I think we have begun that process with this legislation, and I ask my colleagues to support it.

I yield back the balance of my time.

Mr. Speaker, I rise in strong support of H.R. 3846, the ''United States Customs and Border Protection Authorization Act.''

I am proud to be an original cosponsor of the bill, sponsored by my Subcommittee Chairman, the gentlelady from Michigan, Mrs. MILLER.

U.S. Customs and Border Protection is among the largest and most significant of the Department of Homeland Security's components.

CBP is charged with ensuring the security of America's borders while facilitating legitimate trade and travel.

Despite the essential nature of CBP's mission, it has not been authorized in law since the reorganization of the Department of Homeland Security announced by Secretary of Homeland Security Michael Chertoff nine years ago this month.

It is imperative that CBP is authorized in law to ensure that Congress can conduct proper oversight of the agency and its programs.

This legislation does just that.

I am pleased that the bill includes several amendments offered by Democratic Members during consideration by the Homeland Security Committee.

I was particularly pleased that the Committee accepted an amendment I offered to help address the recent surge in the number of unaccompanied children entering the U.S., at increasingly younger ages, particularly in my home state of Texas.

This issue requires immediate attention from Congress, given that the welfare of so many children is at stake.

I am also pleased that during Committee consideration an amendment offered by the gentlelady from California, Ms. SANCHEZ, was adopted to enhance CBP's oversight of and adherence to short-term detention standards at its facilities.

While these facilities are not intended to house individuals for long-term immigration detention, it is imperative that basic standards are adhered to in order to ensure the health and wellbeing of people, including children, in CBP custody.

I am also pleased that the Committee accepted an amendment offered by the gentleman from California, Mr. SWALWELL, stating that CBP may not enter into or renew a trusted traveler program agreement with a foreign government unless that government reports lost and stolen passport data to INTERPOL.

We know that passengers on Malaysia Airlines Flight 370 were traveling on stolen passports.

While the U.S. has relatively limited ability to ensure foreign governments utilize INTERPOL's database, encouraging them to report their own lost and stolen passports improves the quality of INTERPOL's lists used by the U.S. to screen travelers to and from our country.

That said, I was disappointed that the Committee did not accept an amendment I offered to increase by an additional 2,000 the number of CBP officers deployed at our ports of entry.

Congress recently provided the resources necessary to hire 2,000 additional CBP officers, but still more are needed.

I understand current budgetary constraints, but so many of the challenges CBP faces at our ports of entry are related to or affected by persistent staffing shortages.

Congress has a responsibility to do its part to alleviate those shortages and I hope to continue to work with my colleagues, on both sides of the aisle, on this important issue.

That said, I strongly support the bill and am pleased that Customs and Border Protection will, for the first time, be authorized in its current form.

In closing, I would like to thank the gentlelady from Michigan, Mrs. MILLER, for the bipartisan process.

I believe we produced a solid bill that should garner broad bi-partisan support in the House today.

I am particularly pleased that at this time when there is so much rancor about the Administration's response to the influx of fleeing unaccompanied children at our Southwest Border, we are standing together to authorize resources for the CBP to continue to do its part.

With that Mr. Speaker, I urge my colleagues to support H.R. 3846, the United States Customs and Border Protection Authorization Act.

Mrs. MILLER of Michigan. Mr. Speaker, I yield myself such time as I may consume.

I would just say in closing, first of all, I thought that the chairman of the Homeland Security Committee, Mr. MCCAUL, made some excellent, excellent remarks. One of the things that he said that is absolutely true, and I know all of us feel this, is every time we talk to a CBP officer, one of the men and women who so bravely secure our borders, they can't quite believe that Congress has never authorized their agency. It is not a great thing for their morale that we have never really paid them the attention that they deserve.

So I think this bill is, as I said at the beginning of my remarks, such an important first step for this Congress to be able to do that.

With the humanitarian crisis that is happening at our southern border with this tsunami of unaccompanied children that is coming in, we all see the video each and every day of our brave men and women, our CBP officers, trying to handle that. They have responsibilities there, things that they are doing there that are taking them away, quite frankly, as they are handling the children, taking them away from their duties and responsibilities of stopping the drug cartels, et cetera, from entering our borders. I just think this bill is incredibly important.

I would also mention as well, as we talk about the issues on the southern border, which are certainly in all of our news each and every day, but America has more than one border. We have the northern border as well. I see the dean of the House, Mr. DINGELL, is on the floor. He and I, both being from the northern border State of Michigan, have worked together very diligently on northern border issues. We have in Michigan the two busiest northern border crossings on the entire northern tier of our Nation there. Again, our CBP officers have stopped so many that wish our Nation harm, whether that is human smuggling or drug smuggling or what have you, we have some unique dynamics on the northern border as well, as well as our maritime border.

Mr. Speaker, this is a very, very important bill. Again, securing the homeland is certainly foremost of all of our responsibilities.

I would once again urge our colleagues to support H.R. 3846, the United States Customs and Border Protection Authorization Act, and I yield back the balance of my time.

Mr. THOMPSON of Mississippi. Mr. Speaker, I rise in support of H.R. 3846, the ''United States Customs and Border Protection Authorization Act.''

The bill before us today seeks to authorize U.S. Customs and Border Protection (CBP) for the first time since the establishment of the Department of Homeland Security.

As one of the largest operational components within DHS, CBP is charged with the critical, dual mission of securing our Nation's borders while facilitating legitimate trade and travel.

It is imperative that CBP is authorized in law in a manner consistent with its current organizational structure.

Only then can Congress conduct full and appropriate oversight of the agency and its activities.

The bill before us today serves that purpose by establishing CBP, its leadership structure, and its functions in law.

I am pleased to say that H.R. 3846 is a bipartisan product that has benefitted from input from Members on both sides of the aisle during the Committee process. Democratic Members of the Committee on Homeland Security offered important amendments on unaccompanied children crossing the border; electronic searches at the border; standards at short-term detention facilities; and professionalism and accountability for CBP personnel.

I want to congratulate the Chairman and Ranking Member of the Subcommittee on Border and Maritime Security, Rep. CANDICE MILLER and Rep. JACKSON LEE, for their hard work on this measure.

The bill before us today reflects the results of the bipartisan spirit in which they conduct their work, and it should be something all Members can give their strong support.

Mr. Speaker, I urge my colleagues to support H.R. 3846, the ''United States Customs and Border Protection Authorization Act.''

The SPEAKER pro tempore. The question is on the motion offered by the gentlewoman from Michigan (Mrs. MILLER) that the House suspend the rules and pass the bill, H.R. 3846, 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.

NATIONAL CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION ACT OF 2014

Mr. MCCAUL. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 3696) to amend the Homeland Security Act of 2002 to make certain improvements regarding cybersecurity

and critical infrastructure protection, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 3696

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 ''National Cybersecurity and Critical Infrastructure Protection Act of 2014''.

SEC. 2. TABLE OF CONTENTS.

The table of contents for this Act is as follows:

Sec. 1. Short title.
Sec. 2. Table of contents.

TITLE I—SECURING THE NATION AGAINST CYBER ATTACK

Sec. 101. Homeland Security Act of 2002 definitions.
Sec. 102. Enhancement of cybersecurity.
Sec. 103. Protection of critical infrastructure and information sharing.
Sec. 104. National Cybersecurity and Communications Integration Center.
Sec. 105. Cyber incident response and technical assistance.
Sec. 106. Streamlining of Department cybersecurity organization.

TITLE II—PUBLIC-PRIVATE COLLABORATION ON CYBERSECURITY

Sec. 201. Public-private collaboration on cybersecurity.
Sec. 202. SAFETY Act and qualifying cyber incidents.
Sec. 203. Prohibition on new regulatory authority.
Sec. 204. Prohibition on additional authorization of appropriations.
Sec. 205. Prohibition on collection activities to track individuals' personally identifiable information.
Sec. 206. Cybersecurity scholars.
Sec. 207. National Research Council study on the resilience and reliability of the Nation's power grid.

TITLE III—HOMELAND SECURITY CYBERSECURITY WORKFORCE

Sec. 301. Homeland security cybersecurity workforce.
Sec. 302. Personnel authorities.

TITLE I—SECURING THE NATION AGAINST CYBER ATTACK

SEC. 101. HOMELAND SECURITY ACT OF 2002 DEFINITIONS.

Section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101) is amended by adding at the end the following new paragraphs:

''(19) The term 'critical infrastructure' has the meaning given that term in section 1016(e) of the USA Patriot Act (42 U.S.C. 5195c(e)).

''(20) The term 'critical infrastructure owner' means a person that owns critical infrastructure.

''(21) The term 'critical infrastructure operator' means a critical infrastructure owner or other person that manages, runs, or operates, in whole or in part, the day-to-day operations of critical infrastructure.

''(22) The term 'cyber incident' means an incident, or an attempt to cause an incident, that, if successful, would—

''(A) jeopardize or imminently jeopardize, without lawful authority, the security, integrity, confidentiality, or availability of an information system or network of information systems or any information stored on, processed on, or transiting such a system or network;

''(B) constitute a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies related to such a system or network, or an act of terrorism against such a system or network; or

''(C) result in the denial of access to or degradation, disruption, or destruction of such a system or network, or the defeat of an operations control or technical control essential to the security or operation of such a system or network.

''(23) The term 'cybersecurity mission' means activities that encompass the full range of threat reduction, vulnerability reduction, deterrence, incident response, resiliency, and recovery activities to foster the security and stability of cyberspace.

''(24) The term 'cybersecurity purpose' means the purpose of ensuring the security, integrity, confidentiality, or availability of, or safeguarding, an information system or network of information systems, including protecting such a system or network, or data residing on such a system or network, including protection of such a system or network, from—

''(A) a vulnerability of such a system or network;

''(B) a threat to the security, integrity, confidentiality, or availability of such a system or network, or any information stored on, processed on, or transiting such a system or network;

''(C) efforts to deny access to or degrade, disrupt, or destroy such a system or network; or

''(D) efforts to gain unauthorized access to such a system or network, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting such a system or network.

''(25) The term 'cyber threat' means any action that may result in unauthorized access to, exfiltration of, manipulation of, harm of, or impairment to the security, integrity, confidentiality, or availability of an information system or network of information systems, or information that is stored on, processed by, or transiting such a system or network.

''(26) The term 'cyber threat information' means information directly pertaining to—

''(A) a vulnerability of an information system or network of information systems of a government or private entity;

''(B) a threat to the security, integrity, confidentiality, or availability of such a system or network of a government or private entity, or any information stored on, processed on, or transiting such a system or network;

''(C) efforts to deny access to or degrade, disrupt, or destroy such a system or network of a government or private entity;

''(D) efforts to gain unauthorized access to such a system or network, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting such a system or network; or

''(E) an act of terrorism against an information system or network of information systems.

''(27) The term 'Federal civilian information systems'—

''(A) means information, information systems, and networks of information systems that are owned, operated, controlled, or licensed for use by, or on behalf of, any Federal agency, including such systems or networks used or operated by another entity on behalf of a Federal agency; but

''(B) does not include—

''(i) a national security system; or

''(ii) information, information systems, and networks of information systems that are owned, operated, controlled, or licensed solely for use by, or on behalf of, the Department of Defense, a military department, or an element of the intelligence community.

''(28) The term 'information security' means the protection of information, information systems, and networks of information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

''(A) integrity, including guarding against improper information modification or destruction, including ensuring nonrepudiation and authenticity;

''(B) confidentiality, including preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

''(C) availability, including ensuring timely and reliable access to and use of information.

''(29) The term 'information system' means the underlying framework and functions used to process, transmit, receive, or store information electronically, including programmable electronic devices, communications networks, and industrial or supervisory control systems and any associated hardware, software, or data.

''(30) The term 'private entity' means any individual or any private or publically-traded company, public or private utility (including a utility that is a unit of a State or local government, or a political subdivision of a State government), organization, or corporation, including an officer, employee, or agent thereof.

''(31) The term 'shared situational awareness' means an environment in which cyber threat information is shared in real time between all designated Federal cyber operations centers to provide actionable information about all known cyber threats.''.

SEC. 102. ENHANCEMENT OF CYBERSECURITY.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002 is amended by adding at the end the following new section:

''SEC. 226. ENHANCEMENT OF CYBERSECURITY.

''The Secretary, in collaboration with the heads of other appropriate Federal Government entities, shall conduct activities for cybersecurity purposes, including the provision of shared situational awareness to each other to enable real-time, integrated, and operational actions to protect from, prevent, mitigate, respond to, and recover from cyber incidents.''.

(b) CLERICAL AMENDMENTS.—

(1) SUBTITLE HEADING.—The heading for subtitle C of title II of such Act is amended to read as follows:

''Subtitle C—Cybersecurity and Information Sharing''.

(2) TABLE OF CONTENTS.—The table of contents in section 1(b) of such Act is amended—

(A) by adding after the item relating to section 225 the following new item:

''Sec. 226. Enhancement of cybersecurity.'';

and

(B) by striking the item relating to subtitle C of title II and inserting the following new item:

''Subtitle C—Cybersecurity and Information Sharing''.

SEC. 103. PROTECTION OF CRITICAL INFRASTRUCTURE AND INFORMATION SHARING.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002, as amended by section 102, is further amended by adding at the end the following new section:

''SEC. 227. PROTECTION OF CRITICAL INFRASTRUCTURE AND INFORMATION SHARING.

