, upon request, operational and technical cybersecurity training to State and local government and fusion center analysts and operators to address cybersecurity risks or incidents;

''(F) provide, in coordination with the Chief Privacy Officer and the Chief Civil Rights and Civil Liberties Officer of the Department, privacy and civil liberties training to State and local governments related to cybersecurity;

''(G) provide, upon request, operational and technical assistance to State and local governments to implement tools, products, resources, policies, guidelines, and procedures on information security by—

''(i) deploying technology to assist such State or local government to continuously diagnose and mitigate against cyber threats and vulnerabilities, with or without reimbursement;

''(ii) compiling and analyzing data on State and local information security; and

''(iii) developing and conducting targeted operational evaluations, including threat and vulnerability assessments, on the information systems of State and local governments;

''(H) assist State and local governments to develop policies and procedures for coordinating vulnerability disclosures, to the extent practicable, consistent with international and national standards in the information technology industry, including standards developed by the National Institute of Standards and Technology; and

''(I) ensure that State and local governments, as appropriate, are made aware of the tools, products, resources, policies, guidelines, and procedures on information security developed by the Department and other appropriate Federal departments and agencies for ensuring the security and resiliency of Federal civilian information systems.

''(2) TRAINING.—Privacy and civil liberties training provided pursuant to subparagraph (F) of paragraph (1) shall include processes, methods, and information that—

''(A) are consistent with the Department's Fair Information Practice Principles developed pursuant to section 552a of title 5, United States Code (commonly referred to as the 'Privacy Act of 1974' or the 'Privacy Act');

''(B) reasonably limit, to the greatest extent practicable, the receipt, retention, use, and disclosure of information related to cybersecurity risks and incidents associated with specific persons that is not necessary, for cybersecurity purposes, to protect an information system or network of information systems from cybersecurity risks or to mitigate cybersecurity risks and incidents in a timely manner;

''(C) minimize any impact on privacy and civil liberties;

''(D) provide data integrity through the prompt removal and destruction of obsolete or erroneous names and personal information that is unrelated to the cybersecurity risk or incident information shared and retained by the Center in accordance with this section;

''(E) include requirements to safeguard cyber threat indicators and defensive measures retained by the Center, including information that is proprietary or business-sensitive that may be used to identify specific persons from unauthorized access or acquisition;

''(F) protect the confidentiality of cyber threat indicators and defensive measures associated with specific persons to the greatest extent practicable; and

''(G) ensure all relevant constitutional, legal, and privacy protections are observed.''.

(b) CONGRESSIONAL OVERSIGHT.—Not later than two years after the date of the enactment of this Act, the national cybersecurity and communications integration center of the Department of Homeland Security shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate information on the activities and effectiveness of such activities under subsection (g) of the second section 226 of the Homeland Security Act of 2002 (6 U.S.C. 148; relating to the national cybersecurity and communications integration center), as added by subsection (a) of this section, on State and local information security. The center shall seek feedback from State and local governments regarding the effectiveness of such activities and include such feedback in the information required to be provided under this subsection.

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

The Chair recognizes the gentleman from Texas.

GENERAL LEAVE

Mr. HURD of Texas. Mr. Speaker, I ask unanimous consent that all Members have 5 legislative days within which to revise and extend their remarks and to 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. HURD of Texas. Mr. Speaker, I yield myself such time as I may consume.

The need to address cybersecurity at the State and local levels is of the utmost importance. From our local DMV offices and courthouses to our critical infrastructure, the exploitable vulnerabilities and possible consequences are alarming.

Yet, in the cybersecurity realm, State and local governments often do not have access to the technical capabilities and training that the Federal Government does.

My bill, H.R. 3869, the State and Local Cyber Protection Act, is a critical step in the resolution of this problem.

In 2010, the National Governors Association released a statement on the importance of cybersecurity in protecting the ability of Federal, State, and local governments to perform their vital functions.

They stated:

''Due to the breadth and scope of the State role in entitlement services, facilitating travel and commerce, regulatory oversight, licensing and citizen services, states gather, process, store, and share extensive amounts of personal information. From cradle to grave, the states are the nexus of identity information for individuals. This makes the states prime targets for external and internal cyber threats.''

