Cybersecurity: Legislation, Hearings, and Executive Branch Documents

Rita Tehan
Information Research Specialist

February 1, 2018

Congressional Research Service
7-5700
www.crs.gov
R43317

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

Cybersecurity vulnerabilities challenge governments, businesses, and individuals worldwide. Attacks have been initiated against individuals, corporations, and countries. Targets have included government networks, companies, and political organizations, depending upon whether the attacker was seeking military intelligence, conducting diplomatic or industrial espionage, engaging in cybercrime, or intimidating political activists. In addition, national borders mean little or nothing to cyberattackers, and attributing an attack to a specific location can be difficult, which may make responding problematic.

Despite many recommendations made over the past decade, most major legislative provisions relating to cybersecurity had been enacted prior to 2002. However, on December 18, 2014, five cybersecurity bills were signed by the President. These bills changed federal cybersecurity programs in a number of ways:

- codifying the role of the National Institute of Standards and Technology (NIST) in developing a "voluntary, industry-led set of standards" to reduce cyber risk;
- codifying the Department of Homeland Security's (DHS's) National Cybersecurity and Communications Integration Center as a hub for interactions with the private sector;
- updating the Federal Information Security Management Act (FISMA) by requiring the Office of Management and Budget (OMB) to "eliminate ... inefficient and wasteful reports"; and
- requiring DHS to develop a "comprehensive workforce strategy" within a year and giving DHS new authorities for cybersecurity hiring.

This report provides links to cybersecurity legislation in the 112th, 113th, 114th, and 115th Congresses. Congress has held cybersecurity hearings every year since 2001. This report also provides links to cybersecurity-related committee hearings in the 113th, 114th, and 115th Congresses.

In the 115th Congress, 12 bills have received committee consideration or passed one or both chambers.

In the 114th Congress, the House passed eight bills:

- H.R. 1073, Critical Infrastructure Protection Act.
- H.R. 1560, Protecting Cyber Networks Act.
- H.R. 1731, National Cybersecurity Protection Advancement Act of 2015.
- H.R. 3490, Strengthening State and Local Cyber Crime Fighting Act.
- H.R. 3510, Department of Homeland Security Cybersecurity Strategy Act of 2015.
- H.R. 3869, State and Local Cyber Protection Act of 2015.
- H.R. 3878, Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2015.
- H.R. 4743, National Cybersecurity Preparedness Consortium Act of 2016.

The Senate passed one bill in the 114th Congress:

- S. 754, Cybersecurity Information Sharing Act of 2015.

On December 18, 2015, H.R. 2029, the Consolidated Appropriations Act, was signed into public law (P.L. 114-113). The omnibus law's cybersecurity provisions are located in Division N (Cybersecurity Act of 2015), including Title I, Cybersecurity Information Sharing; Title II, National Cybersecurity Advancement; Title III, Federal Cybersecurity Workforce Assessment; and Title IV, Other Cyber Matters. The measure represents a compromise between the House and Senate intelligence committees and the House Homeland Security Committee. It includes various components of three separate information sharing bills: H.R. 1560 and H.R. 1731, passed by the House in April 2015, and S. 754, passed by the Senate in October 2015. The bill encourages private companies to voluntarily share information about cyber threats with each other as well as the government. Firms that participate in the information sharing will receive liability protection.

Executive orders authorize the President to manage federal government operations. Presidential directives pertain to all aspects of U.S. national security policy as authorized by the President. This report provides a list of executive orders and presidential directives pertaining to information and computer security.

Contents

Tables

Contacts

Summary of Legislation

Most major legislative provisions relating to cybersecurity had been enacted prior to 2002, despite many recommendations made over the past decade.

112th Congress: Summary of Legislative Action

In the 112th Congress, the White House sent a comprehensive, seven-part legislative proposal (*White House Proposal*) to Congress on May 12, 2011.[1] Some elements of that proposal were included in both House and Senate bills. The House passed a series of bills that addressed a variety of issues—from toughening law enforcement of cybercrimes to giving the Department of Homeland Security (DHS) oversight of federal information technology and critical infrastructure security to lessening liability for private companies that adopt cybersecurity best practices. The Senate pursued a comprehensive cybersecurity bill (S. 3414) with several committees working to create a single vehicle for passage, backed by the White House, but the bill failed to overcome two cloture votes and did not pass. Despite the lack of enactment of cybersecurity legislation in the 112th Congress, there still appears to be considerable support in principle for significant legislation to address most of the issues.

113th Congress: Summary of Legislative Action

In the 113th Congress, five cybersecurity bills were signed by the President on December 18, 2014:

- H.R. 2952, the Cybersecurity Workforce Assessment Act, which requires the DHS to develop a cyber-workforce strategy;
- S. 1353, the Cybersecurity Enhancement Act of 2014, which codifies the National Institute of Standards and Technology's (NIST's) role in cybersecurity;
- S. 1691, the Border Patrol Agent Pay Reform Act of 2014, which gives DHS new authorities for cybersecurity hiring;
- S. 2519, the National Cybersecurity Protection Act of 2014, which codifies DHS's cybersecurity center; and
- S. 2521, the Federal Information Security Modernization Act of 2014, which reforms federal IT security management.