''(a) PROTECTION OF CRITICAL INFRASTRUCTURE.—

''(1) IN GENERAL.—The Secretary shall coordinate, on an ongoing basis, with Federal, State, and local governments, national laboratories, critical infrastructure owners, critical infrastructure operators, and other cross sector coordinating entities to—

''(A) facilitate a national effort to strengthen and maintain secure, functioning, and resilient critical infrastructure from cyber threats;

''(B) ensure that Department policies and procedures enable critical infrastructure owners and critical infrastructure operators to receive real-time, actionable, and relevant cyber threat information;

''(C) seek industry sector-specific expertise to—

''(i) assist in the development of voluntary security and resiliency strategies; and

''(ii) ensure that the allocation of Federal resources are cost effective and reduce any burden on critical infrastructure owners and critical infrastructure operators;

''(D) upon request of entities, facilitate and assist risk management efforts of such entities to reduce vulnerabilities, identify and disrupt threats, and minimize consequences to their critical infrastructure;

''(E) upon request of critical infrastructure owners or critical infrastructure operators, provide education and assistance to such owners and operators on how they may use protective measures and countermeasures to strengthen the security and resilience of the Nation's critical infrastructure; and

''(F) coordinate a research and development strategy to facilitate and promote advancements and innovation in cybersecurity technologies to protect critical infrastructure.

''(2) ADDITIONAL RESPONSIBILITIES.—The Secretary shall—

''(A) manage Federal efforts to secure, protect, and ensure the resiliency of Federal civilian information systems using a risk-based and performance-based approach, and, upon request of critical infrastructure owners or critical infrastructure operators, support such owners' and operators' efforts to secure, protect, and ensure the resiliency of critical infrastructure from cyber threats;

''(B) direct an entity within the Department to serve as a Federal civilian entity by and among Federal, State, and local governments, private entities, and critical infrastructure sectors to provide multi-directional sharing of real-time, actionable, and relevant cyber threat information;

''(C) build upon existing mechanisms to promote a national awareness effort to educate the general public on the importance of securing information systems;

''(D) upon request of Federal, State, and local government entities and private entities, facilitate expeditious cyber incident response and recovery assistance, and provide analysis and warnings related to threats to and vulnerabilities of critical information systems, crisis and consequence management support, and other remote or on-site technical assistance with the heads of other appropriate Federal agencies to Federal, State, and local government entities and private entities for cyber incidents affecting critical infrastructure;

''(E) engage with international partners to strengthen the security and resilience of domestic critical infrastructure and critical infrastructure located outside of the United States upon which the United States depends; and

''(F) conduct outreach to educational institutions, including historically black colleges and universities, Hispanic serving institutions, Native American colleges, and institutions serving persons with disabilities, to encourage such institutions to promote cybersecurity awareness.

''(3) RULE OF CONSTRUCTION.—Nothing in this section may be construed to require any private entity to request assistance from the Secretary, or require any private entity requesting such assistance to implement any measure or recommendation suggested by the Secretary.

''(b) CRITICAL INFRASTRUCTURE SECTORS.—The Secretary, in collaboration with the heads of other appropriate Federal agencies, shall designate critical infrastructure sectors (that may include subdivisions of sectors within a sector as the Secretary may determine appropriate). The critical infrastructure sectors designated under this subsection may include the following:

''(1) Chemical.

''(2) Commercial facilities.

''(3) Communications.

''(4) Critical manufacturing.

''(5) Dams.

''(6) Defense Industrial Base.

''(7) Emergency services.

''(8) Energy.

''(9) Financial services.

''(10) Food and agriculture.

''(11) Government facilities.

''(12) Healthcare and public health.

''(13) Information technology.

''(14) Nuclear reactors, materials, and waste.

''(15) Transportation systems.

''(16) Water and wastewater systems.

''(17) Such other sectors as the Secretary determines appropriate.

''(c) SECTOR SPECIFIC AGENCIES.—The Secretary, in collaboration with the relevant critical infrastructure sector and the heads of other appropriate Federal agencies, shall recognize the Federal agency designated as of November 1, 2013, as the 'Sector Specific Agency' for each critical infrastructure sector designated under subsection (b). If the designated Sector Specific Agency for a particular critical infrastructure sector is the Department, for the purposes of this section, the Secretary shall carry out this section. The Secretary, in coordination with the heads of each such Sector Specific Agency shall—

''(1) support the security and resilience activities of the relevant critical infrastructure sector in accordance with this subtitle; and

''(2) provide institutional knowledge and specialized expertise to the relevant critical infrastructure sector.

''(d) SECTOR COORDINATING COUNCILS.—

''(1) RECOGNITION.—The Secretary, in collaboration with each critical infrastructure sector and the relevant Sector Specific Agency, shall recognize and partner with the Sector Coordinating Council for each critical infrastructure sector designated under subsection (b) to coordinate with each such sector on security and resilience activities and emergency response and recovery efforts.

''(2) MEMBERSHIP.—

''(A) IN GENERAL.—The Sector Coordinating Council for a critical infrastructure sector designated under subsection (b) shall—

''(i) be comprised exclusively of relevant critical infrastructure owners, critical infrastructure operators, private entities, and representative trade associations for the sector;

''(ii) reflect the unique composition of each sector; and

''(iii) as appropriate, include relevant small, medium, and large critical infrastructure owners, critical infrastructure operators, private entities, and representative trade associations for the sector.

''(B) PROHIBITION.—No government entity with regulating authority shall be a member of the Sector Coordinating Council.

''(C) LIMITATION.—The Secretary shall have no role in the determination of the membership of a Sector Coordinating Council.

''(3) ROLES AND RESPONSIBILITIES.—The Sector Coordinating Council for a critical infrastructure sector shall—

''(A) serve as a self-governing, self-organized primary policy, planning, and strategic communications entity for coordinating with the Department, the relevant Sector-Specific Agency designated under subsection (c), and the relevant Information Sharing and Analysis Centers under subsection (e) on security and resilience activities and emergency response and recovery efforts;

''(B) establish governance and operating procedures, and designate a chairperson for the sector to carry out the activities described in this subsection;

''(C) coordinate with the Department, the relevant Information Sharing and Analysis Centers under subsection (e), and other Sector Coordinating Councils to update, maintain, and exercise the National Cybersecurity Incident Response Plan in accordance with section 229(b); and

''(D) provide any recommendations to the Department on infrastructure protection technology gaps to help inform research and development efforts at the Department.

''(e) SECTOR INFORMATION SHARING AND ANALYSIS CENTERS.—

''(1) RECOGNITION.—The Secretary, in collaboration with the relevant Sector Coordinating Council and the critical infrastructure sector represented by such Council, and in coordination with the relevant Sector Specific Agency, shall recognize at least one Information Sharing and Analysis Center for each critical infrastructure sector designated under subsection (b) for purposes of paragraph (3). No other Information Sharing and Analysis Organizations, including Information Sharing and Analysis Centers, may be precluded from having an information sharing relationship within the National Cybersecurity and Communications Integration Center established pursuant to section 228. Nothing in this subsection or any other provision of this subtitle may be construed to limit, restrict, or condition any private entity or activity utilized by, among, or between private entities.

''(2) ROLES AND RESPONSIBILITIES.—In addition to such other activities as may be authorized by law, at least one Information Sharing and Analysis Center for a critical infrastructure sector shall—

''(A) serve as an information sharing resource for such sector and promote ongoing multi-directional sharing of real-time, relevant, and actionable cyber threat information and analysis by and among such sector, the Department, the relevant Sector Specific Agency, and other critical infrastructure sector Information Sharing and Analysis Centers;

''(B) establish governance and operating procedures to carry out the activities conducted under this subsection;

''(C) serve as an emergency response and recovery operations coordination point for such sector, and upon request, facilitate cyber incident response capabilities in coordination with the Department, the relevant Sector Specific Agency and the relevant Sector Coordinating Council;

''(D) facilitate cross-sector coordination and sharing of cyber threat information to prevent related or consequential impacts to other critical infrastructure sectors;

''(E) coordinate with the Department, the relevant Sector Coordinating Council, the relevant Sector Specific Agency, and other critical infrastructure sector Information Sharing and Analysis Centers on the development, integration, and implementation of procedures to support technology neutral,

real-time information sharing capabilities and mechanisms within the National Cybersecurity and Communications Integration Center established pursuant to section 228, including—

''(i) the establishment of a mechanism to voluntarily report identified vulnerabilities and opportunities for improvement;

''(ii) the establishment of metrics to assess the effectiveness and timeliness of the Department's and Information Sharing and Analysis Centers' information sharing capabilities; and

''(iii) the establishment of a mechanism for anonymous suggestions and comments;

''(F) implement an integration and analysis function to inform sector planning, risk mitigation, and operational activities regarding the protection of each critical infrastructure sector from cyber incidents;

''(G) combine consequence, vulnerability, and threat information to share actionable assessments of critical infrastructure sector risks from cyber incidents;

''(H) coordinate with the Department, the relevant Sector Specific Agency, and the relevant Sector Coordinating Council to update, maintain, and exercise the National Cybersecurity Incident Response Plan in accordance with section 229(b); and

''(I) safeguard cyber threat information from unauthorized disclosure.

''(3) FUNDING.—Of the amounts authorized to be appropriated for each of fiscal years 2014, 2015, and 2016 for the Cybersecurity and Communications Office of the Department, the Secretary is authorized to use not less than $25,000,000 for any such year for operations support at the National Cybersecurity and Communications Integration Center established under section 228(a) of all recognized Information Sharing and Analysis Centers under paragraph (1) of this subsection.

''(f) CLEARANCES.—The Secretary—

''(1) shall expedite the process of security clearances under Executive Order 13549 or successor orders for appropriate representatives of Sector Coordinating Councils and the critical infrastructure sector Information Sharing and Analysis Centers; and

''(2) may so expedite such processing to—

''(A) appropriate personnel of critical infrastructure owners and critical infrastructure operators; and

''(B) any other person as determined by the Secretary.

''(g) PUBLIC-PRIVATE COLLABORATION.—The Secretary, in collaboration with the critical infrastructure sectors designated under subsection (b), such sectors' Sector Specific Agencies recognized under subsection (c), and the Sector Coordinating Councils recognized under subsection (d), shall—

''(1) conduct an analysis and review of the existing public-private partnership model and evaluate how the model between the Department and critical infrastructure owners and critical infrastructure operators can be improved to ensure the Department, critical infrastructure owners, and critical infrastructure operators are equal partners and regularly collaborate on all programs and activities of the Department to protect critical infrastructure;

''(2) develop and implement procedures to ensure continuous, collaborative, and effective interactions between the Department, critical infrastructure owners, and critical infrastructure operators; and

''(3) ensure critical infrastructure sectors have a reasonable period for review and comment of all jointly produced materials with the Department.

''(h) RECOMMENDATIONS REGARDING NEW AGREEMENTS.—Not later than 180 days after the date of the enactment of this section, the Secretary shall submit to the appropriate congressional committees recommendations on how to expedite the implementation of information sharing agreements for cybersecurity purposes between the Secretary and critical information owners and critical infrastructure operators and other private entities. Such recommendations shall address the development and utilization of a scalable form that retains all privacy and other protections in such agreements in existence as of such date, including Cooperative and Research Development Agreements. Such recommendations should also include any additional authorities or resources that may be needed to carry out the implementation of any such new agreements.

''(i) RULE OF CONSTRUCTION.—No provision of this title may be construed as modifying, limiting, or otherwise affecting the authority of any other Federal agency under any other provision of law.''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by adding after the item relating to section 226 (as added by section 102) the following new item:

''Sec. 227. Protection of critical infrastructure and information sharing.''.

SEC. 104. NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002, as amended by sections 102 and 103, is further amended by adding at the end the following new section:

''SEC. 228. NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.

''(a) ESTABLISHMENT.—There is established in the Department the National Cybersecurity and Communications Integration Center (referred to in this section as the 'Center'), which shall be a Federal civilian information sharing interface that provides shared situational awareness to enable real-time, integrated, and operational actions across the Federal Government, and share cyber threat information by and among Federal, State, and local government entities, Information Sharing and Analysis Centers, private entities, and critical infrastructure owners and critical infrastructure operators that have an information sharing relationship with the Center.

''(b) COMPOSITION.—The Center shall include each of the following entities:

''(1) At least one Information Sharing and Analysis Center established under section 227(e) for each critical infrastructure sector.

''(2) The Multi-State Information Sharing and Analysis Center to collaborate with State and local governments.

''(3) The United States Computer Emergency Readiness Team to coordinate cyber threat information sharing, proactively manage cyber risks to the United States, collaboratively respond to cyber incidents, provide technical assistance to information system owners and operators, and disseminate timely notifications regarding current and potential cyber threats and vulnerabilities.

''(4) The Industrial Control System Cyber Emergency Response Team to coordinate with industrial control systems owners and operators and share industrial control systems-related security incidents and mitigation measures.

''(5) The National Coordinating Center for Telecommunications to coordinate the protection, response, and recovery of national security emergency communications.

''(6) Such other Federal, State, and local government entities, private entities, organizations, or individuals as the Secretary may consider appropriate that agree to be included.

''(c) CYBER INCIDENT.—In the event of a cyber incident, the Secretary may grant the entities referred to in subsection (a) immediate temporary access to the Center as a situation may warrant.