Cybersecurity is a shared responsibility involving all levels of government and the private sector. While much has been done over the last several years to improve the Nation's cybersecurity, a number of challenges remain. This bill would allow State and local governments access to the assistance, training, and tools, voluntarily and upon request, that are required to secure our Nation's information systems at every level.

This bill instructs the National Cybersecurity and Communications Integration Center, the NCCIC, at the Department of Homeland Security to coordinate with States and locals on securing their information systems.

The NCCIC will do so by assisting in the identification of system vulnerabilities and possible solutions for State and local information security systems.

They will be developing a Web portal to communicate available tools for States and locals, providing technical training for State and local cybersecurity analysts, providing assistance and implementing cybersecurity tools upon request, providing privacy and civil liberties training, and informing States and locals on the current cybersecurity guidelines already developed at the Federal level.

Lastly, the State and Local Cyber Protection Act would require the NCCIC to seek feedback from State and local governments once the law is implemented and voluntary assistance has begun in order to gauge the effectiveness of these efforts and to ensure that progress is being made.

The Department of Homeland Security has a substantial responsibility to States and locals in the cyber realm as State and local systems host a wide range of sensitive PII and critical infrastructure data, making them especially attractive for cyberattacks. By reinforcing the relationship between DHS and State and local governments, we are supporting and urging for the continued development of cyber protection for our State and local governments.

I urge all Members to join me in supporting this bill.

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

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

I rise in support of H.R. 3869, the State and Local Cyber Protection Act of 2015.

Let me first of all thank the gentleman from Texas for his leadership in working on this legislation, to again acknowledge our chairs—Mr. MCCAUL and Mr. THOMPSON—and also to acknowledge Mr. RATCLIFFE and Mr. RICHMOND for their leadership on this issue.

Mr. Speaker, the threat of the cyber attack is growing, and the damage caused by those attacks, whether it is the theft of personally identifiable information or the disruption of operations, is becoming more costly.

FEMA has identified cybersecurity as an area for national improvement in its National Preparedness Report every year since it was first published in 2012. That finding is based, in large part, on State self-assessments reflecting a lack of confidence in cybersecurity capabilities. The threat posed by criminal and terrorist hackers continues to evolve even as State and local governments work to gain a stronger footing in the cybersecurity mission area.

Let me say that this country continues to grow, continues to increase its population, and continues to become dependent on the cybersecurity infrastructure. Helping to engage State and local entities by training is a crucial, crucial action, if I might applaud the gentleman, but also say it is a very important mission for both the Homeland Security Department and the Committee on Homeland Security. The Department of Homeland Security has resources and capabilities that, when shared with State and local governments, can help them step up their games.

H.R. 3869, the State and Local Cyber Protection Act of 2015, would codify ongoing efforts by instructing the National Cybersecurity and Communications Integration Center, the NCCIC, and the Department of Homeland Security to coordinate with State and local governments and to, upon request, provide assistance to secure their information systems.

Information systems run water entities in our communities. I remember visiting one that was up on the Web, if you will, that could be altered by a cyber attack. This legislation would codify DHS' ongoing coordination effort to give assurances to State and local governments that DHS stands ready to partner with them to protect their network.

Under this bill, DHS is authorized to assist State and local governments to deploy technology capable of diagnosing and mitigating against cyber threats and vulnerabilities.

H.R. 3869 authorizes DHS to provide training to State and local entities regarding integrating policies to protect privacy and civil liberties into their cybersecurity efforts.

It is increasingly important that all levels of government be capable of identifying information system vulnerabilities and of protecting them from unauthorized access, disclosure, and disruption of data.

I will say to the gentleman from Texas (Mr. HURD) that we have always, as a committee, been reminded of privacy and civil liberties issues while also protecting the American people. To build that capability, the Federal Government has a role to play in assisting State and local entities by providing both technical training on cybersecurity and guidance on potential privacy and civil liberties implications.

Mr. Speaker, many stakeholders throughout the country have told us this bill is a vital, much-needed step in advancing national cybersecurity capabilities.