The National Defense Authorization Act for Fiscal Year 2014 became P.L. 113-66 on December 26, 2013.

In February 2013, the White House issued an executive order designed to improve the cybersecurity of U.S. critical infrastructure.[2] Executive Order 13636 attempts to enhance the security and resiliency of critical infrastructure through voluntary, collaborative efforts involving federal agencies and owners and operators of privately owned critical infrastructure, as well as the use of existing federal regulatory authorities. Given the absence of comprehensive cybersecurity legislation, some security observers contend that E.O. 13636 is a necessary step in

[1] The White House, Complete Cybersecurity Proposal, 2011, https://obamawhitehouse.archives.gov/sites/default/files/omb/legislative/letters/law-enforcement-provisions-related-to-computer-security-full-bill.pdf.

[2] Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," *Federal Register* 78, no. 33 (February 19, 2013): 11737–11744.

securing vital assets against cyberthreats. Others have expressed the view that the executive order could make enactment of a bill less likely or could lead to government intrusiveness into private-sector activities through increased regulation under existing statutory authority. For further discussion of the executive order, see CRS Report R42984, *The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress*, by Eric A. Fischer et al.

114th Congress: Summary of Legislative Action

In February 2015, the White House issued Executive Order 13691,[3] which, along with a legislative proposal, is aimed at enhancing information sharing in cybersecurity among private sector entities. It promotes the use of information sharing and analysis organizations (ISAOs), which were defined in the Homeland Security Act (6 U.S.C. §131(5)) as entities that gather, analyze, and share information on the security of critical infrastructure (CI)[4] to assist in defense against and recovery from incidents. The White House initiatives would broaden the reach of ISAOs beyond CI to any affinity group. In that sense, they differ from the more familiar information sharing and analysis centers (ISACs), created in response to Presidential Decision Directive (PDD) 63 in 1998 specifically to address information-sharing needs in CI sectors.

Also in February 2015, the Obama Administration established, via presidential memorandum,[5] the Cyber Threat Intelligence Integration Center (CTIIC) to be established by the Director of National Intelligence (DNI). Its purposes are to provide integrated analysis on foreign cybersecurity threats and incidents affecting national interests and to support relevant government entities, including the National Cybersecurity and Communications Integration Center (NCCIC) at the Department of Homeland Security (DHS), as well as others at the Department of Defense (DOD) and Department of Justice (DOJ).

More than 20 bills have been introduced in the 114th Congress that would address several issues, including data-breach notification, incidents involving other nation-states, information sharing, law enforcement and cybercrime, protection of critical infrastructure (CI), workforce development, and education. The Obama Administration has released proposals for three bills—on information sharing, data-breach notification, and revision of cybercrime laws. Several bills have received or are expected to receive committee or floor action.

On April 22, 2015, the House passed H.R. 1560, which will provide liability protection to companies that share cyber threat information with the government and other companies so long as personal information is removed before the sharing of such information. On April 23, 2015, the House passed H.R. 1731, which will encourage information sharing with the Department of Homeland Security by protecting entities from civil liabilities.

On October 27, 2015, the Senate passed S. 754, the Cybersecurity Information Sharing Act of 2015 (CISA), by a vote of 74-21 (Roll call vote 291). The House approved companion legislation in April, so the cybersecurity measure is now on track to reach President Obama's desk and be signed into law, once a conference report is negotiated. CISA attempts to open up communication

[3] E.O. 13691, Encouraging Private-Sector Cybersecurity Collaboration, White House, February 12, 2015, at http://www.whitehouse.gov/the-press-office/2015/02/12/fact-sheet-executive-order-promoting-private-sector-cybersecurity-inform.

[4] PDD-63, Critical Infrastructure Protection, White House, May 22, 1998, at http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.

[5] Presidential Memorandum—Establishment of the Cyber Threat Intelligence Integration Center. White House, February 25, 2015, at http://www.whitehouse.gov/the-press-office/2015/02/25/presidential-memorandum-establishment-cyber-threat-intelligence-integrat.

channels between industry and federal agencies by offering legal immunity to companies that share data with the government. For more information on what is covered in the Senate bill, see CRS Legal Sidebar WSLG1429, *Senate Passes Cybersecurity Information Sharing Bill –What's Next?*, by Andrew Nolan.

On November 30, 2015, the House passed H.R. 3490, which would establish in the Department of Homeland Security 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. On December 10, 2015, the House passed H.R. 3869, the State and Local Cyber Protection Act of 2015, which requires the Department of Homeland Security's (DHS's) national cybersecurity and communications integration center (NCCIC) to assist state and local governments with cybersecurity, and on December 16, 2015, the House passed H.R. 3878, Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2015, which requires DHS to seek to enhance cybersecurity situational awareness and information sharing between and with maritime security stakeholders from federal, state, local, and tribal governments, public safety and emergency response agencies, law enforcement and security organizations, maritime industry participants, port owners and operators, and maritime terminal owners and operators.

