114th Congress
Cybersecurity Activity
Updated: December 2016

EXECUTIVE ACTIVITY

On July 26, 2016, the President released his United States Cyber Incident Coordination Policy Directive, to set forth principles governing the Federal Government’s response to any cyber security incident. Furthermore, for any significant incident, the policy directive also establishes the lead federal agencies for coordinating the broad response. The PPD lists its principles guiding response efforts as: Shared Responsibility, Risk-based Response, Respecting Affected Entities, Unity of Governmental Effort, and Enabling Restoration and Recovery.

On May 25, 2016, the President released the final Data Security Policy Principles and Framework (Security Framework) for his Precision Medicine Initiative (PMI), as an effort to protect private patient information concerning personal health, genetic, and environmental information. The Security Framework builds on the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and can be used to develop detailed implementation guidelines that address organizations’ specific data security needs.

On February 24, 2016, the President signed the Judicial Redress Act of 2015 (H.R. 1428, S. 1600) into law. The bill authorizes the Department of Justice (DOJ) to designate foreign countries to regional economic integration organizations whose natural citizens may bring civil actions under the Privacy Act of 1974 against certain U.S. government agencies for purpose of accessing, amending, or redressing unlawful disclosures of records transferred from a foreign country to the United States to prevent, investigate, detect, or prosecute criminal offenses.

On February 9, 2016, President Obama unveiled his Cybersecurity National Action Plan (CNAP). In the CNAP, the President calls for a sweeping range of actions in both the public and private sectors in order to revitalize the nations IT infrastructure. These actions include:

a) The establishment of the Commission on Enhancing National Cybersecurity
b) Proposal for a $3.1 billion dollar fund to be set aside for modernizing government IT systems
   a. The plan also creates the position of Federal Chief Information Security Officer
   c) Adding additional layers of protection to the public’s various systems. Such as, multi-factor authentication
d) A $19 billion dollar cybersecurity budget for FY 2017

On February 9, 2016, President Obama signed Executive Order 13718: Commission on Enhancing National Cybersecurity. This order establishes the Commission on Enhancing National Cyber Security within the Department of Commerce. The Commission is to be composed of 12 President-appointed, non-government members. Commission members are tasked with studying advancements in technology and the IT field and making recommendations
to address cyber-vulnerabilities and strengthen cybersecurity in both the public and private sectors.

On January 22, 2016, the Obama administration indicated that it would establish a new office, the National Background Investigations Bureau (NBIB), to handle background investigations for the entire federal government. The NBIB will absorb the Office of Personnel Management’s (OPM) existing Federal Investigative Services (FIS) and will report to the OPM Director. The design, development, security, and operation of the background investigations IT systems will be handled by the Department of Defense. The President has earmarked an additional $95 million in his 2017 budget to pay for this upgraded IT system.

On April 1, 2015, the President signed Executive Order 13694: Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities. This order authorizes the Secretary of Treasury, in consultation with the Attorney General and the Secretary of State, to impose sanctions on individuals that he determines to be responsible for cyber activities that seriously threaten the United States. This power is meant to freeze the ill-gotten gains of malicious cyber activity, and is a complimentary law enforcement tool to those already available.

On February 25, 2015, President Obama directed the Director of National Intelligence to establish the Cyber Threat Intelligence Integration Center. The CTIIC will provide integrated all-source intelligence analysis related to foreign cyber threats and cyber incidents affecting U.S. national interests; support the U.S. government centers responsible for cybersecurity and network defense; and facilitate and support efforts by the government to counter foreign cyber threats. Once established, the CTIIC will join the National Cybersecurity and Communications Integration Center (NCCIC), the National Cyber Investigative Joint Task Force (NCIJTF), and U.S. Cyber Command as integral parts of the United States Government’s capability to protect our citizens, our companies, and our Nation from cyber threats.

The CTIIC will not be an operational center but will collect intelligence to assist other agencies like the NCCIC and the NCIJTF as they carry out their cybersecurity missions. No destination for the center has been established yet, but their current plan is to have the center located in metro Washington, DC.

On January 13, 2015, the Administration wrote a letter to Congress urging action on the following three priorities: 1) enhancing cyber threat information sharing within the private sector and between the private sector and the Federal Government; 2) protecting individuals by requiring businesses to notify consumers if personal information is compromised; and 3) strengthening and clarifying the ability of law enforcement to investigate and prosecute cybercrimes.
The FY2016 Budget provides $14 billion to support cybersecurity efforts.

I. Updated Department of Homeland Security Cybersecurity Authority and Information Sharing

   a. The Administration proposes to update the Department of Homeland Security Cybersecurity Authority and information sharing by codifying mechanisms for enabling cybersecurity information between private and government entities, as well as among private entities, to better protect information systems and more effectively respond to cybersecurity incidents.

II. Updated Law Enforcement Provisions Related to Computer Security. The major changes are as follows:

   1. Prosecuting Organized Crime Groups That Utilize Cyber Attacks. This change adds offenses under the Computer Fraud and Abuse Act (18 U.S.C. § 1030) to the list of racketeering activities in the Racketeering Influenced and Corrupt Organizations Act (RICO at 18 U.S.C. § 1961(1)). This change would increase certain penalties and make it easier to prosecute organized criminal groups that engage in computer network and similar attacks.

   2. Deterring the Development and Sale of Computer and Cell Phone Spying Devices. These provisions provide additional tools to address violations of 18 U.S.C. § 2512, which criminalizes the sale, distribution, and advertising of surreptitious interception devices.

   3. Modernizing the Computer Fraud and Abuse Act. This updates and clarifies several provisions of the Computer Fraud and Abuse Act (18 U.S.C. § 1030) to enhance effectiveness against attacks on computers and computer networks, including those by insiders.

   4. Ensuring Authority for Courts to Shut Down Botnets. This proposal would empower courts to issue injunctions to disrupt or shut down botnets. The amendment would also create liability protection for companies that act in compliance with court orders under the section, and allow courts to order reimbursement where companies incur reasonably necessary compliance costs.
LEGISLATIVE ACTIVITY

I. Bills Passed by the House

1) H.R. 5877 - United States- Israel Advanced Research Partnership Act of 2016

**Sponsor:** Rep. Ratcliffe, John [R-TX-4] (Introduced 07/14/2016)

**Latest Action:** 11/30/2016 Received in the Senate. 2 cosponsors.

**Bill Summary**
To amend the Homeland Security Act of 2002 and the United States-Israel Partnership Act of 2014 to promote cooperative homeland security research and antiterrorism programs relating to cybersecurity.


**Sponsor:** Rep. Langevin, James R. [D-RI-2] (Introduced 07/14/2016)

**Latest Action:** 11/30/2016 Received in the Senate. 1 cosponsor.

**Bill Summary**
This bill authorizes the Department of Homeland Security to promote cooperative research and development between the United States and Israel on cybersecurity; and for the demonstration and commercialization of cybersecurity technology.