''(d) ROLES AND RESPONSIBILITIES.—The Center shall—

''(1) promote ongoing multi-directional sharing by and among the entities referred to in subsection (a) of timely and actionable cyber threat information and analysis on a real-time basis that includes emerging trends, evolving threats, incident reports, intelligence information, risk assessments, and best practices;

''(2) coordinate with other Federal agencies to streamline and reduce redundant reporting of cyber threat information;

''(3) provide, upon request, timely technical assistance and crisis management support to Federal, State, and local government entities and private entities that own or operate information systems or networks of information systems to protect from, prevent, mitigate, respond to, and recover from cyber incidents;

''(4) facilitate cross-sector coordination and sharing of cyber threat information to prevent related or consequential impacts to other critical infrastructure sectors;

''(5) collaborate and facilitate discussions with Sector Coordinating Councils, Information Sharing and Analysis Centers, Sector Specific Agencies, and relevant critical infrastructure sectors on the development of prioritized Federal response efforts, if necessary, to support the defense and recovery of critical infrastructure from cyber incidents;

''(6) collaborate with the Sector Coordinating Councils, Information Sharing and Analysis Centers, Sector Specific Agencies, and the relevant critical infrastructure sectors on the development and implementation of procedures to support technology neutral real-time information sharing capabilities and mechanisms;

''(7) collaborate with the Sector Coordinating Councils, Information Sharing and Analysis Centers, Sector Specific Agencies, and the relevant critical infrastructure sectors to identify requirements for data and information formats and accessibility, system interoperability, and redundant systems and alternative capabilities in the event of a disruption in the primary information sharing capabilities and mechanisms at the Center;

''(8) within the scope of relevant treaties, cooperate with international partners to share information and respond to cyber incidents;

''(9) safeguard sensitive cyber threat information from unauthorized disclosure;

''(10) require other Federal civilian agencies to—

''(A) send reports and information to the Center about cyber incidents, threats, and vulnerabilities affecting Federal civilian information systems and critical infrastructure systems and, in the event a private vendor product or service of such an agency is so implicated, the Center shall first notify such private vendor of the vulnerability before further disclosing such information;

''(B) provide to the Center cyber incident detection, analysis, mitigation, and response information; and

''(C) immediately send and disclose to the Center cyber threat information received by such agencies;

''(11) perform such other duties as the Secretary may require to facilitate a national effort to strengthen and maintain secure, functioning, and resilient critical infrastructure from cyber threats;

''(12) implement policies and procedures to—

''(A) provide technical assistance to Federal civilian agencies to prevent and respond to data breaches involving unauthorized acquisition or access of personally identifiable information that occur on Federal civilian information systems;

''(B) require Federal civilian agencies to notify the Center about data breaches involving unauthorized acquisition or access of personally identifiable information that occur on Federal civilian information systems without unreasonable delay after the discovery of such a breach; and

''(C) require Federal civilian agencies to notify all potential victims of a data breach involving unauthorized acquisition or access of personally identifiable information that occur on Federal civilian information systems without unreasonable delay, based on a reasonable determination of the level of risk of harm and consistent with the needs of law enforcement; and

''(13) participate in exercises run by the Department's National Exercise Program, where appropriate.

''(e) INTEGRATION AND ANALYSIS.—The Center, in coordination with the Office of Intelligence and Analysis of the Department, shall maintain an integration and analysis function, which shall —

''(1) integrate and analyze all cyber threat information received from other Federal agencies, State and local governments, Information Sharing and Analysis Centers, private entities, critical infrastructure owners, and critical infrastructure operators, and share relevant information in near real-time;

''(2) on an ongoing basis, assess and evaluate consequence, vulnerability, and threat information to share with the entities referred to in subsection (a) actionable assessments of critical infrastructure sector risks from cyber incidents and to assist critical infrastructure owners and critical infrastructure operators by making recommendations to facilitate continuous improvements to the security and resiliency of the critical infrastructure of the United States;

''(3) facilitate cross-sector integration, identification, and analysis of key interdependencies to prevent related or consequential impacts to other critical infrastructure sectors;

''(4) collaborate with the Information Sharing and Analysis Centers to tailor the analysis of information to the specific characteristics and risk to a relevant critical infrastructure sector; and

''(5) assess and evaluate consequence, vulnerability, and threat information regarding cyber incidents in coordination with the Office of Emergency Communications of the Department to help facilitate continuous improvements to the security and resiliency of public safety communications networks.

''(f) REPORT ON CYBER ATTACKS AGAINST FEDERAL GOVERNMENT NETWORKS.—The Secretary shall submit to the Committee on Homeland Security of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Comptroller General of the United States an annual report that summarizes major cyber incidents involving Federal civilian agency information systems and provides aggregate statistics on the number of breaches, the extent of any personally identifiable information that was involved, the volume of data exfiltrated, the consequential impact, and the estimated cost of remedying such breaches.

''(g) REPORT ON THE OPERATIONS OF THE CENTER.—The Secretary, in consultation with the Sector Coordinating Councils and appropriate Federal Government entities, shall submit to the Committee on Homeland Security of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Comptroller General of the United States an annual report on—

''(1) the capability and capacity of the Center to carry out its cybersecurity mission in accordance with this section, and sections 226, 227, 229, 230, 230A, and 230B;

''(2) the extent to which the Department is engaged in information sharing with each critical infrastructure sector designated under section 227(b), including—

''(A) the extent to which each such sector has representatives at the Center; and

''(B) the extent to which critical infrastructure owners and critical infrastructure operators of each critical infrastructure sector participate in information sharing at the Center;

''(3) the volume and range of activities with respect to which the Secretary collaborated with the Sector Coordinating Councils and the Sector-Specific Agencies to promote greater engagement with the Center; and

''(4) the volume and range of voluntary technical assistance sought and provided by the Department to each critical infrastructure owner and critical infrastructure operator.''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by adding after the item relating to section 227 (as added by section 103) the following new item:

''Sec. 228. National Cybersecurity and Communications Integration Center.''.

(c) GAO REPORT.—Not later than one year after the date of the enactment of this Act, the Comptroller General of the United States 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 the effectiveness of the National Cybersecurity and Communications Integration Center established under section 228 of the Homeland Security Act of 2002, as added by subsection (a) of this section, in carrying out its cybersecurity mission (as such term is defined in section 2 of the Homeland Security Act of 2002, as amended by section 101) in accordance with this Act and such section 228 and sections 226, 227, 229, 230, 230A, and 230B of the Homeland Security Act of 2002, as added by this Act.

SEC. 105. CYBER INCIDENT RESPONSE AND TECHNICAL ASSISTANCE.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002, as amended by sections 102, 103, and 104, is further amended by adding at the end the following new section:

''SEC. 229. CYBER INCIDENT RESPONSE AND TECHNICAL ASSISTANCE.

''(a) IN GENERAL.—The Secretary shall establish Cyber Incident Response Teams to—

''(1) upon request, provide timely technical assistance and crisis management support to Federal, State, and local government entities, private entities, and critical infrastructure owners and critical infrastructure operators involving cyber incidents affecting critical infrastructure; and

''(2) upon request, provide actionable recommendations on security and resilience measures and countermeasures to Federal, State, and local government entities, private entities, and critical infrastructure owners and critical infrastructure operators prior to, during, and after cyber incidents.

''(b) COORDINATION.—In carrying out subsection (a), the Secretary shall coordinate with the relevant Sector Specific Agencies, if applicable.

''(c) CYBER INCIDENT RESPONSE PLAN.—The Secretary, in coordination with the Sector Coordinating Councils, Information Sharing and Analysis Centers, and Federal, State, and local governments, shall develop, regularly update, maintain, and exercise a National Cybersecurity Incident Response Plan which shall—

''(1) include effective emergency response plans associated with cyber threats to critical infrastructure, information systems, or networks of information systems;

''(2) ensure that such National Cybersecurity Incident Response Plan can adapt to and reflect a changing cyber threat environment, and incorporate best practices and lessons learned from regular exercises, training, and after-action reports; and

''(3) facilitate discussions on the best methods for developing innovative and useful cybersecurity exercises for coordinating between the Department and each of the critical infrastructure sectors designated under section 227(b).

''(d) UPDATE TO CYBER INCIDENT ANNEX TO THE NATIONAL RESPONSE FRAMEWORK.—The Secretary, in coordination with the heads of other Federal agencies and in accordance with the National Cybersecurity Incident Response Plan under subsection (c), shall regularly update, maintain, and exercise the Cyber Incident Annex to the National Response Framework of the Department.''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by adding after the item relating to section 228 (as added by section 104) the following new item:

''Sec. 229. Cyber incident response and technical assistance.''.

SEC. 106. STREAMLINING OF DEPARTMENT CYBERSECURITY ORGANIZATION.

(a) CYBERSECURITY AND INFRASTRUCTURE PROTECTION DIRECTORATE.—The National Protection and Programs Directorate of the Department of Homeland Security shall, after the date of the enactment of this Act, be known and designated as the ''Cybersecurity and Infrastructure Protection Directorate''. Any reference to the National Protection and Programs Directorate of the Department in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Cybersecurity and Infrastructure Protection Directorate of the Department.

(b) SENIOR LEADERSHIP OF THE CYBERSECURITY AND INFRASTRUCTURE PROTECTION DIRECTORATE.—

(1) IN GENERAL.—Paragraph (1) of section 103(a) of the Homeland Security Act of 2002 (6 U.S.C. 113(a)) is amended by adding at the end the following new subparagraphs:

''(K) Under Secretary for Cybersecurity and Infrastructure Protection.

''(L) Deputy Under Secretary for Cybersecurity.

''(M) Deputy Under Secretary for Infrastructure Protection.''.

(2) CONTINUATION IN OFFICE.—The individuals who hold the positions referred to in subparagraphs (K), (L), and (M) of subsection (a) of section 103 of the Homeland Security Act of 2002 (as added by paragraph (1) of this subsection) as of the date of the enactment of this Act may continue to hold such positions.

(c) REPORT ON IMPROVING THE CAPABILITY AND EFFECTIVENESS OF THE CYBERSECURITY AND COMMUNICATIONS OFFICE.—To improve the operational capability and effectiveness in carrying out the cybersecurity mission (as such term is defined in section 2 of the Homeland Security Act of 2002, as amended by section 101) of the Department of Homeland Security, the Secretary 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—

(1) the feasibility of making the Cybersecurity and Communications Office of the Department an operational component of the Department;

(2) recommendations for restructuring the SAFETY Act Office within the Department to protect and maintain operations in accordance with the Office's mission to provide incentives for the development and deployment of anti-terrorism technologies while elevating the profile and mission of the Office, including the feasibility of utilizing third-party registrars for improving the throughput and effectiveness of the certification process.

(d) REPORT ON CYBERSECURITY ACQUISITION CAPABILITIES.—The Secretary of Homeland Security shall assess the effectiveness of the Department of Homeland Security's acquisition processes and the use of existing authorities for acquiring cybersecurity technologies to ensure that such processes and authorities are capable of meeting the needs and demands of the Department's cybersecurity mission (as such term is defined in section 2 of the Homeland Security Act of 2002, as amended by section 101). Not later than 180 days after the date of the enactment of this Act, the Secretary 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 the effectiveness of the Department's acquisition processes for cybersecurity technologies.

(e) RESOURCE INFORMATION.—The Secretary of Homeland Security shall make available Department of Homeland Security contact information to serve as a resource for Sector Coordinating Councils and critical infrastructure owners and critical infrastructure operators to better coordinate cybersecurity efforts with the Department relating to emergency response and recovery efforts for cyber incidents.

TITLE II—PUBLIC-PRIVATE COLLABORATION ON CYBERSECURITY

SEC. 201. PUBLIC-PRIVATE COLLABORATION ON CYBERSECURITY.

(a) NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.—

(1) IN GENERAL.—The Director of the National Institute of Standards and Technology, in coordination with the Secretary of Homeland Security, shall, on an ongoing basis, facilitate and support the development of a voluntary, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to reduce cyber risks to critical infrastructure. The Director, in coordination with the Secretary—

(A) shall—

(i) coordinate closely and continuously with relevant private entities, critical infrastructure owners and critical infrastructure operators, Sector Coordinating Councils, Information Sharing and Analysis Centers, and other relevant industry organizations, and incorporate industry expertise to the fullest extent possible;

(ii) consult with the Sector Specific Agencies, Federal, State and local governments, the governments of other countries, and international organizations;

(iii) utilize a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, that may be voluntarily adopted by critical infrastructure owners and critical infrastructure operators to help them identify, assess, and manage cyber risks;

(iv) include methodologies to—

(I) identify and mitigate impacts of the cybersecurity measures or controls on business confidentiality; and

(II) protect individual privacy and civil liberties;

(v) incorporate voluntary consensus standards and industry best practices, and align with voluntary international standards to the fullest extent possible;

(vi) prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and processes; and

(vii) include such other similar and consistent elements as determined necessary; and

(B) shall not prescribe or otherwise require—

(i) the use of specific solutions;

(ii) the use of specific information technology products or services; or

(iii) that information technology products or services be designed, developed, or manufactured in a particular manner.

(2) LIMITATION.—Information shared with or provided to the Director of the National Institute of Standards and Technology or the Secretary of Homeland Security for the purpose of the activities under paragraph (1) may not be used by any Federal, State, or local government department or agency to regulate the activity of any private entity.

(b) AMENDMENT.—

(1) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002, as amended by sections 102, 103, 104, and 105, is further amended by adding at the end the following new section:

"SEC. 230. PUBLIC-PRIVATE COLLABORATION ON CYBERSECURITY.

''(a) MEETINGS.—The Secretary shall meet with the Sector Coordinating Council for each critical infrastructure sector designated under section 227(b) on a biannual basis to discuss the cybersecurity threat to critical infrastructure, voluntary activities to address cybersecurity, and ideas to improve the public-private partnership to enhance cybersecurity, in which the Secretary shall—

''(1) provide each Sector Coordinating Council an assessment of the cybersecurity threat to each critical infrastructure sector designated under section 227(b), including information relating to—

''(A) any actual or assessed cyber threat, including a consideration of adversary capability and intent, preparedness, target attractiveness, and deterrence capabilities;

''(B) the extent and likelihood of death, injury, or serious adverse effects to human health and safety caused by an act of terrorism or other disruption, destruction, or unauthorized use of critical infrastructure;

''(C) the threat to national security caused by an act of terrorism or other disruption, destruction, or unauthorized use of critical infrastructure; and

''(D) the harm to the economy that would result from an act of terrorism or other disruption, destruction, or unauthorized use of critical infrastructure; and

''(2) provide recommendations, which may be voluntarily adopted, on ways to improve cybersecurity of critical infrastructure.