On December 18, 2015, H.R. 2029, the Consolidated Appropriations Act, was signed into public law (P.L. 114-113). The omnibus law's cybersecurity provisions are located in Division N (Cybersecurity Act of 2015), including Title I, Cybersecurity Information Sharing; Title II, National Cybersecurity Advancement; Title III, Federal Cybersecurity Workforce Assessment; and Title IV, Other Cyber Matters. The measure represents a compromise between the House and Senate intelligence committees and the House Homeland Security Committee. It includes various components of three separate information sharing bills: H.R. 1560 and H.R. 1731, passed by the House in April 2015, and S. 754, passed by the Senate in October 2015. The bill encourages private companies to voluntarily share information about cyber threats with each other as well as the government. Firms that participate in the information sharing will receive liability protection.

115th Congress: Summary of Legislative Action

Twelve bills have received committee consideration or passed one or both chambers in the 115th Congress. See **Table 1** and **Table 2** for a list of these bills.

CRS Reports and Other CRS Products: Legislation

- CRS Report R43831, *Cybersecurity Issues and Challenges: In Brief*, by Eric A. Fischer
- CRS In Focus IF10610, *Cybersecurity Legislation in the 113th and 114th Congresses*, by Eric A. Fischer
- CRS Report R44069, *Cybersecurity and Information Sharing: Comparison of H.R. 1560 (PCNA and NCPAA) and S. 754 (CISA)*, by Eric A. Fischer
- CRS Report R43996, *Cybersecurity and Information Sharing: Comparison of H.R. 1560 and H.R. 1731 as Passed by the House*, by Eric A. Fischer and Stephanie M. Logan
- CRS Report R42114, *Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation*, by Eric A. Fischer
- CRS Report R43821, *Legislation to Facilitate Cybersecurity Information Sharing: Economic Analysis*, by N. Eric Weiss
- CRS Report R42475, *Data Security Breach Notification Laws*, by Gina Stevens

Legislation in the 115th, 114th, and 113th Congresses

The following tables list House and Senate bills in the 115th, 114th, and 113th Congresses. Thus far, in the 115th Congress, 12 bills have received committee consideration, or passed one or both chambers. **Table 1** is a list of House bills in the 115th Congress, and **Table 2** is a list of Senate bills. **Table 3** and **Table 4** list bills in the 114th Congress. **Table 5** and **Table 6** list bills in the 113th Congress.

Table 1. 115th Congress Legislation: House

Bill No.	Title	Committee(s)	Date Introduced	Latest Major Action	Date
H.R. 239	Support for Rapid Innovation Act of 2017	Homeland Security	January 4, 2017	Passed House	January 10, 2017
H.R. 584	Cyber Preparedness Act of 2017	Homeland Security	January 17, 2017	Passed House	January 31, 2017
H.R. 589	Department of Energy Research and Innovation Act	Science, Space, and Technology	January 20, 2017	Passed House	January 24, 2017
H.R. 612	United States-Israel Cybersecurity Cooperation Enhancement Act of 2017	Homeland Security	January 23, 2017	Passed House	January 31, 2017
H.R. 1224	NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017	Science, Space, and Technology	February 27, 2017	Ordered to be reported by Yeas and Nays: 19-14	March 1, 2017
H.R. 1616	Strengthening State and Local Cyber Crime Fighting Act of 2017	Judiciary, Homeland Security	May 16, 2017	Became Public Law (P.L. 115-76)	November 2, 2017
H.R. 2105	NIST Small Business Cybersecurity Act	Science, Space and Technology	April 20, 2017	Passed House by voice vote	October 11, 2017
H.R. 2227	Modernizing Government Technology Act	Appropriations	April 28, 2017	Passed House by voice vote	May 17, 2017
H.R. 3101	Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2017	House - Homeland Security, Transportation and Infrastructure | Senate - Commerce, Science, and Transportation	June 28, 2017	Passed House by voice vote	October 24, 2017
H.R. 3202	Cyber Vulnerability Disclosure Reporting Act	Homeland Security and Governmental Affairs.	July 12, 2017	Passed House by voice vote	January 9, 2018

Bill No.	Title	Committee(s)	Date Introduced	Latest Major Action	Date
H.R. 3359	Cybersecurity and Infrastructure Security Agency Act of 2017	Homeland Security; Energy and Commerce; Oversight and Government Reform; Transportation and Infrastructure	July 24, 2017	Passed House by voice vote	December 11, 2017
H.R. 3776	Cyber Diplomacy Act of 2017	Foreign Affairs	September 14, 2017	Passed House by voice vote	January 17, 2018

Source: Compiled by the Congressional Research Service (CRS) from Congress.gov.

Note: This list includes bills with committee action or a House vote.