3) H.R. 5594 – National Strategy for combating Terrorist, Underground, and Other Illicit Financing Act

**Sponsor:** Rep. Fitzpatrick, Michael G. [R-PA-8] (Introduced 06/28/2016)

**Latest Action:** 07/12/2016 Received in the Senate and Read twice and referred to the Committee on Banking, Housing, and Urban Affairs. 23 cosponsors.

**Bill Summary**
This bill directs the President, acting through the Department of the Treasury, to develop a national strategy for combating the financing of terrorism and related forms of illicit finance. The national strategy shall focus upon selected aspects, including: (6) illicit finance and cybercrime; and (7) technology.
4) **H.R. 5537 – Digital GAP Act**

**Sponsor:** Rep. Royce, Edward R. [R-CA-39] (Introduced 06/21/2016)  
**Latest Action:** 09/08/2016 Received in the Senate and Read twice and referred to the Committee on Foreign Relations. 7 cosponsors.

**Bill Summary**  
This bill expresses the sense of Congress that: the Department of State should designate an Assistant Secretary for Technology, International Communications, and Cyberspace to lead diplomatic cyberspace policy for internet access, governance, and freedom, telecommunications networks and communications technology, and cyber security.

5) **H.R. 5459 - Cyber Preparedness Act of 2016**

**Sponsor:** Rep. Donovan, Daniel M., Jr. [R-NY-11] (Introduced 06/13/2016)  
**Latest Action:** 09/27/2016 Received in the Senate and referred to the Committee on Homeland Security and Governmental Affairs. 3 cosponsors.

**Bill Summary**  
This bill amends the Homeland Security Act of 2002 to expand the responsibilities of the Department of Homeland Security’s State, Local, and Regional Fusion Center Initiative to include serving as a point of contact to ensure the dissemination of cybersecurity risk information within the scope of its information sharing environment with state, local, and regional fusion centers.

6) **H.R. 5388 – Support for Rapid Innovation Act of 2016**

**Sponsor:** Rep. Ratcliffe, John [R-TX-4] (Introduced 06/07/2016)  
**Latest Action:** 06/22/2016 Received in the Senate and Read twice and referred to the Committee on Homeland Security and Governmental Affairs. 1 cosponsor.

**Bill Summary**  
This bill amends the Homeland Security Act of 2002 to direct the Under Secretary for Science and Technology of the Department of Homeland Security to support the research, development, testing, evaluation, and transition of cybersecurity technologies.

7) **H.R. 5312 – Networking and Information Technology Research and Development Act of 2016**

**Sponsor:** Rep. LaHood, Darin [R-IL-18] (Introduced 05/24/2016)  
**Latest Action:** 06/14/2016 Received in the Senate and Read twice and referred to the Committee on Commerce, Science, and Transportation. 8 cosponsors.
Bill Summary
(Sec. 5) This bill amends the High-Performance Computing Act of 1991 to rename the National High-Performance Computing program as the Networking and Information Technology Research and Development Program. The program, in addition to its current requirements, shall: conduct or arrange for research and development on human-computer interactions, visualization, and big data, as well as the enhancement of cybersecurity.


Latest Action: 09/22/2016 Received in the Senate. 18 cosponsors.

Bill Summary
This bill requires the Small Business Administration (SBA) and the Department of Homeland Security (DHS) to develop a Small Business Development Center Cyber Strategy after the Government Accountability Office issues a report that reviews federal cybersecurity resources aimed at assisting small businesses.


Latest Action: 05/17/2016 Received in the Senate and read twice and referred to the Committee on Homeland Security and Governmental Affairs. 6 cosponsors.

Bill Summary
This bill authorizes the Department of Homeland Security (DHS) to work with a consortium, including the National Cybersecurity Preparedness Consortium, to support efforts to address cybersecurity risks and incidents, including threats or acts of terrorism.

10) H.R. 4361 – Government Reform and Improvement Act of 2016

Latest Action: 07/07/2016 Received in Senate and Read twice and referred to the Committee on Homeland Security and Governmental Affairs. 1 cosponsor.

Bill Summary
This bill grants the head of each federal agency the sole and exclusive authority, with respect to any information technology or information system under the control of such agency, to take any action the agency determines to be necessary to reduce or eliminate a present or future security weakness and risk, including to protect the information contained in the information technology or information system.
11) H.R. 3878 – Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2015

**Latest Action:** 02/01/2016 Star Print ordered on the bill. 3 cosponsors.

**Bill Summary**
This bill requires the Department of Homeland Security (DHS) to implement, and evaluate at least every two years, a maritime cybersecurity risk assessment model to evaluate current and future cybersecurity risks. The model must be consistent with the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity and any updates pursuant to the Cybersecurity Enhancement Act of 2014.

12) H.R. 3869 – State and Local Cyber Protection Act of 2015

**Sponsor:** Rep. Hurd, Will [R-TX-23] (Introduced 11/02/2015)
**Latest Action:** 12/14/2015 Received in the Senate and Read twice and referred to the Committee on Homeland Security and Governmental Affairs. 5 cosponsors.

**Bill Summary**
This bill amends the Homeland Security Act of 2002 to require the Department of Homeland Security's (DHS's) national cybersecurity and communications integration center (NCCIC) to assist state and local governments with cybersecurity. The NCCIC must seek feedback from state and local governments on the effectiveness of such activities and provide such information to Congress.

13) H.R. 3578 – DHS Science and Technology Reform and Improvement Act of 2015

**Sponsor:** Rep. Ratcliffe, John [R-TX-4] (Introduced 09/18/2015)
**Last Action:** 12/14/2015 Received in the Senate and Read twice and referred to the Committee on Homeland Security and Governmental Affairs. 2 cosponsors.

**Bill Summary**
This bill amends the Homeland Security Act of 2002 to declare that the Directorate of Science and Technology of the Department of Homeland Security (DHS) shall be the primary research, development, testing, and evaluation arm of DHS, responsible for coordinating such activities to strengthen the security and resiliency of the United States. The Directorate shall be headed by the DHS Undersecretary for Science and Technology, who shall: (1) serve as the DHS senior scientific advisor, and (2) identify and develop countermeasures to terrorist threats that may serve as the basis for a national strategy.

**Sponsor:** Rep. Richmond, Cedric L. [D-LA-2] (Introduced 09/15/2015)

**Latest Action:** 10/07/2015 Received in the Senate and Read twice and referred to the Committee on Homeland Security and Governmental Affairs. 3 cosponsors.

**Bill Summary**
This bill amends the Homeland Security Act of 2002 to require the Department of Homeland Security (DHS) to develop a cybersecurity strategy that includes: (1) strategic and operational goals and priorities to execute the full range of DHS's cybersecurity responsibilities; and (2) information on programs, policies, and activities in furtherance of the cybersecurity functions of the national cybersecurity and communications integration center (NCCIC), investigations capabilities, research and development, and engagement with international partners. It prohibits this strategy from being construed as permitting DHS to engage in monitoring, surveillance, exfiltration, or other collection activities to track an individual's personally identifiable information.