''(b) REPORT.—

''(1) IN GENERAL.—Starting 30 days after the end of the fiscal year in which the National Cybersecurity and Critical Infrastructure Protection Act of 2013 is enacted and annually thereafter, the Secretary shall submit to the appropriate congressional committees a report on the state of cybersecurity for each critical infrastructure sector designated under section 227(b) based on discussions between the Department and the Sector Coordinating Council in accordance with subsection (a) of this section. The Secretary shall maintain a public copy of each report, and each report may include a nonpublic annex for proprietary, business-sensitive information, or other sensitive information. Each report shall include, at a minimum information relating to—

''(A) the risk to each critical infrastructure sector, including known cyber threats, vulnerabilities, and potential consequences;

''(B) the extent and nature of any cybersecurity incidents during the previous year, including the extent to which cyber incidents jeopardized or imminently jeopardized information systems;

''(C) the current status of the voluntary, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to reduce cyber risks within each critical infrastructure sector; and

''(D) the volume and range of voluntary technical assistance sought and provided by the Department to each critical infrastructure sector.

''(2) SECTOR COORDINATING COUNCIL RESPONSE.—Before making public and submitting each report required under paragraph (1), the Secretary shall provide a draft of each report to the Sector Coordinating Council for the critical infrastructure sector covered by each such report. The Sector Coordinating Council at issue may provide to the Secretary a written response to such report within 45 days of receiving the draft. If such Sector Coordinating Council provides a written response, the Secretary shall include such written response in the final version of each report required under paragraph (1).

''(c) LIMITATION.—Information shared with or provided to a Sector Coordinating Council, a critical infrastructure sector, or the Secretary for the purpose of the activities under subsections (a) and (b) may not be used by any Federal, State, or local government department or agency to regulate the activity of any private entity.''.

(2) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by adding after the item relating to section 229 (as added by section 105) the following new item:

''Sec. 230. Public-private collaboration on cybersecurity.''.

SEC. 202. SAFETY ACT AND QUALIFYING CYBER INCIDENTS.

(a) IN GENERAL.—The Support Anti-Terrorism By Fostering Effective Technologies Act of 2002 (6 U.S.C. 441 et seq.) is amended—

(1) in section 862(b) (6 U.S.C. 441(b))—

(A) in the heading, by striking ''DESIGNATION OF QUALIFIED ANTI-TERRORISM TECHNOLOGIES'' and inserting ''DESIGNATION OF ANTI-TERRORISM AND CYBERSECURITY TECHNOLOGIES'';

(B) in the matter preceding paragraph (1), by inserting ''and cybersecurity'' after ''anti-terrorism'';

(C) in paragraphs (3), (4), and (5), by inserting ''or cybersecurity'' after ''anti-terrorism'' each place it appears; and

(D) in paragraph (7)—

(i) by inserting ''or cybersecurity technology'' after ''Anti-terrorism technology''; and

(ii) by inserting ''or qualifying cyber incidents'' after ''acts of terrorism'';

(2) in section 863 (6 U.S.C. 442)—

(A) by inserting ''or cybersecurity'' after ''anti-terrorism'' each place it appears;

(B) by inserting ''or qualifying cyber incident'' after ''act of terrorism'' each place it appears; and

(C) by inserting ''or qualifying cyber incidents'' after ''acts of terrorism'' each place it appears;

(3) in section 864 (6 U.S.C. 443)—

(A) by inserting ''or cybersecurity'' after ''anti-terrorism'' each place it appears; and

(B) by inserting ''or qualifying cyber incident'' after ''act of terrorism'' each place it appears; and

(4) in section 865 (6 U.S.C. 444)—

(A) in paragraph (1)—

(i) in the heading, by inserting ''OR CYBERSECURITY'' after ''ANTI-TERRORISM'';

(ii) by inserting ''or cybersecurity'' after ''anti-terrorism'';

(iii) by inserting ''or qualifying cyber incidents'' after ''acts of terrorism''; and

(iv) by inserting ''or incidents'' after ''such acts''; and

(B) by adding at the end the following new paragraph:

''(7) QUALIFYING CYBER INCIDENT.—

''(A) IN GENERAL.—The term 'qualifying cyber incident' means any act that the Secretary determines meets the requirements under subparagraph (B), as such requirements are further defined and specified by the Secretary.

''(B) REQUIREMENTS.—A qualifying cyber incident meets the requirements of this subparagraph if—

''(i) the incident is unlawful or otherwise exceeds authorized access authority;

''(ii) the incident disrupts or imminently jeopardizes the integrity, operation, confidentiality, or availability of programmable electronic devices, communication networks, including hardware, software and data that are essential to their reliable operation, electronic storage devices, or any other information system, or the information that system controls, processes, stores, or transmits;

''(iii) the perpetrator of the incident gains access to an information system or a network of information systems resulting in—

''(I) misappropriation or theft of data, assets, information, or intellectual property;

''(II) corruption of data, assets, information, or intellectual property;

''(III) operational disruption; or

''(IV) an adverse effect on such system or network, or the data, assets, information, or intellectual property contained therein; and

''(iv) the incident causes harm inside or outside the United States that results in material levels of damage, disruption, or casualties severely affecting the United States population, infrastructure, economy, or national morale, or Federal, State, local, or tribal government functions.

''(C) RULE OF CONSTRUCTION.—For purposes of clause (iv) of subparagraph (B), the term 'severely' includes any qualifying cyber incident, whether at a local, regional, state, national, international, or tribal level, that affects—

''(i) the United States population, infrastructure, economy, or national morale, or

''(ii) Federal, State, local, or tribal government functions.''.

(b) FUNDING.—Of the amounts authorized to be appropriated for each of fiscal years 2014, 2015, and 2016 for the Department of Homeland Security, the Secretary of Homeland Security is authorized to use not less than $20,000,000 for any such year for the Department's SAFETY Act Office.

SEC. 203. PROHIBITION ON NEW REGULATORY AUTHORITY.

This Act and the amendments made by this Act (except that this section shall not apply in the case of section 202 of this Act and the amendments made by such section 202) do not—

(1) create or authorize the issuance of any new regulations or additional Federal Government regulatory authority; or

(2) permit regulatory actions that would duplicate, conflict with, or supercede regulatory requirements, mandatory standards, or related processes.

SEC. 204. PROHIBITION ON ADDITIONAL AUTHORIZATION OF APPROPRIATIONS.

No additional funds are authorized to be appropriated to carry out this Act and the amendments made by this Act. This Act and such amendments shall be carried out using amounts otherwise available for such purposes.

SEC. 205. PROHIBITION ON COLLECTION ACTIVITIES TO TRACK INDIVIDUALS' PERSONALLY IDENTIFIABLE INFORMATION.

Nothing in this Act shall permit the Department of Homeland Security to engage in the monitoring, surveillance, exfiltration, or other collection activities for the purpose of tracking an individual's personally identifiable information.

SEC. 206. CYBERSECURITY SCHOLARS.

The Secretary of Homeland Security shall determine the feasibility and potential benefit of developing a visiting security researchers program from academia, including cybersecurity scholars at the Department of Homeland Security's Centers of Excellence, as designated by the Secretary, to enhance knowledge with respect to the unique challenges of addressing cyber threats to critical infrastructure. Eligible candidates shall possess necessary security clearances and have a history of working with Federal agencies in matters of national or domestic security.

SEC. 207. NATIONAL RESEARCH COUNCIL STUDY ON THE RESILIENCE AND RELIABILITY OF THE NATION'S POWER GRID.

(a) INDEPENDENT STUDY.—Not later than 60 days after the date of the enactment of this Act, the Secretary of Homeland Security, in coordination with the heads of other departments and agencies, as necessary, shall enter into an agreement with the National Research Council to conduct research of the future resilience and reliability of the Nation's electric power transmission and distribution system. The research under this subsection shall be known as the ''Saving More American Resources Today Study'' or the ''SMART Study''. In conducting such research, the National Research Council shall—

(1) research the options for improving the Nation's ability to expand and strengthen the capabilities of the Nation's power grid, including estimation of the cost, time scale for implementation, and identification of the scale and scope of any potential significant health and environmental impacts;

(2) consider the forces affecting the grid, including technical, economic, regulatory, environmental, and geopolitical factors, and how such forces are likely to affect—

(A) the efficiency, control, reliability and robustness of operation;

(B) the ability of the grid to recover from disruptions, including natural disasters and terrorist attacks;

(C) the ability of the grid to incorporate greater reliance on distributed and intermittent power generation and electricity storage;

(D) the ability of the grid to adapt to changing patterns of demand for electricity; and

(E) the economic and regulatory factors affecting the evolution of the grid;

(3) review Federal, State, industry, and academic research and development programs and identify technological options that could improve the future grid;

(4) review studies and analyses prepared by the North American Electric Reliability Corporation (NERC) regarding the future resilience and reliability of the grid;

(5) review the implications of increased reliance on digital information and control of the power grid for improving reliability, resilience, and congestion and for potentially increasing vulnerability to cyber attack;

(6) review regulatory, industry, and institutional factors and programs affecting the future of the grid;

(7) research the costs and benefits, as well as the strengths and weaknesses, of the options identified under paragraph (1) to address the emerging forces described in paragraph (2) that are shaping the grid;

(8) identify the barriers to realizing the options identified and suggest strategies for overcoming those barriers including suggested actions, priorities, incentives, and possible legislative and executive actions; and

(9) research the ability of the grid to integrate existing and future infrastructure, including utilities, telecommunications lines, highways, and other critical infrastructure.

(b) COOPERATION AND ACCESS TO INFORMATION AND PERSONNEL.—The Secretary shall ensure that the National Research Council receives full and timely cooperation, including full access to information and personnel, from the Department of Homeland Security, the Department of Energy, including the management and operating components of the Departments, and other Federal departments and agencies, as necessary, for the purposes of conducting the study described in subsection (a).

(c) REPORT.—

(1) IN GENERAL.—Not later than 18 months from the date on which the Secretary enters into the agreement with the National Research Council described in subsection (a), the National Research Council shall submit to the Secretary and the Committee on Homeland Security and the Committee on Energy and Commerce of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Energy and Natural Resources of the Senate a report containing the findings of the research required by that subsection.

(2) FORM OF REPORT.—The report under paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

(d) FUNDING.—Of the amounts authorized to be appropriated for 2014 for the Department of Homeland Security, the Secretary of Homeland Security is authorized to obligate and expend not more than $2,000,000 for the National Research Council report.

TITLE III—HOMELAND SECURITY CYBERSECURITY WORKFORCE

SEC. 301. HOMELAND SECURITY CYBERSECURITY WORKFORCE.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002, as amended by sections 101, 102, 103, 104, 105, and 201, is further amended by adding at the end the following new section:

''SEC. 230A. CYBERSECURITY OCCUPATION CATEGORIES, WORKFORCE ASSESSMENT, AND STRATEGY.

''(a) SHORT TITLE.—This section may be cited as the 'Homeland Security Cybersecurity Boots-on-the-Ground Act'.

''(b) CYBERSECURITY OCCUPATION CATEGORIES.—

''(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this section, the Secretary shall develop and issue comprehensive occupation categories for individuals performing activities in furtherance of the cybersecurity mission of the Department.

''(2) APPLICABILITY.—The Secretary shall ensure that the comprehensive occupation categories issued under paragraph (1) are used throughout the Department and are made available to other Federal agencies.

''(c) CYBERSECURITY WORKFORCE ASSESSMENT.—

''(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this section and annually thereafter, the Secretary shall assess the readiness and capacity of the workforce of the Department to meet its cybersecurity mission.

''(2) CONTENTS.—The assessment required under paragraph (1) shall, at a minimum, include the following:

''(A) Information where cybersecurity positions are located within the Department, specified in accordance with the cybersecurity occupation categories issued under subsection (b).

''(B) Information on which cybersecurity positions are—

''(i) performed by—

''(I) permanent full time departmental employees, together with demographic information about such employees' race, ethnicity, gender, disability status, and veterans status;

''(II) individuals employed by independent contractors; and

''(III) individuals employed by other Federal agencies, including the National Security Agency; and

''(ii) vacant.

''(C) The number of individuals hired by the Department pursuant to the authority granted to the Secretary in 2009 to permit the Secretary to fill 1,000 cybersecurity positions across the Department over a three year period, and information on what challenges, if any, were encountered with respect to the implementation of such authority.

''(D) Information on vacancies within the Department's cybersecurity supervisory workforce, from first line supervisory positions through senior departmental cybersecurity positions.

''(E) Information on the percentage of individuals within each cybersecurity occupation category who received essential training to perform their jobs, and in cases in which such training is not received, information on what challenges, if any, were encountered with respect to the provision of such training.

''(F) Information on recruiting costs incurred with respect to efforts to fill cybersecurity positions across the Department in a manner that allows for tracking of overall recruiting and identifying areas for better coordination and leveraging of resources within the Department.

''(d) WORKFORCE STRATEGY.—

''(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this section, the Secretary shall develop, maintain, and, as necessary, update, a comprehensive workforce strategy that enhances the readiness, capacity, training, recruitment, and retention of the cybersecurity workforce of the Department.