Table 2. 115th Congress Legislation: Senate

Bill No.	Title	Committee(s)	Date Introduced	Latest Major Action	Date
S. 79	Securing Energy Infrastructure Act	Energy and Natural Resources	January 10, 2017	Subcommittee hearing held	March 28, 2017
S. 770	MAIN STREET Cybersecurity Act of 2017	Commerce, Science, and Transportation	March 29, 2017	Passed Senate	September 28, 2017
S. 782	PROTECT Our Children Act of 2017	Judiciary	March 30, 2017	Became Public Law (P.L. 115-82)	November 2, 2017

Source: Compiled by the Congressional Research Service (CRS) from Congress.gov.

Note: This list includes bills with committee action or a Senate vote.

Table 3. 114th Congress Legislation: House

Bill No.	Title	Committee(s)	Date Introduced	Latest Major Action	Date
H.R. 451	Safe and Secure Federal Websites Act of 2015	Oversight and Government Reform	January 21, 2015	Reported (amended) by the committee	January 6, 2016

Bill No.	Title	Committee(s)	Date Introduced	Latest Major Action	Date
H.R. 1073	Critical Infrastructure Protection Act (CIPA)	Homeland Security	February 25, 2015	Measure, as amended, passed in the House by voice vote, under suspension of the rules (two-thirds vote required)	November 16, 2015
H.R. 1560	Protecting Cyber Networks Act	Intelligence	March 24, 2015	Passed by House April 22, Roll Cal Vote 170, Received in Senate	April 22, 2015
H.R. 1731	National Cybersecurity Protection Advancement Act	Homeland Security	April 14, 2015	Passed House, Roll Call Vote 173	April 23, 2015
H.R. 1770	Data Security and Breach Notification Act of 2015	Energy and Commerce	April 14, 2015	Reported (Amended) by the Committee	January 3, 2017
H.R. 2029[6]	Consolidated Appropriations Act	Appropriations	April 24, 2015	Became P.L. 114-113	December 18, 2015
H.R. 2205	Data Security Act of 2015	Energy and Commerce; Financial Services	May 1, 2015	Ordered to be Reported (Amended) by the Yeas and Nays: 46 - 9	December 9, 2015
H.R. 3490	Strengthening State and Local Cyber Crime Fighting Act	Homeland Security and Judiciary	September 11, 2015	Passed House (Amended) by voice vote	November 30, 2015
H.R. 3510	Department of Homeland Security Cybersecurity Act of 2015	Homeland Security	September 17, 2015	Passed House by voice vote	October 6, 2015
H.R. 3869	State and Local Cyber Protection Act of 2015	Homeland Security	November 2, 2015	Passed House	December 10, 2015

[6] The omnibus law's cybersecurity provisions are located in Division N (Cybersecurity Act of 2015), including Title I, Cybersecurity Information Sharing, Title II, National Cybersecurity Advancement, Title III, Federal Cybersecurity Workforce Assessment, and Title IV, Other Cyber Matters. The measure represents a compromise between the House and Senate intelligence committees and the House Homeland Security Committee. It includes various components of three separate information sharing bills: H.R. 1560 and H.R. 1731, passed by the House in April 2015, and S. 754, passed by the Senate in October 2015.

Bill No.	Title	Committee(s)	Date Introduced	Latest Major Action	Date
H.R. 3878	Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2015	Homeland Security; Transportation and Infrastructure	November 2, 2015	Passed House by voice vote	December 16, 2015
H.R. 4743	National Cybersecurity Preparedness Consortium Act of 2016	House Homeland Security and Senate Homeland Security and Governmental Affairs	March 15, 2016	Passed House	May 16, 2016
H.R. 5064	Improving Small Business Cyber Security Act of 2016	Small Business, Homeland Security	April 26, 2016	Reported by Homeland Security Committee	July 1, 2016
H.R. 5459	Cyber Preparedness Act of 2016	Homeland Security	June 16, 2016	Passed House	September 26, 2016
H.R. 6032	Data Breach Insurance Act	Ways and Means	September 14, 2016	Referred to committee	

Source: Compiled by the Congressional Research Service (CRS) from Congress.gov.

Note: This list includes bills with committee action or a House vote.

Table 4. 114th Congress Legislation: Senate

Bill No.	Title	Committee(s)	Date Introduced	Latest Major Action	Date
H.R. 2029[7]	Consolidated Appropriations Act	Appropriations	April 24, 2015	Became P.L. 114-113	December 18, 2015
S. 135	Secure Data Act of 2015	Commerce, Science, and Transportation	January 8, 2015	Referred to committee	January 8, 2015
S. 177	Data Security and Breach Notification Act of 2015	Commerce, Science, and Transportation	January 13, 2015	Referred to committee	January 13, 2015
S. 456	Cyber Threat Sharing Act of 2015	Homeland Security and Governmental Affairs	February 11, 2015	Referred to committee	February 11, 2015
S. 754	Cybersecurity Information Sharing Act of 2015	Intelligence	March 17, 2015	Passed Senate 74-21, Roll Call Vote 291	October 27, 2015
S. 1027	Data Breach Notification and Punishing Cyber Criminals Acts of 2015	Commerce, Science and Transportation	April 21, 2015	Referred to committee	April 21, 2015
S. 1241	Enhanced Grid Security Act of 2015	Energy and Natural Resources	May 7, 2015	Hearings held	June 9, 2015

Source: Compiled by CRS from Congress.gov.