15) H.R. 3490 – Strengthening State and Local Cyber Crime Fighting Act

**Sponsor:** Rep. Ratcliffe, John [R-TX-4] (Introduced 09/11/2015)

**Latest Action:** 12/01/2015 Received in the Senate and Read twice and referred to the Committee on the Judiciary. 3 cosponsors.

**Bill Summary**
This bill amends the Homeland Security Act of 2002 to establish in the Department of Homeland Security (DHS) a National Computer Forensics Institute to be operated by the U.S. Secret Service for the dissemination of homeland security information related to the investigation and prevention of cyber and electronic crime and related threats to educate, train, and equip state, local, tribal, and territorial law enforcement officers, prosecutors, and judges.


**Sponsor:** Rep. McCaul, Michael T. [R-TX-10] (Introduced 04/13/2015)

**Last Action:** 04/23/2015 Pursuant to the provisions of H. Res. 212, H.R. 1731 is laid on the table. 1 cosponsor.

**Bill Summary**
Amends the Homeland Security Act of 2002 to allow the Department of Homeland Security's (DHS's) national cybersecurity and communications integration center (NCCIC) to include tribal governments, information sharing and analysis centers, and private entities among its non-federal representatives.
17) H.R. 1560 – Protecting Cyber Networks Act

**Sponsor:** Rep. Nunes, Devin [R-CA-22] (Introduced 03/24/2015)

**Last Action:** 07/14/2016 Read twice and referred to the Committee on Homeland Security and Governmental Affairs. 8 cosponsors.

**Bill Summary**
Amends the National Security Act of 1947 to require the Director of National Intelligence (DNI) to develop and promulgate procedures to promote: (1) the timely sharing of classified and declassified cyber threat indicators in possession of the federal government with private entities, non-federal government agencies, or state, tribal, or local governments; and (2) the sharing of imminent or ongoing cybersecurity threats with such entities to prevent or mitigate adverse impacts.

18) H.R. 1073 – Critical Infrastructure Protection Act (CIPA)

**Sponsor:** Rep. Franks, Trent [R-AZ-8] (Introduced 02/25/2015)

**Latest Action:** 11/17/2015 Received in the Senate and Read twice and referred to the Committee on Homeland Security and Governmental Affairs. 19 cosponsors.

**Bill Summary**
Amends the Homeland Security Act of 2002 to define "EMP" to mean: (1) an electromagnetic pulse caused by intentional means, including acts of terrorism; and (2) a geomagnetic disturbance caused by solar storms or other naturally occurring phenomena. Directs DHS to: (1) include in national planning frameworks the threat of EMP events; and (2) conduct outreach to educate owners and operators of critical infrastructure, emergency planners, and emergency response providers of the threat of EMP events. Directs DHS to conduct research and development to mitigate the consequences of EMP events.

19) H.R. 699 – Email Privacy Act

**Sponsor:** Rep. Yoder, Kevin [R-KS-3] (Introduced 02/04/2015)

**Latest Action:** 04/28/2016 Received in the Senate. 314 cosponsors.

**Bill Summary**
Amends the Electronic Communications Privacy Act of 1986 to prohibit a provider of remote computing service or electronic communication service to the public from knowingly divulging to a governmental entity the contents of any communication that is in electronic storage or otherwise maintained by the provider, subject to exceptions.

Revises provisions under which the government may require a provider to disclose the contents of such communications. Requires the government to obtain
a warrant from a court before requiring providers to disclose the content of such communications regardless of how long the communication has been held in electronic storage by an electronic communication service or whether the information is sought from an electronic communication service or a remote computing service

II. Bills Introduced in the House

1) H.R. 6066 – Cybersecurity Responsibility and Accountability Act of 2016

Latest Action: 09/21/2016 Ordered to be Reported by Voice Vote.
3 cosponsors.

Bill Summary
This bill requires the National Institute of Standards and Technology to incorporate additional cybersecurity requirements in its computer standards for agency information systems and provide the Office of Management and Budget with a process for agencies to implement those standards. NIST must also: (1) support development of information security training and certification for agency heads, (2) address agency-identified information security challenges and knowledge gaps, (3) assess information security statutory requirements, and (4) develop security standards for national security systems.

2) H.R. 6002 – Cybercrime Statistics Act


Bill Summary
This bill authorizes the Attorney General to develop a national strategy to reduce the incidence of cybercrimes against individuals, coordinate investigations of cybercrimes against individuals by Federal law enforcement agencies, and increase the number of Federal prosecutions of cybercrimes against individuals; and authorizes the Director of the FBI to: design and create a category for cybercrime offenses in the UCR. Classify cybercrime against an individual as a Group A offense for the purpose of NIBRS reporting.

3) H.R. 5911 – Countering Violent Extremism Task Force Oversight Act

Sponsor: Rep. Young, Todd C. [R-IN-9] (Introduced 7/14/2016)
Latest Action: 08/19/2016 Referred to the Subcommittee on Counterterrorism and Intelligence. 3 cosponsors.
Bill Summary
This bill would require the Secretary of Homeland Security and the Attorney General to submit a report on the Countering Violent Extremeism Task Force that includes how the Task Force plans and coordinates federal programs to combat extremism through internet, social media, and other sources; and propose policy recommendations for developing coordinated, coherent, cohesive whole-government countering violent extremism programs of the Federal Government.

4) H.R. 5727 – Preventing Iranian Destabilization of Iraq Act of 2016

Latest Action: 07/12/2016 Referred to House Judiciary. 32 cosponsors.

Bill Summary
This bill declares it shall be the policy of the United States to impose sanctions with respect to terrorist organizations and foreign countries, including the government of Iran, that threaten the peace or stability of Iraq. The bill directs the President to impose sanctions to block transactions in property and interests in property in the United States of, and the Department of State or the Department of Homeland Security (DHS) to deny admissions into the United States or revoke the visa of, any foreign person that State or DHS determines: (1) has knowingly materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services in support of, any such act; and The bill directs the President to determine whether specified Iranian officials are responsible for engaging in acts or activities described in this bill and, if so, to impose admissions-related sanctions on such officials; and The President must report, every 180 days for 5 years, on Iranian activities in Iraq.


Bill Summary
The bill prohibits granting a security clearance to, and requires revocation of the security clearance of, any federal officer or employee who has exercised extreme carelessness in the handling of classified information. The bill also amends a provision of the federal criminal code that subjects to criminal penalties anyone entrusted with, or having lawful possession or control
of, national defense information who, through gross negligence, permits that information to be removed from its proper place of custody or delivered to anyone or to be lost, stolen, abstracted, or destroyed.