I urge all of my colleagues to support H.R. 3869.

Mr. Speaker, I support H.R. 3869, the State and Local Cyber Protection Act.

As a Senior Member of the Homeland Security Committee, and Ranking Member of the House Judiciary Committee's Subcommittee on Crime, Terrorism, Homeland Security and Investigations I am well aware of the terrorism and criminal risks to our nation's critical infrastructure, civilian and privacy computer networks.

For this reason, I introduced H.R. 85, the Terrorism Prevention and Critical Infrastructure Protection Act, which directs the Secretary of Homeland Security to work with critical infrastructure owners and operators and state, local, and territorial to take proactive steps to address All Hazards that would impact: national security; economic stability; public health and safety; and/or any combination of these.

This nation is presented with new challenges in confronting threats to our national security, and cybersecurity.

Critical infrastructure remains an essential area that must receive the needed attention to protect it against all threats and all-hazards.

Post-9/11 established the need to anticipate unexpected threats from a variety of sources. The nation must plan to be a step ahead of our enemies in order to effectively detect, deter, and defend against terrorist attacks in whatever form they may arise, including cyberattacks to our nation's critical infrastructure.

It is for these reasons that I proposed H.R. 85, the Terrorism Prevention and Critical Infrastructure Protection Act of 2015. This bill should it become law would greatly assist in our nation's ability to protect critical infrastructure from the worse effects of cyber-attacks.

The nation must be adequately prepared to fight cyber terrorism just as vigorously as we combat other form of terrorism carried out through physical violence. We can be prepared to meet and defeat cyber terrorism threats with legislative efforts like H.R. 85, which would offer tools to effectively address terrorist attacks against critical infrastructure.

The Terrorism Prevention and Critical Infrastructure Protection Act directs the Secretary of Homeland Security (DHS) to:

(1) better engage critical infrastructure owners and operators as volunteers for the purpose of coordination of communication among state, local, tribal, and territorial entities for the purpose of taking proactive steps to manage risk and strengthen the security and resilience of the nation's critical infrastructure against terrorist attacks;

(2) establish terrorism prevention policy to engage with international partners to strengthen the security and resilience of domestic critical infrastructure and critical infrastructure located outside of the United States;

(3) make available research findings and guidance to federal civilian agencies for the identification, prioritization, assessment, remediation, and security of their internal critical infrastructure to assist in the prevention, mediation, and recovery from terrorism events.

The bill sets forth the terrorism protection responsibilities of the Department of Homeland Security as it relates to the Department's responsibility to protection and defends civilian agencies and private sector networks from cyber-attacks.

H.R. 85, Terrorism Prevention and Critical Infrastructure Protection Act also provides guidance to the Secretary of Homeland Security regarding actions to be taken to:

(1) facilitate the timely exchange of terrorism threat and vulnerability information as well as information that allows for the development of a situational awareness capability for federal civilian agencies during terrorist incidents;

(2) implement an integration and analysis function for critical infrastructure that includes operational and strategic analysis on terrorism incidents, threats, and emerging risks; and

(3) support greater terrorism cyber security information sharing by civilian federal agencies with the private sector that protects constitutional privacy and civil liberties rights.

Finally the bill directs the National Research Council to evaluate how well DHS is meeting the objectives of this Act.

I thank Chairman MCCAUL and Ranking Member THOMPSON for their support and collaboration in working with me to improve the bill for consideration by the Full Committee and ultimately the House of Representatives as we work to ensure safety, security, resiliency, trustworthiness of vital critical infrastructure networks, while at the same time ensuring that data used for this purpose does not undermine the privacy and civil liberties of Americans.

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

Mr. HURD of Texas. Mr. Speaker, I have no further requests for time, so I reserve the balance of my time.

Ms. JACKSON LEE. Mr. Speaker, I yield myself the balance of my time.

In closing, I include for the RECORD an article dated October 19 from The Hill newspaper on boosting power grid defenses against ISIS.