[7] The omnibus law's cybersecurity provisions are located in Division N (Cybersecurity Act of 2015), including Title I, Cybersecurity Information Sharing, Title II, National Cybersecurity Advancement, Title III, Federal Cybersecurity Workforce Assessment, and Title IV, Other Cyber Matters. The measure represents a compromise between the House and Senate intelligence committees and the House Homeland Security Committee. It includes various components of three separate information sharing bills: H.R. 1560 and H.R. 1731, passed by the House in April 2015, and S. 754, passed by the Senate in October 2015.

Table 5. 113th Congress, Major Legislation: Senate

Bill No.	Title	Committee(s)	Date Introduced	Latest Major Action	Date
S. 2588	Cybersecurity Information Sharing Act of 2014	Intelligence	July 10, 2014	Reported to Senate without written report	July 10, 2014
S. 2521	Federal Information Security Modernization Act of 2014	Homeland Security and Government Affairs	June 24, 2014	P.L. 113-283	December 18, 2014
S. 2519	National Cybersecurity and Communications Integration Center Act of 2014	Homeland Security and Governmental Affairs	June 24, 2014	P.L. 113-282	December 18, 2014
S. 2410	Carl Levin National Defense Authorization Act for Fiscal Year 2015	Armed Services	June 2, 2014	With written S.Rept. 113-176	June 2, 2014
S. 2354	DHS Cybersecurity Workforce Recruitment and Retention Act of 2014	Homeland Security and Government Affairs	May 20, 2014	With written S.Rept. 113-207	July 14, 2014
S. 1927	Data Security Act of 2014	Banking, Housing, and Urban Affairs	January 15, 2014	Subcommittee on National Security and International Trade and Finance hearings held	February 3, 2014
S. 1691	Border Patrol Agent Pay Reform Act of 2014	Senate Homeland Security and Governmental Affairs; House Oversight and Government Reform; House Homeland Security	November 13, 2013	P.L. 113-277	December 18, 2014
S. 1353	Cybersecurity Act of 2013	Commerce, Science, and Transportation	July 24, 2013	P.L. 113-274	December 18, 2014
S. 1197	National Defense Authorization for Fiscal Year 2014	Armed Services	June 20, 2013	P.L. 113-66	December 26, 2013

Source: Legislative Information System (LIS).

Table 6. 113th Congress, Major Legislation: House

Bill No.	Title	Committee(s)	Date Introduced	Latest Major Action	Date
H.R. 4435	National Defense Authorization Act for Fiscal Year 2015	Armed Services	April 9, 2014	Passed/agreed to in House, Roll no. 240	May 22, 2014
H.R. 3696	National Cybersecurity and Critical Infrastructure Protection Act	Homeland Security and House Science, Space, and Technology	December 11, 2013	Passed/agreed to in House, by voice vote	July 28, 2014
H.R. 3635	Safe and Secure Federal Websites Act of 2014	House Oversight and Government Reform; Senate Homeland Security and Governmental Affairs	December 3, 2013	Passed House by voice vote	July 28, 2014
H.R. 3304	National Defense Authorization Act for Fiscal Year 2014	House Armed Services; Senate Armed Services	October 22, 2013	P.L. 113-66	December 26, 2013
H.R. 3107	Homeland Security Cybersecurity Boots-on-the-Ground Act	Homeland Security	September 17, 2013	Passed/agreed to in House, Roll No. 457	July 28, 2014
H.R. 2952	Critical Infrastructure Research and Development Advancement Act of 2013	Homeland Security	August 1, 2013	P.L. 113-246	December 18, 2014
H.R. 1163	Federal Information Security Amendments Act of 2013	Oversight and Government Reform	March 14, 2013	Passed House. Referred to Senate Committee on Homeland Security and Governmental Affairs	April 17, 2013
H.R. 967	Advancing America's Networking and Information Technology Research and Development Act of 2013	Science, Space, and Technology	March 14, 2013	Passed House, Roll No. 108. Referred to the Senate Commerce, Science, and Transportation Committee	April 17, 2013
H.R. 756	Cybersecurity R&D [Research and Development]	Science, Space, and Technology	February 15, 2013	Passed House, Roll no. 107. Congressional Record text	April 16, 2013
H.R. 624	Cyber Intelligence Sharing and Protection Act (CISPA)	Permanent Select Committee on Intelligence	February 13, 2013	Passed House. Roll no. 117. Referred to Senate Select Committee on Intelligence	April 18, 2013

Source: LIS.