6) **H.R. 5390 – Cybersecurity and Infrastructure Protection Act of 2016**

**Sponsor:** Rep. McCaul, Michael T [R-TX-10] (Introduced 06/07/2016)

**Latest Action:** 06/08/2016 Ordered to be Reported (Amended) by Voice Vote. 2 cosponsors.

**Bill Summary**
This bill amends the Homeland Security Act of 2002 to redesignate the DHS's National Protection and Programs Directorate as the Cybersecurity and Infrastructure Protection Agency (CIPA) to be headed by a Director of National Cybersecurity (appointed by the President with the Senate's consent) to lead national efforts to protect and enhance the security and resilience of U.S. cyber and critical infrastructure.

7) **H.R. 5222 – Iran Cyber Sanctions Act of 2016**

**Sponsor:** Rep. Ratcliffe, John [R-TX-4] (Introduced 05/12/2016)

**Latest Action:** 05/18/2016 Referred to the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations. 0 cosponsors.

**Bill Summary**
This bill requires the President to report to Congress at least every 180 days regarding significant activities undermining cybersecurity conducted by persons on behalf of or at the direction of the government of Iran against the United States (including U.S. persons, entities, or federal, state, or local governments). The reports must: (1) identify persons that have knowingly facilitated, participated or assisted in, engaged in, directed, or provided material support for such activities; (2) describe their conduct; (3) assess the Iranian government's or other foreign governments' direction, facilitation, or material support in such activities; and (4) provide a strategy to counter efforts by persons to conduct such activities, which shall include engaging foreign governments to halt the capabilities of such persons.

The President must include on the Office of Foreign Assets Control's specially designated nationals and blocked persons list persons who are: (1) identified in such reports; or (2) indicted by the Department of Justice in connection with such activities undermining U.S. cybersecurity. Under an exception, the President may exclude such a person from the list by submitting an explanation to Congress. The President must use Executive Order 13694 to impose sanctions against persons included on such list.
8) **H.R. 5220 – Cyber Act of War Act of 2016**


**Latest Action:** 06/07/2016 Referred to the Subcommittee on Emerging Threats and Capabilities. 1 cosponsor.

**Bill Summary**
This bill directs the President to: develop a policy for determining when an action carried out in cyberspace constitutes a use of force against the United States, and revise the Department of Defense Law of War Manual accordingly. In developing this policy, the President shall consider: the ways in which the effects of a cyberattack may be equivalent to the effects of a conventional attack; including physical destruction or casualties, and intangible effects of significant scope or duration.

9) **H.R. 5069 – Cybersecurity Systems and Risks Reporting Act**

**Sponsor:** Rep. McDermott, Jim [D-WA-7] (Introduced 04/26/2016)

**Latest Action:** 04/26/2016 Referred to the House Committee on Financial Services. 0 cosponsor.

**Bill Summary**
To amend the Sarbanes-Oxley Act of 2002 to protect investors by expanding the mandated internal controls reports and disclosures to include cybersecurity systems and risks of publicly traded companies.

10) **H.R. 4897 – Information Technology Modernization Act**


**Latest Action:** 04/11/2016 Referred to the House Committee on Oversight and Government Reform. 20 cosponsors.

**Bill Summary**
This bill establishes in the Treasury an Information Technology Modernization Fund for technology related activities, to improve information technology, and to enhance cybersecurity across the federal government.

11) **H.R. 4860 – Israel Cybersecurity Cooperation Act**

**Sponsor:** Rep. Cicilline, David N. [D-RI-1] (Introduced 03/23/2016)

**Latest Action:** 09/30/2016 Referred to the Subcommittee on Research and Technology. 41 cosponsors.
Bill Summary
This bill authorizes the Department of Homeland Security (DHS) to establish a joint United States-Israel Cybersecurity Center of Excellence based in the United States and Israel to leverage the experience, knowledge, and expertise of institutions of higher education, the private sector, and government entities in cybersecurity and protection of critical infrastructure. The center may promote joint research and development, share best practices and access to American and Israeli innovation, and strengthen partnerships between the United States and Israeli entities.

12) H.R. 4350 – To Repeal the Cybersecurity Act of 2015

Sponsor: Rep. Amash, Justin [R-MI-3] (Introduced 01/08/2016)
Latest Action: 09/30/2016 Referred to the Subcommittee on Research and Technology. 6 cosponsors.

Bill Summary


Latest Action: 11/02/2015 Referred to the House Committee on Foreign Affairs. 0 cosponsor.

Bill Summary
This bill directs the Department of State to: (1) produce a comprehensive strategy, with a classified annex if necessary, relating to U.S. international cyberspace policy; and (2) publicly release such strategy and brief Congress upon its release, including any accompanying classified annex.


Bill Summary
Amends the Homeland Security Act of 2002 to require the Department of Homeland Security (DHS), in coordination with the Office of Management and Budget (OMB), to implement plans to: (1) detect, identify, and remove intruders in federal agencies' information systems; and (2) make advanced network security
tools available for agencies to improve visibility of network activity to detect and mitigate intrusions and anomalous activity.

15) H.R. 3305 – EINSTEIN Act of 2015


Bill Summary
Amends the Homeland Security Act of 2002 to require the Department of Homeland Security (DHS) to deploy, operate, and maintain (to make available for use by any federal agency, with or without reimbursement) capabilities to protect federal agency information and federal civilian information systems, including technologies to continuously diagnose, detect, prevent, and mitigate against cybersecurity risks involving such information or systems.

16) H.R. 3039 – PROTECT US ACT

Latest Action: 07/16/2015 Referred to the Subcommittee on Trade. 3 cosponsors.

Bill Summary
This bill directs the President to submit to Congress a list of countries designated as state-sponsors of cyberattacks. A country shall be so designated if the President determines that the United States or a U.S. person has been targeted in a cyber-enabled activity originating from or directed by a person located in a foreign country, and such activity is likely to result in or have contributed to a threat to U.S. national security or foreign policy, or harmed U.S. economic health or financial stability or a U.S. person, or has the purpose or effect of: harming or compromising the provision of services by a computer or network of computers that support the United States or a U.S. person in a critical infrastructure sector; compromising the provision of services by the United States or a U.S. person in a critical infrastructure sector; disrupting the availability of a computer or network of computers owned or operated by the United States or a U.S. person; or causing a misappropriation of funds or economic resources, trade secrets, personally identifiable information, or financial information of the United States or a U.S. person. The President may impose a trade-related penalty and take other actions, including assistance limitations, trade embargoes, and cyber counter attacks, with respect to a designated country. A country may be removed from the list of state-sponsors of cyberattacks if: (1) the President determines that it no longer meets the requirements for the designation, or (2) Congress enacts a law providing for such removal. A country that has been removed from the list by Congress may not be added back to the list by the President until at least one year after removal.
17) H.R. 1918 - Aaron's Law Act of 2015

**Sponsor:** Rep. Lofgren, Zoe [D-CA-19] (Introduced 04/21/2015)
**Latest Action:** 05/15/2015 Referred to the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations. 5 cosponsors.