''(2) CONTENTS.—The comprehensive workforce strategy developed under paragraph (1) shall include—

''(A) a multiphased recruitment plan, including relating to experienced professionals, members of disadvantaged or underserved communities, the unemployed, and veterans;

''(B) a 5-year implementation plan;

''(C) a 10-year projection of the Department's cybersecurity workforce needs; and

''(D) obstacles impeding the hiring and development of a cybersecurity workforce at the Department.

''(e) INFORMATION SECURITY TRAINING.—Not later than 270 days after the date of the enactment of this section, the Secretary shall establish and maintain a process to verify on an ongoing basis that individuals employed by independent contractors who serve in cybersecurity positions at the Department receive initial and recurrent information security training comprised of general security awareness training necessary to perform their job functions, and role-based security training that is commensurate with assigned responsibilities. The Secretary shall maintain documentation to ensure that training provided to an individual under this subsection meets or exceeds requirements for such individual's job function.

''(f) UPDATES.—The Secretary shall submit to the appropriate congressional committees annual updates regarding the cybersecurity workforce assessment required under subsection (c), information on the progress of carrying out the comprehensive workforce strategy developed under subsection (d), and information on the status of the implementation of the information security training required under subsection (e).

''(g) GAO STUDY.—The Secretary shall provide the Comptroller General of the United States with information on the cybersecurity workforce assessment required under subsection (c) and progress on carrying out the comprehensive workforce strategy developed under subsection (d). The Comptroller General shall submit to the Secretary and the appropriate congressional committees a study on such assessment and strategy.

''(h) CYBERSECURITY FELLOWSHIP PROGRAM.—Not later than 120 days after the date of the enactment of this section, the Secretary shall submit to the appropriate congressional committees a report on the feasibility of establishing a Cybersecurity Fellowship Program to offer a tuition payment plan for undergraduate and doctoral candidates who agree to work for the Department for an agreed-upon period of time.''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by adding after the item relating to section 230 (as added by section 201) the following new item:

''Sec. 230A. Cybersecurity occupation categories, workforce assessment, and strategy.''.

SEC. 302. PERSONNEL AUTHORITIES.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002, as amended by sections 101, 102, 103, 104, 105, 106, 201, and 301 is further amended by adding at the end the following new section:

''SEC. 230B. PERSONNEL AUTHORITIES.

''(a) IN GENERAL.—

''(1) PERSONNEL AUTHORITIES.—The Secretary may exercise with respect to qualified employees of the Department the same authority that the Secretary of Defense has with respect to civilian intelligence personnel and the scholarship program under sections 1601, 1602, 1603, and 2200a of title 10, United States Code, to establish as positions in the excepted service, appoint individuals to such positions, fix pay, and pay a retention bonus to any employee appointed under this section if the Secretary determines that such is needed to retain essential personnel. Before announcing the payment of a bonus under this paragraph, the Secretary 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 written explanation of such determination. Such authority shall be exercised—

''(A) to the same extent and subject to the same conditions and limitations that the Secretary of Defense may exercise such authority with respect to civilian intelligence personnel of the Department of Defense; and

''(B) in a manner consistent with the merit system principles set forth in section 2301 of title 5, United States Code.

''(2) CIVIL SERVICE PROTECTIONS.—Sections 1221 and 2302, and chapter 75 of title 5, United States Code, shall apply to the positions established pursuant to the authorities provided under paragraph (1).

''(3) PLAN FOR EXECUTION OF AUTHORITIES.—Not later than 120 days after the date of the enactment of this section, the Secretary 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 that contains a plan for the use of the authorities provided under this subsection.

''(b) ANNUAL REPORT.—Not later than one year after the date of the enactment of this section and annually thereafter for four years, the Secretary 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 detailed report (including appropriate metrics on actions occurring during the reporting period) that discusses the processes used by the Secretary in implementing this section and accepting applications, assessing candidates, ensuring adherence to veterans' preference, and selecting applicants for vacancies to be filled by a qualified employee.

''(c) DEFINITION OF QUALIFIED EMPLOYEE.—In this section, the term 'qualified employee' means an employee who performs functions relating to the security of Federal civilian information systems, critical infrastructure information systems, or networks of either of such systems.''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by adding after the item relating to section 230A (as added by section 301) the following new item:

''Sec. 230B. Personnel authorities.''.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Texas (Mr. MCCAUL) and the gentlewoman from New York (Ms. CLARKE) 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 may have 5 legislative days in 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 support of H.R. 3696, the National Cybersecurity and Critical Infrastructure Protection Act of 2014. I have worked on this for a long time and introduced this bill with my good friend and colleague, the chairman of the Cybersecurity Subcommittee, the gentleman from Pennsylvania, Congressman PAT MEEHAN. I would also like to thank Ranking Member THOMPSON, as well as Ranking Member CLARKE of the Cybersecurity Subcommittee, for all their hard work in forging this bipartisan bill. These efforts once again prove that we can work together, despite our differences, to craft legislation that improves our national security and helps protect American critical infrastructure from devastating cyber attacks.

Just last week, the Homeland Security Committee heard testimony that we are at a pre-9/11 mindset when it comes to cybersecurity and that the government needs to do a better job at warning the public about the dangers of attacks on networks we rely upon. That was from the 9/11 Commission itself.

Cyber vulnerabilities in our Nation's critical infrastructure are an Achilles heel in our homeland security defenses. Let me be very clear. The cyber threat is real and it is happening right now. The Internet has become the next battlefield for warfare, but unlike land, sea, and air, cyber attacks occur at the speed of light, they are global, and they are more difficult to attribute.

Criminals, hacktivists, terrorists, and nation-state actors such as Russia, China, and Iran are increasingly using malicious malware to hack into U.S. companies for espionage purposes or financial gain, our defense systems to steal our sensitive military information, and our critical infrastructure to gain access to our gas lines, power grids, and water systems.

Iranian hackers, for example, continue to attack the American financial services sector to shut down Web sites and restrict America's access to their bank accounts. Additionally, Iran continues to build more sophisticated cyber weapons to target U.S. energy companies and has demonstrated these capabilities when they attacked Saudi Arabia's national oil company, Aramco, and erased critical files on 30,000 computers. We cannot allow rogue nations like Iran to be able to shut things down and have capabilities that match our defenses. That would be a game-changer for our national security.

The Chinese, in particular, are hacking into major U.S. companies to give their industries competitive economic advantages in our global economy. I applaud the recent efforts taken by the Justice Department for indicting five members of the Chinese government for conducting cyber espionage attacks against U.S. industry, but more needs to be done. Those indictments send a clear message to our adversaries that cyber espionage and theft of American intellectual property, trade secrets, military blueprints, and jobs will not be tolerated.

A recent McAfee and Center for Strategic and International Studies report on the economic impact of cyber crime found an annual effect of roughly $455 billion globally, with 200,000 jobs lost in the United States alone as a result. In fact, former Director of the NSA, General Keith Alexander, described cyber espionage and the loss of American intellectual property and innovation as ''the greatest transfer of wealth in history.''

A recent poll conducted by Defense News revealed that our top Nation's top security analysts see cyber attacks as the greatest threat to our Nation. In fact, Director of National Intelligence, James Clapper, testified earlier this year that: ''Critical infrastructure, particularly the systems used in water management, oil, and gas pipelines, electrical power distribution, and mass transit, provides an enticing target to malicious actors.''

□ 1645

A cyber attack on U.S. critical infrastructure—such as gas pipelines, financial services, transportation, and communication networks—could result in catastrophic regional or national effects on public health or safety, economic security, and national security.

High-profile retail breaches like the ones at Target and Neiman Marcus that compromised the personal information of over 110 million American consumers resonate with Americans, but as bad as those breaches were, a successful cyber attack on our critical infrastructure could cause much more damage in terms of lives lost and monetary damage. We cannot and will not wait for a catastrophic 9/11-scaled cyber attack to occur before moving greatly needed cybersecurity legislation.

The National Cybersecurity and Critical Infrastructure Protection Act ensures that DHS and not the military is responsible for domestic critical infrastructure protection.

Specifically, H.R. 3696 ensures that there is a ''civilian interface'' to the private sector to share real-time cyber threat information across the critical infrastructure sectors, particularly in light of the Snowden revelations.

Importantly, the bill protects civil liberties by putting a civilian agency with the Nation's most robust privacy and civil liberties office in charge of preventing personal information from being shared. While also prohibiting any new regulatory authority, this bill builds upon the groundwork already laid by industry and DHS to facilitate critical infrastructure protection and incidence response efforts.

This bipartisan bill, which is rare in this day and age, Mr. Speaker, is a product of 19 months of extensive outreach and great collaboration with all stakeholders, including more than 300 meetings with experts, industry, government agencies, academics, privacy advocates, and other committees of jurisdiction.

We went through several drafts and countless hours of negotiations to bring this commonsense legislation to the floor with support from all of the critical infrastructure sectors.

I will enter in the RECORD some of the letters of support, representing over 33 trade associations from across industry sectors, U.S. businesses, national security experts, and privacy and civil liberty advocates.

Specifically, we have received support letters from the American Civil Liberties Union, the American Chemistry Council, AT&T, Boeing, Con Edison, the Depository Trust and Clearing Corporation, GridWise Alliance, and multiple trade associations in the energy sector and the financial services sector, Information Technology Industry Council, the Internet Security Alliance, Rapid7, National Defense Industrial Association, Professional Services Council, Oracle, Entergy, Pepco, Verizon, and Symantec.

I believe that is a very impressive showing on behalf of the privacy advocates and also the private sector.

AMERICAN CIVIL LIBERTIES UNION,
January 14, 2014.

Re H.R. 3696, the ''National Cybersecurity and Critical Infrastructure Protection Act of 2013'' (NCCIP Act)

Hon. MICHAEL MCCAUL, Chairman,
Hon. BENNIE THOMPSON, Ranking Member,
Hon. PATRICK MEEHAN, Subcommittee Chairman,
Hon. YVETTE CLARKE, Subcommittee Ranking Member,
House Homeland Security Committee, Washington, DC.

DEAR CHAIRMEN AND RANKING MEMBERS: On behalf of the American Civil Liberties Union (ACLU), its over half a million members, countless additional supporters and activists, and 53 affiliates nationwide, we write in regard to H.R. 3696, the National Cybersecurity and Critical Infrastructure Protection Act of 2013 (NCCIP Act). We have reviewed this legislation and have found that information sharing provisions in this bill do not undermine current privacy laws.

As we testified before the Committee last year, it is crucial that civilian agencies like the Department of Homeland Security lead domestic cybersecurity efforts and the NCCIP Act makes strides towards that end. The bill directs DHS to coordinate cybersecurity efforts among non-intelligence government agencies and critical infrastructure entities. The NCCIP Act smartly does that by focusing on coordination and information sharing within current law and leveraging existing structures that have proven successful in the past. Unlike H.R. 624, the Cyber Intelligence Sharing and Protection Act (CISPA), your bill does not create broad exceptions to the privacy laws for cybersecurity. Instead, it strengthens private-public partnerships by supporting existing Information Sharing and Analysis Centers and Sector Coordinating Councils and reinforces voluntary sharing under current statutes that already provide for many cybersecurity scenarios.

We commend the Committee for advancing cyber legislation that is both pro-security and pro-privacy and we look forward to working with you further on this matter. Please contact Michelle Richardson, Legislative Counsel, at 202–715–0825 or mrichardson@aclu.org for more information.

Sincerely,

LAURA W. MURPHY,
Director,
MICHELLE RICHARDSON,
Legislative Counsel.

AMERICAN GAS ASSOCIATION, EDISON ELECTRIC INSTITUTE, AMERICAN PUBLIC POWER ASSOCIATION, NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION,
January 8, 2014.

Hon. MICHAEL MCCAUL,
Chairman, House Committee on Homeland Security, Washington, DC.
Hon. BENNIE G. THOMPSON,
Ranking Member, House Committee on Homeland Security, Washington, DC.

DEAR CHAIRMAN MCCAUL AND RANKING MEMBER THOMPSON: We write to thank you and your colleagues for your outreach in drafting H.R. 3696, the ''National Cybersecurity and Critical Infrastructure Protection Act of 2013'' (the ''NCCIP Act'').

Like you, we are very focused on protecting the nation's critical energy infrastructure from the impacts of a cyber event. While thankfully the nation has yet to experience a cyber attack that has damaged infrastructure, we appreciate that the House

Committee on Homeland Security has taken the time and effort to craft legislation that attempts to help address the preparedness for and response to such events should they occur in the future.

The undersigned associations represent the vast majority of electric and gas utilities. We are proud of the efforts our members have undertaken, collectively and individually, to improve the reliability and resiliency of their systems. In the gas sector, this encompasses a variety of public, private and, jointly developed public-private sector cybersecurity standards designed to protect pipeline infrastructure and ensure safe and reliable gas delivery. In the electric sector, this includes mandatory and enforceable cybersecurity standards already in place. Developed by the North American Electric Reliability Corporation for review and approval by the Federal Energy Regulatory Commission and applicable Canadian governmental authorities, these standards ensure that owners, users, and operators of the North American bulk electric system meet a baseline level of security.

Even considering those measures, the issue of liability after a cyber event creates serious concerns for us and our members. In particular, we are deeply concerned that no matter what steps are taken, our members could face costly and unnecessary litigation in state or federal courts after a cyber event that would serve no purpose.

Therefore, we applaud Section II of the NCCIP Act, specifically the section seeking to clarify the scope of the Support Anti-Terrorism By Fostering Effective Technologies Act of 2002 (the ''SAFETY Act''). The language of the SAFETY Act statute as well as its Final Rule have always made clear that the protections offered by the law applies to cyber events, and indeed that the SAFETY Act applies regardless of whether a ''terrorist'' group conducted such an attack. However, in practice there has been some hesitancy on the part of industry to utilize the SAFETY Act to protect against federal claims arising out of cyber attacks due to the requirement that the attack be deemed an ''act of terrorism'' by the Secretary of Homeland Security before liability protections become available.