Hearings in the 115th Congress

The following tables list cybersecurity hearings in the 115th Congress. The tables contain identical content but are organized differently.

Table 7 lists House hearings arranged by date (most recent first), and **Table 8** lists House hearings arranged by committee. **Table 9** lists Senate hearings by date. **Table 10** lists Senate hearings arranged by committee. When viewed in HTML, the document titles are active links to the committee's website for that particular hearing.

Table 7. 115th Congress, House Hearings by Date

Title	Date	Committee	Subcommittee
Small Business Information Sharing: Combating Foreign Cyber Threats	January 30, 2018	Small Business	
CDM, The Future of Federal Cybersecurity?	January 17, 2018	Homeland Security	Cybersecurity and Infrastructure Protection
Examining the Role of the Department of Energy in Energy Sector Cybersecurity	December 8, 2017	Energy and Commerce	Oversight and Investigations
Oversight of IT and Cybersecurity at the Department of Veterans Affairs	December 7, 2017	Oversight and Government Reform	Information Technology
Implementation and Cybersecurity Protocols of the Consolidated Audit Trail	November 30, 2017	Financial Services	Capital Markets, Securities, and Investment Hearing
Cybersecurity of Voting Machines	November 29, 2017	Oversight and Government Reform	Information Technology
Maximizing the Value of Cyber Threat Information Sharing	November 15, 2017	Homeland Security	Cybersecurity and Infrastructure Protection
Federal Government and Small Businesses: Promoting Greater Information Sharing for Stronger Cybersecurity	November 15, 2017	Small Business	
Bolstering the Government's Cybersecurity: A Survey of Compliance with the DHS Directive	November 14, 2017	Science, Space & Technology	Oversight
Securing Consumers' Credit Data in the Age of Digital Commerce	November 1, 2017	Energy and Commerce	Digital and Consumer Protection
Data Security: Vulnerabilities and Opportunities for Improvement	November 1, 2017	Financial Services	Financial Institutions and Consumer Credit
Examining Physical Security and Cybersecurity at Our Nation's Ports (Field Hearing)	October 30, 2017	Homeland Security	

Title	Date	Committee	Subcommittee
Bolstering the Government's Cybersecurity: Assessing the Risk of Kaspersky Lab Products to the Federal Government	October 25, 2017	Science, Space & Technology	Oversight
Continuation of Hearing entitled "Examining the Equifax Data Breach	October 25, 2017	Financial Services	
Public-Private Solutions to Educating a Cyber Workforce	October 24, 2017	Homeland Security	Cybersecurity and Infrastructure Protection
Examining the Equifax Data Breach	October 5, 2017	Financial Services	
Examining DHS's Cybersecurity Mission	October 3, 2017	Homeland Security	Cybersecurity and Infrastructure Protection
Oversight of the Equifax Data Breach: Answers for Consumers	October 3, 2017	Energy and Commerce	Digital Commerce and Consumer Protection
Cybersecurity of the Internet of Things	October 3, 2017	Oversight & Government Reform	Information Technology
Challenges of Recruiting and Retaining a Cybersecurity Workforce	September 7, 2017	Homeland Security	Cybersecurity and Infrastructure Protection
Protecting Small Businesses from Cyber Attacks: the Cybersecurity Insurance Option	July 26, 2017	Small Business	
Russia Investigative Task Force Hearing with Former Secretary of Homeland Security Jeh Johnson (Open)	June 21, 2017	Intelligence	
Cybersecurity Regulation Harmonization	June 21, 2017	Homeland Security & Governmental Affairs	
Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry	June 15, 2017	Science, Space and Technology	Research & Technology and Oversight (Joint)
Examining the Role of the Department of Health and Human Services in Health Care Cybersecurity	June 8, 2017	Energy and Commerce	Oversight and Investigations

Title	Date	Committee	Subcommittee
Fiscal Year 2018 Budget Request for U.S. Cyber Command: Cyber Mission Force Support to Department of Defense Operations	May 23, 2017	Armed Services	Emerging Threats and Capabilities
Reviewing the FAFSA Data Breach	May 3, 2017	Oversight and Government Reform	
Reviewing Federal IT Workforce Challenges and Possible Solutions	April 4, 2017	Oversight and Government Reform	Information Technology
The Current State of DHS' Efforts to Secure Federal Networks	March 28, 2017	Homeland Security	Cybersecurity and Infrastructure Protection
A Borderless Battle: Defending Against Cyber Threats	March 22, 2017	Homeland Security	
The Current State of DHS Private Sector Engagement for Cybersecurity	March 9, 2017	Homeland Security	Cybersecurity and Infrastructure Protection
Coordinating Federal Cybersecurity Resources for Small Businesses	March 8, 2017	Small Business	
Cyber Warfare in the 21st Century: Threats, Challenges and Opportunities	March 1, 2017	Armed Services	
Strengthening U.S. Cybersecurity Capabilities	February 14, 2017	Science	Research & Technology
The Electricity Sector's Efforts to Respond to Cybersecurity Threats	February 1, 2017	Energy & Commerce	

Source: Compiled by CRS from Congress.gov.