**Bill Summary**

1. Establish that mere breach of terms of service, employment agreements, or contracts are not automatic violations of the CFAA. By using legislative language based closely on recent important 9th and 4th Circuit Court opinions, Aaron’s Law would instead define ‘access without authorization’ under the CFAA as gaining unauthorized access to information by circumventing technological or physical controls – such as password requirements, encryption, or locked office doors. Notwithstanding this change, hack attacks such as phishing, injection of malware or keystroke loggers, denial-of-service attacks, and viruses would continue to be fully prosecutable under strong CFAA provisions that Aaron’s Law does not modify.

2. Aaron’s Law also brings balance back to the CFAA by eliminating a redundant provision of the law that subject an individual for multiple sanctions for the same CFAA violation.

3. Finally, Aaron’s Law would bring greater proportionality to CFAA penalties. Currently, the CFAA’s penalties are tiered, and prosecutors have wide discretion to ratchet up the severity of the penalties in several circumstances, leaving little room for non-felony charges under CFAA (i.e., charges with penalties carrying less than a year in prison). For example, under current law a prosecutor can seek to inflate potential sentences by stacking new charges atop previous violations of state laws. Aaron’s Law would reform the penalty for a violation to ensure prosecutors cannot seek to inflate sentences by stacking multiple.

18) H.R. 1770 - Draft of Data Security and Breach Notification Act of 2015

**Sponsor:** Rep. Blackburn, Marsha [R-TN-7] (Introduced 04/14/2015)
**Latest Action:** 04/17/2015 Referred to the Subcommittee on Commerce, Manufacturing, and Trade. 3 cosponsors.

**Bill Summary**

To require certain entities who collect and maintain personal information of individuals to secure such information and to provide notice to such individuals in the case of a breach of security involving such information, and for other purposes.
The new legislation would hold companies to a new national digital security standard that the authors claim is flexible enough not to restrain companies. It would also require that companies who have been breached notify people whose data may have been stolen within 30 days, unless there isn’t a reasonable risk of identity theft of financial harm.

19) H.R. 1704 – Personal Data Notification and Protection Act of 2015

**Sponsor:** Rep. Langevin, James R. [D-RI-2] (Introduced 03/26/2015)

**Latest Action:** 04/29/2015 Referred to the Subcommittee on the Constitution and Civil Justice. 0 cosponsors.

**Bill summary**

The bill provides uniformity in the measures required of companies in the event of a security breach related to sensitive personally identifiable information. In addition to delineating the required procedures in the event of a breach, the proposed Act also aims to provide consistent standards for what constitutes a “security breach” and “sensitive personally identifiable information” at the federal level to supersede the numerous iterations of these concepts scattered throughout applicable state laws.


**Sponsor:** Rep. Fleischmann, Charles J. "Chuck" [R-TN-3] (Introduced 01/21/2015)

**Latest Action:** 01/06/2016 Placed on the Union Calendar, Calendar No. 293. 38 Cosponsors.

**Bill Summary**

Prohibits a federal agency from deploying or making available to the public a new federal personally identifiable information website (new Federal PII Website) until the chief information officer of the agency submits a certification to Congress that the website is fully functional and secure, as those terms are defined by this Act. Defines "new Federal PII website" as a website that: (1) is operated by (or under contract with) an agency; (2) elicits, collects, stores, or maintains personally identifiable information (i.e., information that can be used to identify an individual, such as a social security number, a date and place of birth, a mother's maiden name, biometric records, or other information linked to an individual); and (3) is first made accessible to the public and collects or stores personally identifiable information on or after October 1, 2012.

Directs the Director of the Office of Management and Budget (OMB) to establish and oversee policies and procedures for federal agencies to follow in the event of a breach of information security involving the disclosure of personally identifiable
information, including: (1) notice, not later than 72 hours after discovery of a breach or possible breach, to individuals whose personally identifiable information could be compromised as a result of such breach; (2) timely reporting to a federal cyber security center designated by this Act; and (3) any additional actions that the Director finds necessary and appropriate.


**Sponsor:** Rep. Salmon, Matt [AZ-5] (Introduced 1/12/2015)
**Latest Action:** 2/2/2015- Referred to the Subcommittee on Crime, Terrorism, Homeland Security and Investigations. 4 cosponsors.

**Bill Summary**
This legislation states that a provider of remote computing service or electronic communication service to the public shall not knowingly divulge to any governmental entity the contents of certain communications without a warrant.

22) H.R. 234 – Cyber Intelligence Sharing and Protection Act

**Sponsor:** Rep. Dutch Ruppersberger [D-MD-2] (Introduced 01/08/2015)
**Latest Action:** 2/2/2015- Referred to the Subcommittee on the Constitution and Civil Justice. 3 cosponsors

**Bill Summary**
Directs the federal government to provide for real-time sharing of cyber threat information between all designated federal cyber operations centers and requires the Director of National Intelligence (DNI) to allow the intelligence community to share cyber threat intelligence with private-sector entities and utilities possessing appropriate certifications or security clearances.

Directs DHS, the Attorney General, the DNI, and the Department of Defense to establish procedures governing the receipt, retention, use, and disclosure of non-publicly available cyber threat information shared with the federal government and sets forth requirements for the use and protection of shared information.

Provides civil and criminal liability protections to cybersecurity providers, contracting entities, and self-protected entities acting in good faith to obtain or share threat information or to safeguard systems from threats and allows the federal government to use shared cyber threat information to deter attacks and investigate criminal activity.

**Sponsor:** Rep. Conyers, John, Jr. [MI-13] (Introduced 1/6/2015)
**Latest Action:** 1/22/2015 Referred to the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations. 1 cosponsor

**Bill Summary**
Amends the federal criminal code to provide criminal penalties for intentional failures to provide required notices of a security breach involving sensitive personally identifiable information and requires those with knowledge of a major security breach to provide prompt notice to the U.S. Secret Service or the Federal Bureau of Investigation.

24) H.R. 60 – Cyber Defense National Guard Act

**Sponsor:** Rep Jackson Lee, Sheila [TX-18] (introduced 1/6/2015)
**Latest Major Action:** 1/6/2015 Referred to the House Committee on Intelligence (Permanent Select). 0 cosponsors

**Bill Summary**
Requires the Director of National Intelligence to report to Congress regarding the feasibility of establishing a Cyber Defense National Guard. Requires the report to address: (1) the number of persons who would be needed to defend the critical infrastructure of the United States from a cyber-attack or man-made intentional or unintentional catastrophic incident; (2) elements of the federal government that would be best equipped to recruit, train, and manage such a National Guard; (3) resources that can be pre-positioned and training that can be instilled to assure responsiveness if an incident disrupts communications in a region or area; (4) logistics of allowing governors to use such a National Guard in states during times of cyber emergency; and (5) whether a force trained to defend U.S. networks in a major attack or natural or man-made disaster will benefit overall efforts to defend the interests of the United States.