[From The Hill, Oct. 19, 2015]

JACKSON LEE PUSHES TO BOOST POWER-GRID DEFENSES AGAINST ISIS

(By Katie Bo Williams)

Rep. Sheila Jackson Lee (D–Texas) on Friday called for action on a bill bolstering power-grid cybersecurity after a Department of Homeland Security (DHS) official said the Islamic State in Iraq and Syria (ISIS) is trying to hack American electrical power companies.

''No solace should be taken in the fact that ISIS has been unsuccessful,'' Jackson Lee said. ''ISIS need only be successful once to have catastrophic impact on regional electricity supply.''

Caitlin Durkovich, assistant secretary for infrastructure protection at DHS, told energy firm executives at an industry conference in Philadelphia last week that ISIS ''is beginning to perpetrate cyberattacks.''

Law enforcement officials speaking at the same event indicated that the group's efforts have so far been unsuccessful, thanks in part to a Balkanized power grid and an unsophisticated approach.

''Strong intent. Thankfully, low capability,'' said John Riggi, a section chief at the FBI's cyber division. ''But the concern is that they'll buy that capability.''

Jackson Lee, a senior member of the House Homeland Security Committee and ranking member on the Judiciary Committee's Subcommittee on Crime, Terrorism, Homeland Security, and Investigations, in January introduced the Terrorism Prevention and Critical Infrastructure Protection Act.

The bill directs DHS to work with critical infrastructure companies to boost their cyber defenses against terrorist attacks, part of a swath of legislation that has attempted to codify the agency's responsibilities in that area.

Late last year, the Senate passed its version of the House-passed National Cybersecurity and Critical Infrastructure Protection Act.

The bill officially authorized an already-existing cybersecurity information-sharing hub at DHS.

Although a deadly attack on power plants or the electric grid—a ''cyber Pearl Harbor''—is still only a hypothetical, experts warn critical infrastructure sites are increasingly at risk, as electric grids get smarter.

National Security Agency Director Michael Rogers told lawmakers last fall that China and ''one or two'' other countries would be able to shut down portions of critical U.S. infrastructure with a cyberattack. Researchers suspect Iran to be on that list.

In August, DHS announced the creation of a new subcommittee dedicated to preventing attacks on the power grid.

The new panel is tasked with identifying how well the department's lifeline sectors are prepared to meet threats and recover from a significant cyber event.

The committee will also provide recommendations for a more unified approach to state and local cybersecurity.

''There is a great deal that has been done and is being done now to secure our networks,'' Homeland Security Secretary Jeh Johnson told the House Judiciary Committee in July. ''There is more to do.''

Ms. JACKSON LEE. Mr. Speaker, State and local governments have been struggling to keep pace with the evolving threats posed by cyber breaches. They just cannot do it alone. We have the resources. This Department was crafted and designed to be able to reach out beyond these parameters to ensure that local governments and State governments felt that they were secure.

I believe that the enactment of H.R. 3869 would send a clear message about our commitment to helping State and local governments address the perennial cybersecurity challenges that permeate their providing services for their constituents, which have been identified every year, according to the National Preparedness Report.

In having formerly chaired this infrastructure committee, I know that the need still remains great and that we have an opportunity to keep building and improving on that resource.

Again, I urge my colleagues to vote ''yes'' on H.R. 3869.

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

Mr. HURD of Texas. Mr. Speaker, I yield myself such time as I may consume.

I concur with the gentlewoman. Once again, I urge my colleagues to support H.R. 3869.

I yield back the balance of my time.

The SPEAKER pro tempore (Mr. THOMPSON of Pennsylvania). The question is on the motion offered by the gentleman from Texas (Mr. HURD) that the House suspend the rules and pass the bill, H.R. 3869, as amended.

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

The title of the bill was amended so as to read: ''A bill to amend the Homeland Security Act of 2002 to assist State and local coordination on cybersecurity with the national cybersecurity and communications integration center, and for other purposes.''.

A motion to reconsider was laid on the table.

FIRST RESPONDER IDENTIFICATION OF EMERGENCY NEEDS IN DISASTER SITUATIONS

Mr. HURD of Texas. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 2795) to require the Secretary of Homeland Security to submit a study on the circumstances which may impact the effectiveness and availability of first responders before, during, or after a terrorist threat or event, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 2795

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,