Table 8. 115th Congress, House Hearings by Committee

Committee	Subcommittee	Title	Date
Armed Services	Emerging Threats and Capabilities	Fiscal Year 2018 Budget Request for U.S. Cyber Command: Cyber Mission Force Support to Department of Defense Operations	May 23, 2017
Armed Services		Cyber Warfare in the 21st Century: Threats, Challenges and Opportunities	March 1, 2017
Energy and Commerce	Oversight and Investigations	Examining the Role of the Department of Energy in Energy Sector Cybersecurity	December 8, 2017
Energy and Commerce	Digital and Consumer Protection	Securing Consumers' Credit Data in the Age of Digital Commerce	November 1, 2017
Energy and Commerce	Digital and Consumer Protection	Oversight of the Equifax Data Breach: Answers for Consumers	October 3, 2017
Energy & Commerce	Oversight and Investigations	Examining the Role of the Department of Health and Human Services in Health Care Cybersecurity	June 8, 2017
Energy & Commerce		The Electricity Sector's Efforts to Respond to Cybersecurity Threats	February 1, 2017
Financial Services	Financial Institutions and Consumer Credit	Implementation and Cybersecurity Protocols of the Consolidated Audit Trail	November 30, 2017
Financial Services	Financial Institutions and Consumer Credit	Data Security: Vulnerabilities and Opportunities for Improvement	November 1, 2017
Financial Services		Continuation of Hearing entitled "Examining the Equifax Data Breach	October 25, 2017
Financial Services		Examining the Equifax Data Breach	October 5, 2017
Homeland Security	Cybersecurity and Infrastructure Protection	CDM, The Future of Federal Cybersecurity?	January 17, 2018
Homeland Security	Cybersecurity and Infrastructure Protection	Maximizing the Value of Cyber Threat Information Sharing	November 15, 2017
Homeland Security		Examining Physical Security and Cybersecurity at Our Nation's Ports (Field Hearing)	October 30, 2017

Committee	Subcommittee	Title	Date
Homeland Security	Cybersecurity and Infrastructure Protection	Public-Private Solutions to Educating a Cyber Workforce	October 24, 2017
Homeland Security	Cybersecurity and Infrastructure Protection	Examining DHS's Cybersecurity Mission	October 3, 2017
Homeland Security	Cybersecurity and Infrastructure Protection	Challenges of Recruiting and Retaining a Cybersecurity Workforce	September 7, 2017
Homeland Security		Cybersecurity Regulation Harmonization	June 21, 2017
Homeland Security	Cybersecurity and Infrastructure Protection	The Current State of DHS' Efforts to Secure Federal Networks	March 28, 2017
Homeland Security		A Borderless Battle: Defending Against Cyber Threats	March 22, 2017
Homeland Security	Cybersecurity and Infrastructure Protection	The Current State of DHS Private Sector Engagement for Cybersecurity	March 9, 2017
Intelligence		Russia Investigative Task Force Hearing with Former Secretary of Homeland Security Jeh Johnson (Open)	June 21, 2017
Oversight and Government Reform	Information Technology	Oversight of IT and Cybersecurity at the Department of Veterans Affairs	December 7, 2017
Oversight and Government Reform	Information Technology	Cybersecurity of Voting Machines	November 29, 2017
Oversight and Government Reform	Information Technology	Cybersecurity of the Internet of Things	October 3, 2017
Oversight and Government Reform		Reviewing the FAFSA Data Breach	May 3, 2017
Oversight and Government Reform	Information Technology	Reviewing Federal IT Workforce Challenges and Possible Solutions	April 4, 2017
Science, Space and Technology	Oversight	Bolstering the Government's Cybersecurity: A Survey of Compliance with the DHS Directive	November 14, 2017
Science, Space and Technology	Oversight	Bolstering the Government's Cybersecurity: Assessing the Risk of Kaspersky Lab Products to the Federal Government	October 25, 2017
Science, Space and Technology	Research & Technology and Oversight (Joint)	Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry	June 15, 2017

Committee	Subcommittee	Title	Date
Science, Space and Technology	Research & Technology	Strengthening U.S. Cybersecurity Capabilities	February 14, 2017
Small Business		Small Business Information Sharing: Combating Foreign Cyber Threats	January 30, 2018
Small Business		Federal Government and Small Businesses: Promoting Greater Information Sharing for Stronger Cybersecurity	November 15, 2017
Small Business		Protecting Small Businesses from Cyber Attacks: the Cybersecurity Insurance Option	July 26, 2017
Small Business		Coordinating Federal Cybersecurity Resources for Small Businesses	March 8, 2017

Source: Compiled by CRS from Congress.gov.