25) H.R. 53 – Cyber Security Education and Federal Workforce Enhancement Act

**Sponsor:** Rep. Jackson Lee, Sheila [TX-18] (introduced 1/6/2015)
**Latest Major Action:** 04/29/2015 Referred to the Subcommittee on Higher Education and Workforce Training. 0 cosponsors

**Bill Summary**
Amends the Homeland Security Act of 2002 to establish within the Department of Homeland Security (DHS) an Office of Cybersecurity Education and Awareness Branch to make recommendations to DHS regarding: (1) recruitment of
information assurance, cybersecurity, and computer security professionals; (2) grants, training programs, and other support for kindergarten through grade 12, secondary, and post-secondary computer security education programs; (3) guest lecturer programs in which professional computer security experts lecture computer science students at institutions of higher education; (4) youth training programs for students to work in part-time or summer positions at federal agencies; and (5) programs to support underrepresented minorities in computer security fields with programs at minority-serving institutions, including historically black colleges and universities, Hispanic-serving institutions, native American colleges, Asian-American institutions, and rural colleges and universities. Requires the NSF to report to Congress regarding the causes of the high dropout rates of women and minority students enrolled in science, technology, engineering, and mathematics programs.

III. Bills Passed by the Senate


Latest Action: 09/08/2016 Conference held. 04/20/2016 Passed Senate. 0 cosponsors.

Bill Summary
This is a wide-ranging energy reform bill that includes a number of cybersecurity provisions intended to protect the power grid from cyber-attack. In particular, the Department of Energy would be authorized to direct companies in a cyber crisis. It also provides for enhanced research funding and directs the DOE to work more closely with our North American power grid partners, Canada and Mexico.

2) S. 754 – Cybersecurity Information Sharing Act of 2015

Last Action: 10/28/2015 Held at the desk. 0 cosponsors.

Bill Summary
This title requires the Director of National Intelligence (DNI) and the Departments of Homeland Security (DHS), Defense (DOD), and Justice (DOJ) to develop and promulgate procedures to promote the sharing of: (1) classified and declassified cyber threat indicators in possession of the federal government with private entities, nonfederal government agencies, or state, tribal, or local governments; (2) unclassified indicators with the public; (3) information with entities under cybersecurity threats to prevent or mitigate adverse effects; and (4) cybersecurity best practices with attention to the challenges faced by small businesses.
IV. Bills Introduced in the Senate


Sponsor: Sen. Cornyn, John [R-TX] (Introduced 09/07/2016)
Latest Action: 09/07/2016 Read twice and referred to the Committee on Homeland Security and Governmental Affairs. 1 cosponsors.

Bill Summary
The Secretary of Homeland Security may work with a consortium, including the National Cybersecurity Preparedness Consortium, to support efforts to address cybersecurity risks and incidents including threats of terrorism and acts of terrorism; and
The Secretary of Homeland Security may work with a consortium to assist the national cybersecurity and communications integration center of the Department of Homeland Security to:
(1) provide training to State and local first responders and officials specifically for preparing for and responding to cybersecurity risks and incidents, including threats of terrorism and acts of terrorism.
(2) develop and update a curriculum utilizing existing programs and models in accordance with such section 227, for State and local first responders and officials, related to cybersecurity risks and incidents.
(3) provide technical assistance services to build and sustain capabilities in support of preparedness for and response to cybersecurity risks and incidents, including threats of terrorism and acts of terrorism, in accordance with such section 227.

2) S. 3267 – Countering Iranian Threats Act of 2016

Sponsor: Sen. Corker, Bob [R-TN] (Introduced 07/14/2016)
Latest Action: 07/14/2016 Read twice and referred to the Committee on Foreign Relations. 7 cosponsors.

Bill Summary
This bill requires the President to submit to Congress any certification that the person or persons to whom sanctions were imposed under Executive Order 13694, has not engaged in, or provided support for any activity defined in Executive
Order 13694, for a period of 12 months prior to the submission of the certification; and
the sanctions will remain in effect for 90 days following the President’s submission of this certification to Congress; and
the President shall designate any person under this subsection that the president determines has directly or indirectly engaged in significant activities undermining cybersecurity by the Government of Iran or persons acting on behalf of the Government of Iran. Such persons who are designated shall be subject to all applicable sanctions under Executive Order 13694; and
the President shall submit to congress an annual report that describes significant activities undermining cybersecurity by the Government of Iran.

3) **S. 3263 – Modernizing Outdated and Vulnerable Equipment and Information Technology Act of 2016**

**Sponsor:** Sen. Moran, Jerry [R-KS] (Introduced 07/14/2016)

**Latest Action:** 07/14/2016 Read twice and referred to the committee on Homeland Security and Governmental Affairs. 3 cosponsors.

**Bill Summary**
The act proposes to accelerate the acquisition and deployment of cloud computing services, and support an efficient Federal certification standard for qualifying cloud service providers that balance encouraging the adoption of strong security practices while avoiding the imposition of unduly burdensome restrictive requirements that would deter investment in cloud systems.

4) **S. 3160 – SOS Act**

**Sponsor:** Sen. Perdue, David [R-GA] (Introduced 07/12/2016)

**Latest Action:** 07/12/2016 Read twice and referred to Committee on Foreign Relations. 4 cosponsors.

**Bill Summary**
This bill requires Department of State employees engaging in work-related electronic communications to use only state.gov email accounts, telephonic systems owned and managed by the State Department, or other systems owned and managed by the State Department or another appropriate federal agency; and the State Department must report annually on: (1) every security violation, including unauthorized transfers of classified information into electronic systems, transmissions, or storage not certified for handling classified information; and (2) its justification for failing to terminate an employee who commits a violation after having committed previous security violations during the prior 10 years or to request a Federal Bureau of Investigation review of such a violation; and
The State Department must submit a plan to train State Department employees to: (1) identify classified information in materials subject to Freedom of Information Act requests, (2) ensure that intelligence community officials have an opportunity to make classification determinations on information potentially originating with the intelligence community, and (3) certify annually that they have archived their emails and documents in accordance with federal law.

5) **S. 3135 – Taking Responsibility Using Secured Technologies Act of 2016**

**Sponsor:** Sen. Gardner, Cory [R-CO] (Introduced 07/06/2016)

**Latest Action:** 07/06/2016 Read twice and referred to the Committee on Homeland Security and Governmental Affairs. 15 cosponsors.

**Bill Summary**
This bill expresses the sense of Congress that: (1) former Secretary of State Hillary Clinton should have any security clearance she holds revoked and should be denied access to classified information unless she earns the legal right to such access, and (2) any of her colleagues who demonstrated extreme carelessness in their handling of classified information should no longer have access to that information.

The bill prohibits granting a security clearance to, and requires revocation of the security clearance of, any federal officer or employee who has exercised extreme carelessness in the handling of classified information.