The decision to include in H.R. 3696 a provision that explicitly allows the Secretary of Homeland Security to declare that a ''qualifying cyber incident'' triggers the liability protections of the SAFETY Act is an excellent one. Removing the need to link a cyber attack to an ''act of terrorism'' is a good step. While state liability actions remain a concern, the industry and vendors of cyber security technologies and services will be much more likely to use the SAFETY Act program, thereby fulfilling the law's original intent of promoting the widespread deployment of products and services that can deter, defend against, respond to, mitigate, defeat, or otherwise mitigate a variety of malicious events, including those related to cyber security.

We share your goal of protecting the nation's critical infrastructure from cyber threats and appreciate your efforts to address this important national security issue. We look forward to continuing to work together to ensure H.R. 3696 remains focused on these principles as it moves through the legislative process.

Respectfully,

AMERICAN GAS ASSOCIATION,
AMERICAN PUBLIC POWER ASSOCIATION,
EDISON ELECTRIC INSTITUTE,
NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION.

AT&T SERVICES, INC.,
Washington, DC, January 8, 2014.

Hon. MICHAEL T. MCCAUL,
Chairman, Committee on Homeland Security, Washington, DC.

DEAR CHAIRMAN MCCAUL: We applaud you and your staff for working so hard to update and streamline the Homeland Security Act of 2002 to address today's cyber security challenges. In your efforts to update the important role of the Department of Homeland Security within the national policy framework for critical infrastructure protection, you and your staff have actively listened to multiple stakeholder concerns to ensure that the best aspects of existing private public partnerships, which are the hallmark of our nation's efforts to address cyber threats, remain as such.

Your bill joins other important items introduced by your colleagues in the 113th Congress. We look forward to continuing to work with you and your colleagues to forge a bipartisan legislative framework for the practice of cybersecurity in the coming decade that encourages continued private sector investment in innovation and cyber education and provides legal clarity in the day-to-day operational world of identifying and addressing cyber threats in a globally interconnected network of networks.

Sincerely,

TIMOTHY P. MCKONE.

JANUARY 13, 2014.

Hon. MICHAEL MCCAUL,
Chairman, Committee on Homeland Security, U.S. House of Representatives, Washington, DC.

Hon. BENNIE THOMPSON,
Ranking Member, Committee on Homeland Security, U.S. House of Representatives, Washington, DC.

DEAR CHAIRMAN MCCAUL AND RANKING MEMBER THOMPSON: The undersigned organizations, representing the financial services industry, appreciate your efforts to introduce H.R. 3696, the National Cybersecurity and Critical Infrastructure Protection Act. We welcome your leadership in this crucial fight against cyber threats and your work in forging this commonsense, bipartisan legislation.

While Congress considers much needed legislative action, our associations and the financial services industry have taken major steps to address the cybersecurity threats facing the Nation's critical infrastructure. The financial services sector continues to invest in our infrastructure, has improved coordination among institutions of all sizes, and is continually enhancing our partnerships with government.

H.R. 3696 recognizes the necessary partnership between the private and public sectors that is required to better protect our Nation's cybersecurity infrastructure. Among other provisions, this bill would strengthen existing mechanisms such as the Financial Services Sector Coordinating Council (FSSCC) and the Financial Services Information Sharing and Analysis Center (FS–ISAC) that help our sector identify threats, respond to cyber incidents and coordinate with government partners. These organizations work closely with partners throughout the government, including our sector specific agency, the Department of Treasury, as well as the Department of Homeland Security. Each agency has a civilian mission and plays a unique role in sector cybersecurity efforts and both work to strengthen the sector's understanding of the threat environment.

Additionally H.R. 3696 seeks to improve the provisioning of security clearances for those involved in cybersecurity information sharing. Your recognition that this is a system that demands improvement is strongly supported by our industry and we further encourage the expansion of this to specifically include individuals within critical infrastructure responsible for key aspects of network defense or mitigation. It is essential that all sizes of institutions within critical infrastructure receive access to classified threat information in a timely manner.

Finally, H.R. 3696 expands the existing Support Anti-Terrorism by Fostering Effective Technologies Act (SAFETY Act) to provide important legal liability protections for providers and users of certified cybersecurity technology in the event of a qualified Cybersecurity incident. We urge Congress to work with the Department of Homeland Security to ensure that, should this provision be adopted, the expanded SAFETY Act is implemented in a manner that does not duplicate or conflict with existing regulatory requirements, mandatory standards, or the evolving voluntary National Institute for Standards and Technology (NIST) Cybersecurity Framework. An expansion of the program must be coupled with additional funding to enable DHS to handle the increased scope of program and subsequent increase in applicants. Further, it is incumbent that an expansion enables DHS to streamline its SAFETY Act review and approval process so as not to discourage participation in the program.

Our sector has actively engaged in the implementation of Executive Order 13636 and the development by the National Institute of Standards and Technology of a Cybersecurity Framework. We believe the process outlined in H.R. 3696 should reflect the Framework developed through this cross-sector collaborative process.

Each of our organizations and respective member firms have made cybersecurity a top priority. We are committed to working with you as you lead in this crucial fight for cybersecurity of critical infrastructure.

American Bankers Association, The Clearing House, Consumer Bankers Association, Credit Union National Association (CUNA), Electronic Funds Transfer Association, Financial Services—Information Sharing and Analysis Center (FS–ISAC), Financial Services Roundtable, Independent Community Bankers Association (ICBA) Investment Company Institute, NACHA—The Electronic Payments Association, National Association of Federal Credit Unions (NAFCU), Securities Industry and Financial Markets Association (SIFMA).

Mr. MCCAUL. I want to give a great deal of thanks not only to the Members involved, but to the staff on this committee on both sides of the aisle who have worked countless hours to bring this bill to its fruition on the floor of the House.

I also would like to bring special attention to the endorsement from the ACLU. They refer to H.R. 3696 as ''both pro-security and pro-privacy.'' When have we heard these two coming together?

Striking a balance between security and privacy, I believe, is one of the most difficult challenges in developing cybersecurity legislation, and I am so very proud that this committee and this bill achieves that goal.

I want to close with the threat that I see out there from cyber. People ask me: What keeps you up at night? We can talk about al Qaeda, Mr. Putin, or

ISIS in Iraq and Syria, we can talk about our border and the threats south of the border, but when I see our offensive capability and what we can do offensively, knowing at night that we don't have the defensive capability to stop attacks not only to steal things, not only criminal IP theft, not just espionage, but the power to shut things down and to bring this country to its knees with a cyber 9/11, Mr. Speaker, is really what keeps me up at night.

My father was a World War II bombardier on a B–17. He flew over 32 missions in Europe in support of the D-day invasion and the Battle of the Bulge. In his days, bombs won that war.

We have a new kind of warfare out there. It is a digital warfare, and the game has changed. It is done anonymously. There are no boundaries to this cyber threat any more. It can come from anywhere, at any time, without being able to attribute it back to the source from where the attack came from.

This bill will for the first time codify DHS' ability—and the NCCIC, which is their cyber command, to better defend and support critical infrastructure in the United States that we so heavily depend on, and it will ultimately protect not only our economy and our infrastructure, but ultimately protect the American people.

With that, Mr. Speaker, I ask my colleagues to support this important legislation to protect America, and I reserve the balance of my time.

Ms. CLARKE of New York. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I rise in strong support of H.R. 3696, the National Cybersecurity and Critical Infrastructure Protection Act of 2014, and I am pleased to be here today as an original cosponsor of this legislation.

This bipartisan legislation gives the Department of Homeland Security the legislative authority it needs to carry out its cyber mission and to help protect our Nation's critical infrastructure from cyber attacks and intrusions.

The approach taken in this bill is very much in line with DHS' approach since 2007, when President Bush designated the Department as the lead Federal civilian agency for cybersecurity.

This is a dual mission. DHS is responsible for working with Federal civilian agencies to protect Federal IT networks and the dot-gov domain. At the same time, DHS is responsible for effectively partnering with the private sector to raise its level of cyber hygiene and foster greater cybersecurity.

I am pleased that H.R. 3696 authorizes the 247 operations of the National Cybersecurity and Communications Integration Center, also referred to as NCCIC. The NCCIC has been the epicenter for information sharing about the activities of cyberterrorists and criminals and the reporting of cyber incidents by critical infrastructure owners and operators.

Additionally, the bill codifies ongoing efforts to raise the level of cybersecurity within critical infrastructure sectors. Specifically, it authorizes the development and implementation, in coordination with the private sector, of voluntary risk-based security standards.

This provision essentially codifies the process that the National Institute of Standards and Technology, also known as NIST, undertook pursuant to an executive order that President Obama issued in February of 2013.

Under the approach taken in this bill, we are asking business and government to come together to find an adaptable and cooperative cybersecurity framework, not an off-the-shelf or check-the-box solution, to raise the level of cybersecurity across the Nation.

I am pleased that the measured and targeted approach taken to working with the private sector was supported by the American Civil Liberties Union, which called our bill ''pro-security and pro-privacy.''

The President said it best:

> It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.

While I am also pleased about all we do with respect to the Department's mission to work with the private sector on cybersecurity, I am a bit disappointed that key language that clarifies DHS' roles with respect to other Federal agencies and protection of the dot-gov domain is not in the bill before you today.

Unfortunately, the striking of these provisions appears to have been the price the Committee on Homeland Security had to pay to get this important legislation to the floor.

It seems that the provisions that would have given DHS specific authority to respond in a more timely manner to Federal network breaches were opposed by another committee chairman. Unfortunately, that chairman has willfully chosen to ignore reality.

The reality is that since 2008, DHS has assumed responsibility for working with agencies to protect the dot-gov domain, not the Office of Management and Budget.

It is my hope that, as this legislation moves through the legislative process, there will be progress on efforts to ensure that the law reflects this reality.

With that, Mr. Speaker, I urge passage of H.R. 3696, and I reserve the balance of my time.

Mr. MCCAUL. Mr. Speaker, I yield such time as he may consume to the gentleman from Pennsylvania (Mr. MEEHAN), chairman of the Committee on Homeland Security's Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, who has spent, I must say, countless hours advancing this bill, meeting with the private sector and privacy groups to get to this point where we are today.

I want to commend you, sir, for a job well done.

Mr. MEEHAN. I want to thank the gentleman from Texas and my colleagues from both sides of the aisle.

Mr. Speaker, I rise in strong support of H.R. 3696, the National Cybersecurity and Critical Infrastructure Protection Act of 2014.

Before I really talk about the substance, I want to associate myself for a moment with the comments and very effective commentary of the gentleman from Texas (Mr. MCCAUL), but his closing, I think, really summed it up. It is not just what we are doing; but why does this matter? Why does this matter now?

We have generated tremendous economic prosperity by virtue of the creation of a global Internet, but the fact of the matter is that while this has closed our world and enabled instantaneous communications and other kinds of benefits, it has also created a situation, for the first time in the history of our Nation, in which we aren't protected by two oceans and, effectively, two friendly countries on our borders. Now, we are able to be accessed from anywhere in the world at a moment's notice.

It was instructive to me that I often used to say, when we were handling a case, that you let the evidence be put in through the words of the witnesses. If you pay attention to the words of the witness, that is more powerful than what you can say.

It is instructive to me that the first thing former CIA Director and former Secretary of Defense Leon Panetta did when he stepped down as Secretary of Defense was to travel to New York and warn not just New York, but this Nation about the potential impact of what he termed a ''cyber Pearl Harbor.''

As a result, this is a critically important and timely issue that we are working on. As importantly, it has been addressed in an effective bipartisan fashion.

In the wake of more aggressive and escalating cyber attacks on our Nation's critical infrastructure, including our financial systems, NASDAQ, and the recent Neiman Marcus and Target breaches of Americans' personal information, we bring H.R. 3696 to the House floor.

□ 1700

Cyber attacks and cyber hacks are now front and center in our homeland, and the media is reporting more now than ever on what cyber targets already know—that the threat is constant and evolving.

Americans expect Congress to act.

We who serve in Congress and government know all too well that the cyber threat is real and imminent and can do catastrophic damage and destruction to the critical infrastructure of our Nation—our bridges, tunnels, oil

and gas pipelines, water systems, financial systems and their markets, air traffic control systems, and more. Today, the U.S. House of Representatives takes a significant step forward in protecting and securing cyberspace through the cyber infrastructure act that we have put on the floor today.

I am very proud of this bill and of all of the good work and due diligence that went into it. Chairman MCCAUL and I and our staffs held over 300 stakeholder meetings to ensure we got this legislation right.

I want to thank as well my good friends on the other side of the aisle—Ranking Member BENNIE THOMPSON and subcommittee Ranking Member YVETTE CLARKE—for their leadership and their work collectively on this.

This is bipartisan legislation but not just amongst those of us working together here within the House. As the chairman identified, it has also been supported by private sector stakeholders, by the ACLU. In fact, the ACLU has called it—and the chairman as well—pro-security and pro-privacy. That is because, very notably, this bill puts the Department of Homeland Security, a civilian agency with the Nation's first-created and most robust privacy office, in charge of preventing personal information from getting inadvertently caught in the net, which is a big, important part of the work that has been done here.

This bill builds upon the Department of Homeland Security's unique public-private partnership in securing the Nation's critical infrastructure, and it codifies the Department's critical cybersecurity mission. Public-private is important, as 90 percent of the assets in the cyber world are in the private sector. The Department of Homeland Security works with the other Federal Government partners in a collaborative effort to secure our Nation against cyber attacks, and this bill cements DHS' critical role.