The bill also amends a provision of the federal criminal code that subjects to criminal penalties anyone entrusted with, or having lawful possession or control of, national defense information who, through gross negligence, permits that information to be removed from its proper place of custody or delivered to anyone or to be lost, stolen, abstracted, or destroyed. The bill explicitly states that "gross negligence," for these purposes, includes extreme or reckless carelessness.

6) **S.3084 – American Innovation and Competitiveness Act**

**Sponsor:** Sen. Gardner, Cory [R-CO] (Introduced 06/22/2016)

**Latest Action:** 12/01/2016 Committee on Commerce, Science, and Transportation. Placed on Senate Legislative Calendar under General Orders. Calendar No. 695. 3 cosponsors

**Bill Summary**
The National Institute of Standards and Technology (NIST) shall: (1) research information systems for future cybersecurity needs; and (2) develop a process to
research and identify, or if necessary, develop cryptography standards and guidelines for future cybersecurity needs, including quantum-resistant cryptography standards.


Sponsor: Sen. Vitter, David [R-LA] (Introduced 06/06/2016)
Latest Action: 06/09/2016 Placed on Senate Legislative Calendar under General Orders. Calendar No. 511. 2 cosponsors.

Bill Summary
This bill amends the Small Business Act to authorize the Small Business Administration (SBA) to make grants to small business development centers (SBDCs) in furtherance of a Small Business Development Center Cyber Strategy to be developed by the SBA and the DHS after the GAO submits a report that reviews the cybersecurity resources of federal agencies aimed at assisting small businesses.
SBDCs shall provide access to external cyber security specialists to counsel small businesses.
DHS and other federal agencies coordinating with DHS may assist SBDCs, through the dissemination of cyber security risk information and other homeland security information, to help small businesses in developing such cyber security infrastructure, threat awareness, and employee training programs.

8) S. 3018 – Securing Energy Infrastructure Act

Sponsor: Sen. King, Angus S., Jr. [I-ME] (Introduced 06/06/2016)
Latest Action: 07/12/2016 Committee on Energy and Natural Resources Subcommittee on Energy. Hearings held. 5 cosponsors.

Bill Summary
To provide for the establishment of a pilot program to identify security vulnerabilities of certain entities in the energy sector.


Sponsor: Sen. Ernst, Joni [R-IA] (Introduced 05/23/2016)
Latest Action: 09/27/2016 Committee on Homeland Security and Governmental Affairs. Placed on Senate Legislative Calendar under General orders. Calendar No. 647. 0 cosponsors

Bill Summary
To provide agencies with discretion in securing information technology and information systems. In carrying out section 3554 of title 44, United States Code,
any action taken by the head of an agency that is necessary to limit, restrict, or prohibit access to any website the head of the agency determines to present a current or future security weakness or risk to the information technology or information system under the control of the agency, and any impact or implementation of such action, shall not be subject to chapter 71 of title 5, United States Code.

10) S. 2931 – Botnet Prevention Act of 2016

Sponsor: Sen. Graham, Lindsey [R-SC] (Introduced 05/16/2016)
Latest Action: 05/18/2016 Committee on the Judiciary Subcommittee on Crime and Terrorism. Hearings held. 2 cosponsors.

Bill Summary
To amend title 18, United States Code, to protect Americans from cybercrime.

11) S. 2905 – Cyber Act of War Act of 2016

Sponsor: Sen. Rounds, Mike [R-SD] (Introduced 05/09/2016)
Latest Action: 05/09/2016 Read twice and referred to the Committee on Foreign Relations. 1 cosponsor.

Bill Summary
This bill directs the President to: develop a policy for determining when an action carried out in cyberspace constitutes an act of war against the United States, and revise the Department of Defense Law of War Manual accordingly. In developing this policy, the President shall consider: the ways in which a cyber attack's effects may be equivalent to a conventional attack's effects, including physical destruction or casualties; and intangible effects of significant scope or duration.

12) S. 2764 – Cyber AIR Act

Latest Action: 04/07/2016 Read twice and referred to the Committee on Commerce, Science, and Transportation. 0 cosponsor.

Bill Summary
This bill directs the Department of Transportation (DOT) to require domestic or foreign air carriers and manufacturers of aircraft or electronic control, communications, maintenance, or ground support systems for aircraft to disclose to the Federal Aviation Administration (FAA) any attempted or successful cyberattack against any system on board an aircraft or against any maintenance or ground support system for aircraft.
13) S. 2756 – Iran Cyber Sanctions Act of 2016

**Sponsor:** Sen. Rounds, Mike [R-SD] (Introduced 04/06/2016)

**Latest Action:** 04/06/2016 Read twice and referred to the Committee on Banking, Housing, and Urban Affairs. 4 cosponsors.

**Bill Summary**
This bill requires the President to report to Congress at least every 180 days regarding significant activities undermining cybersecurity conducted by Iranian persons against the United States or U.S. persons. The reports must: (1) identify Iranians involved in such activities; (2) describe their conduct; (3) assess the Iranian government's or other foreign governments' material support for such activities; and (4) provide a strategy to counter efforts by Iranian persons to conduct such activities, which shall include engaging foreign governments to halt the capabilities of such Iranian persons.

14) S. 2665 – State and Local Cyber Protection Act of 2016

**Sponsor:** Sen. Peters, Gary C. [D-MI]

**Latest Action:** 03/10/2016 Read twice and referred to the Committee on Homeland Security and Governmental Affairs. 1 cosponsor.

**Bill Summary**
This bill amends the Homeland Security Act of 2002 to require the Department of Homeland Security's (DHS's) national cybersecurity and communications integration center (NCCIC) to assist state and local governments with cybersecurity.

15) S. 2410 – Cybersecurity Disclosure Act of 2015

**Sponsor:** Sen. Reed, Jack [D-RI] (Introduced 12/17/2015)

**Latest Action:** 12/17/2015 Read twice and referred to the Committee on Banking, Housing, and Urban Affairs. (Sponsor introductory remarks on measure: CR S8795). 1 cosponsor.

**Bill Summary**
Requires publicly traded companies to disclose in filings with the SEC whether anyone on the board is a cybersecurity expert. If the company does not have one, it will need to explain why an expert is not necessary and that it is taking additional measures to protect data.
16) **S. 2144 – North Korea Sanctions and Policy Enhancement Act of 2015**

* Sponsor: Sen. Gardner, Cory [R-CO] (Introduced 10/06/2015)*
* Latest Action: 10/06/2015 Read twice and referred to the Committee on Foreign Relations. 18 cosponsors.*

**Bill Summary**
Directs the President to investigate information of sanctionable activities involving North Korea and to designate and apply sanctions with respect to any person that knowingly engaged in significant activities undermining cybersecurity through the use of computer networks or systems against foreign persons, governments, or other entities.

17) **S. 2007 – Federal Cybersecurity Workforce Assessment Act**

* Sponsor: Sen. Bennet, Michael F. [D-CO] (Introduced 08/06/2015)*
* Latest Action: 08/06/2015 Read twice and referred to the Committee on Homeland Security and Governmental Affairs. 1 cosponsor.*

**Bill Summary**
This bill requires federal agencies to: (1) identify all personnel positions that require the performance of information technology, cybersecurity, or other cybersecurity-related functions; and (2) assign a corresponding employment code to such positions using a coding structure that the National Institute of Standards and Technology must include in the National Initiative for Cybersecurity Education's National Cybersecurity Workforce Framework.

18) **S. 1869 – Federal Cybersecurity Enhancement Act of 2015**

* Latest Action: 11/17/2016 Placed on Senate Legislative Calendar under General orders. Calendar No. 673. 1 cosponsor.*

**Bill Summary**
Amends the Homeland Security Act of 2002 to require the Department of Homeland Security (DHS), in coordination with the Office of Management and Budget (OMB), to implement an intrusion assessment plan to identify and remove intruders in federal agency information systems.

19) **S. 1806 – SPY Car (Security and Privacy in Your Car) Act of 2015**

* Sponsor: Sen. Markey, Edward J. [D-MA]*
* Latest Action: 07/21/2015 Read twice and referred to the Committee on Commerce, Science, and Transportation. 1 cosponsor.*
**Bill Summary**
This bill directs the National Highway Traffic Safety Administration (NHTSA) to conduct a rulemaking to issue motor vehicle cybersecurity regulations that require motor vehicles manufactured for sale in the United States to protect against unauthorized access to: (1) electronic controls or driving data, including information about the vehicle's location, speed, owner, driver, or passengers; or (2) driving data collected by electronic systems built into a vehicle while that data is stored onboard the vehicle, in transit from the vehicle to another location, or subsequently stored or used off-board the vehicle. The regulations must require vehicles with accessible data or control signals to be capable of detecting, reporting, and stopping attempts to intercept such driving data or control the vehicle.

20) **S. 1241 – Enhanced Grid Security Act of 2015**

**Sponsor:** Sen. Cantwell, Maria [D-WA] (Introduced 05/07/2015)

**Latest Action:** 06/09/2015 Committee on Energy and Natural Resources. Hearings held.

**Bill Summary**
This bill designates the Department of Energy (DOE) as the lead Sector-Specific Agency for cybersecurity for the energy sector (this action comports with the presidential policy directive entitled "Critical Infrastructure Security and Resilience" dated February 12, 2013).

21) **S. 1030 - Aaron's Law Act of 2015**

**Sponsor:** Sen. Wyden, Ron [D-OR] (Introduced 04/21/2015)

**Latest Action:** 04/21/2015 Read twice and referred to the Committee on the Judiciary. (text of measure as introduced: CR S2304-2305). 1 cosponsor.

**Bill Summary**
Amends provisions of the Computer Fraud and Abuse Act (CFAA) prohibiting computer fraud to replace the phrase "exceeds authorized access" with "access without authorization," which is defined as obtaining information on a protected computer that the accessed lacks authorization to obtain by knowingly circumventing one or more technological or physical measures that are designed to exclude or prevent unauthorized individuals from obtaining that information.

Modifies CFAA penalty provisions to: (1) limit the imposition of enhanced penalties to subsequent offenses under such Act (currently, additional penalties are allowed if there is a conviction for another offense) and to criminal acts punishable under federal or state law by a term of imprisonment for more than one year; and (2) require the determination of the value of information for enhanced penalty purposes to be made by reference to fair market value.
22) S. 1027 - Data Breach Notification and Punishing Cyber Criminals Act of 2015

**Sponsor:** Sen. Kirk, Mark Steven [R-IL] (Introduced 04/21/2015)
**Latest Action:** 04/21/2015 Read twice and referred to the Committee on Commerce, Science, and Transportation. 1 cosponsor.

**Bill Summary**
The Data Breach Notification and Punishing Cyber Criminals Act sets a stronger standard for companies to notify in their data has been breached, and increases penalties for cybercrimes. The bill raises the maximum allowable fines and imprisonment for many of the statutes which cyber criminals are charged: identity theft, conspiracy to commit access device fraud, obtaining information from a protected computer without authorization and computer hacking with intent to defraud. It requires consumers to receive notification within 30 days of discovery of data breaches with a description of information potentially accessed, how to inquire about what personal information was breached, and how the information was unlawfully acquired. There will be a new directive for diplomats at the State Department for apprehending and prosecuting cyber criminals as a top priority in ongoing negotiations in countries that do not have an extradition with United States.

23) S. 456 – Cyber Threat Sharing Act of 2015

**Sponsor:** Sen. Carper, Thomas R. [D-DE] (Introduced 02/11/2015)
**Latest Action:** 02/11/2015 Read twice and referred to the Committee on Homeland Security and Governmental Affairs. 0 cosponsor.

**Bill Summary**
Amends the Homeland Security Act of 2002 to permit private entities to: (1) disclose lawfully obtained cyber threat indicators to a private information sharing and analysis organization and the national cybersecurity and communications integration center (NCCIC); and (2) receive indicators disclosed by private entities, the federal government, or state or local governments.


**Sponsor:** Sen. Lee, Mike [R-UT] (Introduced 02/04/2015)
**Latest Action:** 09/16/2015 Committee on the Judiciary. Hearings held. 30 cosponsors.
Bill Summary
Amends the Electronic Communications Privacy Act of 1986 to prohibit a provider of remote computing service or electronic communication service to the public from knowingly divulging to a governmental entity the contents of any communication that is in electronic storage or otherwise maintained by the provider, subject to exceptions.


Latest Action: 1/13/2015 Referred to the Committee on Commerce, Science, and Transportation. 1 cosponsor.

Bill Summary
Protects consumers by requiring “reasonable” security policies and procedures to protect data containing personal information, and provides for nationwide notice in the event of a breach.

V. CISA PASSAGE IN OMNIBUS

H.R. 2029, or the Consolidated Appropriations Act, 2016, was passed with the Cybersecurity Act of 2015 in it. This Act broadened the powers of network operators to monitor their networks for cybersecurity threats, and if deemed to be such, share that information with the Department of Homeland Security. The bill has a requirement that the private sector assess whether any information it is sharing with the Federal government is "not directly related" to a cyber threat and whether it "knows at the time of sharing" that this non-direct information contains personal information of a specific individual or identifies an individual. These private entities must use technical means to scrub that information from what they forward to the government.

In addition to sharing for cybersecurity purposes, the cyber threat information may only be shared for the purpose of responding to, preventing, or mitigating a specific threat of "death or serious bodily injury" or "serious economic harm." Private entities will have liability protection for information sharing activity that is "conducted in accordance" with the bill's provisions.

H Res 727 (Langevin, D-RI), supporting the Commission on Enhancing National Cybersecurity; to Science, Space, and Technology, and Oversight and Government Reform. CR 5/12/16, H2341.

For more information, please contact David Eppstein at david.eppstein@americanbar.org.