Specifically, this bill requires the Department to collaborate with industry to facilitate both the protection of our infrastructure and our response to a cyber attack. The bill, very importantly, strengthens DHS' civilian, transparent interface to allow real-time cyber threat sharing across the critical infrastructure sectors. This legislation also strengthens the integrity of our Nation's information systems, and it makes it more difficult for online hackers to compromise consumer and personal information, like we saw in Target, and it prevents hackers from stealing Americans' business and intellectual property—another point well driven home by the chairman in talking about jobs and of the hundreds of billions of dollars in research and development that are stolen from America by virtue of these cyber attacks.

The ability of these attacks to take place at the level of sophistication necessary to penetrate some of the world's most mature networks should come as no surprise. Foreign adversaries, including China, Iran, and Russian criminal enterprises, have spent years and have invested billions of dollars into crafting and securing the tools and intelligence necessary to target American citizens. Whether it is the theft of wealth or intelligence or that of launching a malicious attack on our Nation's energy, transportation, or chemical networks, American lives and livelihoods remain at risk without sufficient security.

Last year, President Obama issued an executive order on cybersecurity because Congress failed to act on this issue, but the threshold of securing our Nation in the 21st century cannot rely on executive orders and Presidential directives. As Members of Congress, we have the responsibility to act in a way that best protects the American citizens. Our enemies live and breathe to catch us asleep at the switch, and I am unwilling, as my colleagues are, to stand by, speechless, when they are asked, What did you do to prevent a cyber attack? Now is the time to show them what we have and what we can do.

This bill doesn't address every issue in cybersecurity, and it is not a comprehensive cybersecurity fix, but it is a giant and critical step forward. Together, we can unite our Nation against those who wish to do us harm, and I have no doubt that we can get it done. In fact, we have no other choice. I urge the support of H.R. 3696.

Mr. MCCAUL. Mr. Speaker, I have no further requests for time. I believe the gentlewoman from New York has a few additional speakers, so I am prepared to close once the gentlewoman does.

I continue to reserve the balance of my time.

Ms. CLARKE of New York. Mr. Speaker, I yield 2 minutes to the distinguished gentleman from New Jersey (Mr. PAYNE).

Mr. PAYNE. Mr. Speaker, I rise in support of H.R. 3696, the National Cybersecurity and Critical Infrastructure Protection Act.

In October of 2012, Hurricane Sandy wreaked havoc up and down the east coast, including in my home State of New Jersey. According to the Department of Energy, between 2003 and 2012, close to 700 power outages occurred due to weather-related events, costing the Nation an annual average of $18 billion to $33 billion. Even worse, in 2012, Hurricane Sandy carried an estimated price tag of between $40 billion and $52 billion, and as we have seen recently, our power systems are exposed to cyber attacks more than ever before.

Disasters, whether manmade or by Mother Nature, are a drain on our Nation's economy and expose us to other potentially more harmful attacks on our financial industry, water and waste systems, chemical, telecommunications, and energy sectors. Put simply, it is clear that our electric grid needs an upgrade. That is why I am pleased that, during the committee process, the committee unanimously supported my amendment, H.R. 2962, the SMART Grid Study Act.

The study will be conducted by the National Research Council in full cooperation with the Department of Homeland Security and other government agencies as necessary, and will provide a comprehensive assessment of actions necessary to expand and strengthen the capabilities of the electric grid to prepare for, respond to, mitigate, and recover from a natural disaster or a cyber attack. Further, it was supported by the National Electrical Manufacturers Association, the Demand Response and Smart Grid Coalition, and the American Public Power Association.

The SPEAKER pro tempore. The time of the gentleman has expired.

Ms. CLARKE of New York. I yield the gentleman an additional 1 minute.

Mr. PAYNE. Mr. Speaker, in closing, I want to thank Chairman MCCAUL and Ranking Member THOMPSON, Chairman MEEHAN, and Ranking Member CLARKE for really showing us what a bipartisan effort is all about. At Homeland Security, we all have a common goal, which is to keep the homeland and the Nation safe. I urge my colleagues to support this bill.

Ms. CLARKE of New York. Mr. Speaker, I yield 2 minutes to the distinguished gentleman from Rhode Island (Mr. LANGEVIN), the cochair of the House Cybersecurity Caucus.

(Mr. LANGEVIN asked and was given permission to revise and extend his remarks.)

Mr. LANGEVIN. I thank the gentlewoman for yielding.

Mr. Speaker, I rise in strong support of H.R. 3696, H.R. 2952, and H.R. 3107.

I want to thank Ranking Member THOMPSON, Chairman MEEHAN, and Ranking Member CLARKE for their hard work in bringing these bills to the floor today.

Most especially and in particular, I want to thank Chairman MCCAUL, the chairman of the full Homeland Security Committee, who also serves with me as a founder and a cochair of the Congressional Cybersecurity Caucus. I want to thank him for his dedication to bringing these bills to the floor today and for his commitment to enacting strong cybersecurity legislation. In today's political climate, moving significant reform in a consensus manner is exceptionally difficult, and this success reflects Chairman MCCAUL's bipartisan approach.

Mr. Speaker, we all know that we depend on cyberspace and the Internet every day. It is vitally important to the American people. It is an inseparable part of our everyday lives. It is in everything that we do—vital to everything from banking to national security—but it is also highly contested. Unfortunately, the pace of the threats is ever-increasing. We see them every day, whether it is the theft of personal information or of credit card information that is used for criminal intent or

whether it is the theft of intellectual property that costs America its competitiveness and jobs. We also know of the threats to our critical infrastructure in particular, both to our electric grid and to our financial system—things that I have been calling attention to for years now.

We must tap into our creative and innovative spirit to address today's challenges and position ourselves to be agile in the face of both today's threats as well as tomorrow's. I believe that the three bills that are before us today, in conjunction with the information sharing and other measures passed by this House earlier in this Congress, will help to enable a better future for our Nation's cyberspace capabilities.

I know, Mr. Speaker, that we will never be 100 percent secure in cyberspace. It is an ever-evolving and moving threat, and we will never be 100 percent secure. Yet I do know this: that we can close that aperture of vulnerability down to something that is much more manageable, and I urge my colleagues to support the bills that are before us today.

I thank the gentleman from Texas for his leadership, and I strongly urge the support of these three bills.

Ms. CLARKE of New York. Mr. Speaker, I have no more speakers. If the gentleman from Texas has no more speakers, then, in closing, I urge the passage of H.R. 3696. It is legislation that will enhance DHS' ability to execute its cybersecurity mission. I am particularly pleased that it includes language that I authored to help ensure that DHS has the cyber workforce it needs to execute that mission.

I would like to thank Chairman MCCAUL and Ranking Member THOMPSON, as well as the subcommittee chair, Mr. MEEHAN, for their leadership and their vision, and for their understanding that this is something that keeps us up at night, that this is something that this body must move forward to address—that this is a 21st century threat for which we cannot sit idly by and do nothing about. Their leadership on H.R. 3696 and on the suite of cyber legislation on the floor today speaks volumes to moving us in the right direction.

With that, Mr. Speaker, I urge the passage of H.R. 3696, and I yield back the balance of my time.

Mr. MCCAUL. Mr. Speaker, in closing, let me echo the sentiments of the gentlewoman from New York.

I want to thank you and Mr. MEEHAN for your work on this bill. You are truly the workhorses—the engines—behind this bill, and I want to thank you for helping us get to this point where we are today.

Congressman LANGEVIN, we were talking about cybersecurity before it was cool to talk about cybersecurity.

Forming the Cybersecurity Caucus, I think, raises awareness of Members of Congress about how important this issue really is, because, I think, when you talk about this issue, Mr. Speaker, people's eyes tend to glaze over. They don't understand how important this is in protecting the American people.

This is a national security bill. I don't believe partisan politics has a place in that. I was at The Aspen Institute with Jane Harman, who served on our committee and on the Intelligence Committee for many years, who also believes that our adversaries don't care whether we are Democrat or Republican. They care about the fact that we are Americans, and they want to hit us. We have adversaries who want to hit us—China, Russia, Iran, and countless others—in the cybersecurity space.

This is a pro-security and pro-privacy bill. I had a reporter ask me, How could you possibly get the ACLU to agree on any security bill? It protects Americans' privacy but also their security through the private civilian interface to the private sector, and that is how we do it. It is not through the military. The NSA has a foreign intelligence role, and the DHS has a domestic critical infrastructure role. Of course, Director Alexander called cybersecurity and what has happened in recent years the largest transfer of wealth in history.

□ 1715

So when the American people say: Why is this so important; the largest transfer of wealth in American history? Why is this so important? Because cyber can bring down things, can shut down things in a 9/11 style.

We have a historical moment in this Congress to pass the first cybersecurity bill through the House and Senate and be signed into law in the history of the Congress. As this bill passes—I hope, in a few minutes—and we send it over to the Senate, I hope our colleagues on the Senate side will respond to this.

They have made great progress on the Senate side in getting work done on cybersecurity. We have a unique opportunity and a great moment here to pass this bill out of the House, get it married with the Senate bill in a bipartisan way to protect the American people, and get it signed into law by the President, something that we very rarely have seen in this Congress. So I think it is a very historic moment.

To close, Mr. Speaker, when 9/11 happened, a lot of people did a lot of finger pointing around here and pointed to Members of Congress and to the executive branch and said: What did you do to stop this? What did you do to stop this?

We had a 9/11 Commission that pointed out all the vulnerabilities and the things that we didn't do as Members of Congress. I don't want that to happen again today. I want to be able to say, Mr. Speaker, if, God forbid, we get hit, and we get hit hard in a cyber attack against the United States of America, that we as Members of Congress and members of this committee did everything within our power to stop it.

Mr. Speaker, I am proud of the great work we have done together. I look forward to the passage of this bill.

I yield back the balance of my time.

HOUSE OF REPRESENTATIVES, COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,

Washington, DC, February 24, 2014.

Hon. MICHAEL MCCAUL,
Chairman, Committee on Homeland Security, Washington, DC.

DEAR CHAIRMAN MCCAUL: I am writing to you concerning the jurisdictional interest of the Committee on Science, Space, and Technology in H.R. 3696, the ''National Cybersecurity and Critical Infrastructure Protection Act of 2013.'' The bill contains provisions that fall within the jurisdiction of the Committee on Science, Space, and Technology.

I recognize and appreciate the desire to bring this legislation before the House of Representatives in an expeditious manner, and accordingly, I will waive further consideration of this bill in Committee, notwithstanding any provisions that fall within the jurisdiction of the Committee on Science, Space, and Technology. This waiver, of course, is conditional on our mutual understanding that agreeing to waive consideration of this bill should not be construed as waiving, reducing, or affecting the jurisdiction of the Committee on Science, Space, and Technology.

This waiver is also given with the understanding that the Committee on Science, Space, and Technology expressly reserves its authority to seek conferees on any provision within its jurisdiction during any House-Senate conference that may be convened on this, or any similar legislation. I ask for your commitment to support any request by the Committee for conferees on H.R. 3696 as well as any similar or related legislation.

I ask that a copy of this letter and your response be included in the report on H.R. 3696 and also be placed in the Congressional Record during consideration of this bill on the House floor.

Sincerely,

LAMAR SMITH,
Chairman, Committee on Science, Space, and Technology.

HOUSE OF REPRESENTATIVES, COMMITTEE ON HOMELAND SECURITY

Washington, DC, February 24, 2014.

Hon. LAMAR SMITH,
Chairman, Committee on Science, Space, and Technology, Washington, DC.

DEAR CHAIRMAN SMITH: Thank you for your letter regarding H.R. 3696, the ''National Cybersecurity and Critical Infrastructure Protection Act of 2014.'' I acknowledge your Committee's jurisdictional interest in this legislation and agree that by forgoing a sequential referral on this legislation, your Committee is not diminishing or altering its jurisdiction.

I also concur with you that forgoing action on H.R. 3696 does not in any way prejudice the Committee on Science, Space, and Technology with respect to 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 to any House-Senate conference involving H.R. 3696 or similar legislation.

Finally, I will include your letter and this response in the report accompanying H.R. 3696 as well as the Congressional Record during consideration of this bill on the House floor. I appreciate your cooperation regarding this legislation, and I look forward to working with the Committee on Science, Space, and Technology as H.R. 3696 moves through the legislative process.

Sincerely,

MICHAEL T. MCCAUL,
Chairman.

HOUSE OF REPRESENTATIVES, COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, DC, July 23, 2014.

Hon. MICHAEL MCCAUL,
Chairman, Committee on Homeland Security, Washington, DC.

DEAR MR. CHAIRMAN: I am writing concerning H.R. 3696, the ''National Cybersecurity and Critical Infrastructure Protection Act of 2013,'' which your Committee reported on February 5, 2014.

H.R. 3696 contains provisions within the Committee on Oversight and Government Reform's Rule X jurisdiction. As a result of your having consulted with the Committee, and in order to expedite this bill for floor consideration, the Committee on Oversight and Government Reform will forego action on the bill, contingent on the removal of subsection (h) ''Protection of Federal Civilian Information Systems,'' (beginning at line 17 of page 23 of the reported version). This is being done on the basis of our mutual understanding that doing so will in no way diminish or alter the jurisdiction of the Committee on Oversight and Government Reform with respect to the appointment of conferees, or to any future jurisdictional claim over the subject matters contained in the bill or similar legislation.

I would appreciate your response to this letter confirming this understanding, and would request that you include a copy of this letter and your response in the Committee Report and in the Congressional Record during the floor consideration of this bill. Thank you in advance for your cooperation.

Sincerely,

DARRELL ISSA,
Chairman.

HOUSE OF REPRESENTATIVES, COMMITTEE ON HOMELAND SECURITY,
Washington, DC, July 23, 2014.

Hon. DARRELL E. ISSA,
Chairman, Committee on Oversight and Government Reform, Washington, DC.

DEAR CHAIRMAN ISSA: Thank you for your letter regarding the Committee on the Oversight and Government Reform's jurisdictional interest in H.R. 3696, the ''National Cybersecurity and Critical Infrastructure Protection Act of 2013.'' I acknowledge that by foregoing further action on this legislation, your Committee is not diminishing or altering its jurisdiction.

I also concur with you that forgoing action on this bill does not in any way prejudice the Committee on Oversight and Government Reform with respect to its jurisdictional prerogatives on this bill or similar legislation in the future. Moving forward, subsection (h), referred to in your letter, will be removed from H.R. 3696 prior to consideration on the House floor. As you have requested, I would support your effort to seek an appointment of an appropriate number of conferees to any House-Senate conference involving this or similar legislation.

Finally, I will include your letter and this response in the report accompanying H.R. 3696 and in the Congressional Record during consideration of this bill on the House floor. I appreciate your cooperation regarding this legislation, and I look forward to working with the Committee on Oversight and Government Reform as H.R. 3696 moves through the legislative process.

Sincerely,

MICHAEL T. MCCAUL,
Chairman.

HOUSE OF REPRESENTATIVES, COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC, July 22, 2014.

Hon. MICHAEL T. MCCAUL,
Chairman, Committee on Homeland Security, Washington, DC.

DEAR CHAIRMAN MCCAUL: I write concerning H.R. 3696, the ''National Cybersecurity and Critical Infrastructure Protection Act of 2014.'' As you are aware, the bill was referred primarily to the Committee on Homeland Security, but the Committee on Energy and Commerce has a jurisdictional interest in the bill and has requested a sequential referral.

However, given your desire to bring this legislation before the House in an expeditious manner, I will not insist on a sequential referral of H.R. 3696. I do so with the understanding that, by foregoing such a referral, the Committee on Energy and Commerce does not waive any jurisdictional claim on this or similar matters, and the Committee reserves the right to seek the appointment of conferees.

I would appreciate your response to this letter confirming this understanding, and ask that a copy of our exchange of letters on this matter be included in the Congressional Record during consideration of H.R. 3696 on the House floor.

Sincerely,

FRED UPTON,
Chairman.

HOUSE OF REPRESENTATIVES, COMMITTEE ON HOMELAND SECURITY,
Washington, DC, July 23, 2014.

Hon. FRED UPTON,
Chairman, Committee on Energy and Commerce, Washington, DC.

DEAR CHAIRMAN UPTON: Thank you for your letter regarding the Committee on Energy and Commerce's jurisdictional interest in H.R. 3696, the ''National Cybersecurity and Critical Infrastructure Protection Act of 2014.'' I acknowledge that by foregoing a sequential referral on this legislation, your Committee is not diminishing or altering its jurisdiction.

I also concur with you that forgoing action on this bill does not in any way prejudice the Committee on Energy and Commerce with respect to its jurisdictional prerogatives on this bill or similar legislation in the future, and I would support your effort to seek an appointment of an appropriate number of conferees to any House-Senate conference involving this or similar legislation.

Finally, I will include your letter and this response in the Congressional Record during consideration of this bill on the House floor. I appreciate your cooperation regarding this legislation, and I look forward to working with the Committee on Energy and Commerce as H.R. 3696 moves through the legislative process.

Sincerely,

MICHAEL T. MCCAUL,
Chairman.

Ms. JACKSON LEE. Mr. Speaker, I rise in support of H.R. 3696, the National Cybersecurity and Critical Infrastructure Protection Act of 2014.

I would like to thank Chairman MCCAUL and Ranking Member THOMPSON for their leadership on the protection of our nation's critical infrastructure.

Several Jackson Lee amendments were included in the H.R. 3696, the ''National Cybersecurity and Critical Infrastructure Protection Act of 2014.''

I submit to the committee for its consideration the following five amendments that would:

Identify the best methods for developing exercise to challenge the security measures taken to protect critical infrastructure from cyber attacks or incidents;

Assure efforts to conduct outreach to education institutions to promote cybersecurity awareness;

Provide better coordination for cyber incident emergency response and recovery;

Explore the benefits of establishing a visiting scholars program; and

Prioritized response efforts to aid in recovery of critical infrastructure from cyber incidents.

The Jackson Lee amendments improved H.R. 3696:

The first Jackson Lee amendment supports discussions among stakeholders on the best methods of developing innovative cybersecurity exercises for coordinating between the Department and each of the critical infrastructure sectors designated under section 227.

The second Jackson Lee amendment directs the Secretary to conduct outreach to universities, which shall include historically black colleges and universities, Hispanic serving institutions, Native American colleges and institutions serving persons with disabilities to promote cybersecurity awareness.

The third Jackson Lee amendment directs the Secretary of Homeland Security to make available Department contact information to serve as a resource for Sector Coordinating Councils and critical infrastructure owners and critical infrastructure operators to better coordinate cybersecurity efforts with the agency related to emergency response and recovery efforts for cyber incidents.

The fourth Jackson Lee amendment directs the Department of Homeland Security to determine the feasibility and potential benefit of developing a visiting security researchers program from academia, including cybersecurity scholars at the Department of Homeland Security's Centers of Excellence.

The fifth Jackson Lee amendment directs the Secretary of Homeland Security to collaborate with Sector Coordinating Councils, Information Sharing and Analysis Centers, Sector Specific Agencies, and relevant critical infrastructure sectors on the development of prioritized response efforts, if necessary, to support the defense and recovery of critical infrastructure from cyber incidents.

Global dependence on the Internet and particularly the interconnected nature of the cyber-space makes cyber security a very difficult public policy challenge, but H.R. 3696 is making a significant step forward in addressing cyber security threats.

Cyber thieves work around the clock to probe and breach computer systems resulting in the largest unlawful transfer of wealth in history.

H.R. 3696 emphases on public/private partnerships and information sharing is a critically important first step in combating illegal, damaging and expensive data breaches. This legislation already addresses many useful and essential cybersecurity tools and initiatives such as: enhanced education, increased research, information sharing, data breach security and technical assistance strategies.

H.R. 3639 will allow the Department of Homeland Security to partner with and support the efforts of critical infrastructure owners and operators to secure their facilities and guide the agency in its work to create resources to support the global mission of infrastructure protection, which is vital to the nation.

I encourage my colleagues to vote in favor of H.R. 3696.

Mr. THOMPSON of Mississippi. Mr. Speaker, I am pleased to be here today as an original cosponsor of this legislation, the National Cyber Security and Critical Infrastructure Protection Act.

This bipartisan legislation gives the Department of Homeland Security Congressional Authority to more fully carry out its civilian cyber mission, and to increase protection for our national critical infrastructure.

Importantly, this legislation also gives the Committee on Homeland Security a robust oversight position to make sure the Department carries out an innovative and cooperative relationship with industry, to protect the nation's privately owned critical infrastructure.

By giving DHS specific civilian authorities, it codifies what the President has already set into motion with his Cyber Executive Order 13636, issued in February of 2013, but Executive Authority goes only so far, and the President has said that his efforts cannot take the place Congressional action.

Mr. Speaker, we have stepped up to the plate. The legislation that Mr. MCCAUL and I worked on together, directs Federal agencies and private industry to coordinate the development and implementation of voluntary risk-based security standards, and codifies the ongoing process that the National Institute of Standards and Technology (NIST) and private industry have taken on.

We are asking that business and government find an adaptable and cooperative cyber security framework, for both government and private companies, not an off-the-shelf, or check-the-box solution.

We must depend on strong private sector leadership and accountability to focus on our nation's most pressing cyber vulnerabilities, protecting critical systems that when disrupted could cause catastrophic damage to our citizens. I believe this legislation will allow that process to move forward.

The President said it best, "It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy and civil liberties."

Critical infrastructure provides the essential services that underpin American society, and I suggest that the owners and operators of America's critical infrastructure are in a unique position to manage their own business risks with the help of civilian government agencies, to develop operational approaches that can make our critical infrastructure protected and durable.

Mr. Speaker, I have worked long and hard with the chairman to hammer out privacy and liability concerns held by myself, and many others, on both sides of the aisle.

There are no broad exceptions to the current privacy laws in this legislation, and it focuses on information sharing using existing structures. In fact, the ACLU commended the construction of this legislation by saying, ". . . it is both pro-security and pro-privacy . . ."

We still have much work to do to achieve a higher level of cyber security in this country, and internationally.

We must approach the cyber threat arena in a way that is consistent with traditional American values, and by leading on the issue of respecting personal privacy in the efforts to achieve cyber security, we must continue to respect the safeguards for our constitutional right of freedom of speech.

The wrong way is to assume that we must cede all of our personal privacy and freedoms to remain safe.

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. 3696, 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.

CRITICAL INFRASTRUCTURE RESEARCH AND DEVELOPMENT ADVANCEMENT ACT OF 2013

Mr. MEEHAN. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 2952) to amend the Homeland Security Act of 2002 to make certain improvements in the laws relating to the advancement of security technologies for critical infrastructure protection, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 2952

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 ''Critical Infrastructure Research and Development Advancement Act of 2013'' or the ''CIRDA Act of 2013''.

SEC. 2. DEFINITIONS.

Section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101) is amended by redesignating paragraphs (15) through (18) as paragraphs (16) through (19), respectively, and by inserting after paragraph (14) the following:

''(15) The term 'Sector Coordinating Council' means a private sector coordinating council that is—

''(A) recognized by the Secretary as such a Council for purposes of this Act; and

''(B) comprised of representatives of owners and operators of critical infrastructure within a particular sector of critical infrastructure.''.

SEC. 3. CRITICAL INFRASTRUCTURE PROTECTION RESEARCH AND DEVELOPMENT.

(a) STRATEGIC PLAN; PUBLIC-PRIVATE CONSORTIUMS.—

(1) IN GENERAL.—Title III of the Homeland Security Act of 2002 (6 U.S.C. 181 et seq.) is amended by adding at the end the following:

''SEC. 318. RESEARCH AND DEVELOPMENT STRATEGY FOR CRITICAL INFRASTRUCTURE PROTECTION.

''(a) IN GENERAL.—Not later than 180 days after the date of enactment of the Critical Infrastructure Research and Development Advancement Act of 2013, the Secretary, acting through the Under Secretary for Science and Technology, shall transmit to Congress a strategic plan to guide the overall direction of Federal physical security and cybersecurity technology research and development efforts for protecting critical infrastructure, including against all threats. Once every 2 years after the initial strategic plan is transmitted to Congress under this section, the Secretary shall transmit to Congress an update of the plan.

''(b) CONTENTS OF PLAN.—The strategic plan shall include the following:

''(1) An identification of critical infrastructure security risks and any associated security technology gaps, that are developed following—

''(A) consultation with stakeholders, including the Sector Coordinating Councils; and

''(B) performance by the Department of a risk/gap analysis that considers information received in such consultations.

''(2) A set of critical infrastructure security technology needs that—

''(A) is prioritized based on risk and gaps identified under paragraph (1);

''(B) emphasizes research and development of those technologies that need to be accelerated due to rapidly evolving threats or rapidly advancing infrastructure technology; and

''(C) includes research, development, and acquisition roadmaps with clearly defined objectives, goals, and measures.

''(3) An identification of laboratories, facilities, modeling, and simulation capabilities that will be required to support the research, development, demonstration, testing, evaluation, and acquisition of the security technologies described in paragraph (2).

''(4) An identification of current and planned programmatic initiatives for fostering the rapid advancement and deployment of security technologies for critical infrastructure protection. The initiatives shall consider opportunities for public-private partnerships, intragovernment collaboration, university centers of excellence, and national laboratory technology transfer.

''(5) A description of progress made with respect to each critical infrastructure security risk, associated security technology gap, and critical infrastructure technology need identified in the preceding strategic plan transmitted under this section.

''(c) COORDINATION.—In carrying out this section, the Under Secretary for Science and Technology shall coordinate with the Under Secretary for the National Protection and Programs Directorate.

''(d) CONSULTATION.—In carrying out this section, the Under Secretary for Science and Technology shall consult with—

''(1) the critical infrastructure Sector Coordinating Councils;

''(2) to the extent practicable, subject matter experts on critical infrastructure protection from universities, colleges, including historically black colleges and universities, Hispanic- serving institutions, and tribal colleges and universities, national laboratories, and private industry;

''(3) the heads of other relevant Federal departments and agencies that conduct research and development for critical infrastructure protection; and

''(4) State, local, and tribal governments as appropriate.

''SEC. 319. REPORT ON PUBLIC-PRIVATE RESEARCH AND DEVELOPMENT CONSORTIUMS.

''(a) IN GENERAL.—Not later than 180 days after the enactment of the Critical Infrastructure Research and Development Advancement Act of 2013, the Secretary, acting through the Under Secretary for Science and Technology, shall transmit to Congress a report on the Department's utilization of public-private research and development consortiums for accelerating technology development for critical infrastructure protection. Once every 2 years after the initial report is transmitted to Congress under this section, the Secretary shall transmit to Congress an update of the report. The report shall focus on those aspects of critical infrastructure protection that are predominately operated by the private sector and that would most benefit from rapid security technology advancement.

''(b) CONTENTS OF REPORT.—The report shall include—

''(1) a summary of the progress and accomplishments of on-going consortiums for critical infrastructure security technologies;

''(2) in consultation with the Sector Coordinating Councils and, to the extent practicable,