Table 9. 115th Congress, Senate Hearings by Date

Title	Date	Committee	Subcommittee
Protecting Consumers in the Era of Major Data Breaches	November 8, 2017	Commerce, Science and Transportation	
2020 Census: Examining Cost Overruns, Information Security, and Accuracy	October 31, 2017	Homeland Security & Governmental Affairs	
Cyber Technology and Energy Infrastructure	October 26, 2017	Energy and Natural Resources	
Roles and Responsibilities for Defending the Nation from Cyber Attack	October 19, 2017	Armed Services	
Consumer Data Security and the Credit Bureaus Files	October 17, 2017	Banking, Housing and Urban Affairs	
An Examination of the Equifax Cybersecurity Breach	October 4, 2017	Banking, Housing and Urban Affairs	
Equifax: Continuing to Monitor Data-Broker Cybersecurity	October 4, 2017	Judiciary	Privacy, Technology and the Law
Examining the Fintech Landscape	September 12, 2017	Banking, Housing and Urban Affairs	
Open Hearing: Russian Interference in the 2016 U.S. Elections	June 21, 2017	Select Committee on Intelligence	
State-Sponsored Cyberspace Threats: Recent Incidents and U.S. Policy Response	June 13, 2017	Foreign Relations	East Asia, the Pacific, and International Cybersecurity
Cyber Posture of the Services	May 23, 2017	Armed Services	
Cyber Policy, Strategy, and Organization	May 11, 2017	Armed Services	
Worldwide Threats	May 11, 2017	Select Committee on Intelligence	
Cyber Threats Facing America: An Overview of the Cybersecurity Threat Landscape	May 10, 2017	Homeland Security and Governmental Affairs	
United States Cyber Command	May 9, 2017	Armed Services	
Cyber-enabled Information Operations	April 27 2017	Armed Services	Cybersecurity

Title	Date	Committee	Subcommittee
American Leadership in the Asia-Pacific, Part 1: Security Issues	March 29, 2017	Foreign Relations	East Asia, The Pacific, and International Cybersecurity Policy
Cybersecurity threats to the U.S. electric grid and technology advancements to maximize such threats, including S. 79, the "Securing Energy Infrastructure Act."	March 28, 2017	Energy & Natural Resources	Energy
The Promises and Perils of Emerging Technologies for Cybersecurity	March 22, 2017	Commerce, Science and Transportation	
Cyber Strategy and Policy	March 2, 2017	Armed Services	
CLOSED: Cyber Threats	February 7, 2017	Armed Services	
Foreign Cyber Threats to the United States	January 5, 2017	Armed Services	

Source: Compiled by CRS from Congress.gov.

Table 10. 115th Congress, Senate Hearings by Committee

Committee	Subcommittee	Title	Date
Armed Services		Roles and Responsibilities for Defending the Nation from Cyber Attack	October 19, 2017
Armed Services		Cyber Posture of the Services	May 23, 2017
Armed Services		United States Cyber Command	May 9, 2017
Armed Services	Cybersecurity	Cyber-enabled Information Operations	April 27 2017
Armed Services		Cyber Strategy and Policy	March 2, 2017
Armed Services		CLOSED: Cyber Threats	February 7, 2017
Armed Services		Foreign Cyber Threats to the United States	January 5, 2017
Banking, Housing and Urban Affairs		Consumer Data Security and the Credit Bureaus Files	October 17, 2017
Banking, Housing and Urban Affairs		An Examination of the Equifax Cybersecurity Breach	October 4, 2017
Banking, Housing and Urban Affairs		Examining the Fintech Landscape	September 12, 2017
Commerce, Science and Transportation		Protecting Consumers in the Era of Major Data Breaches	November 8, 2017
Commerce, Science and Transportation		The Promises and Perils of Emerging Technologies for Cybersecurity	March 22, 2017
Energy & Natural Resources		Cyber Technology and Energy Infrastructure	October 26, 2017
Energy & Natural Resources	Energy	Cybersecurity threats to the U.S. electric grid and technology advancements to maximize such threats, including S. 79, the “Securing Energy Infrastructure Act.	March 28, 2017
Foreign Relations	East Asia, The Pacific, and International Cybersecurity Policy	State-Sponsored Cyberspace Threats: Recent Incidents and U.S. Policy Response	June 13, 2017

Committee	Subcommittee	Title	Date
Foreign Relations	East Asia, The Pacific, and International Cybersecurity Policy	American Leadership in the Asia-Pacific, Part 1: Security Issues	March 29, 2017
Homeland Security and Governmental Affairs		2020 Census: Examining Cost Overruns, Information Security, and Accuracy	October 31, 2017
Homeland Security and Governmental Affairs		Cyber Threats Facing America: An Overview of the Cybersecurity Threat Landscape	May 10, 2017
Judiciary	Privacy, Technology and the Law	Equifax: Continuing to Monitor Data-Broker Cybersecurity	October 4, 2017
Select Committee on Intelligence		Open Hearing: Russian Interference in the 2016 U.S. Elections	June 21, 2017

Source: Compiled by CRS from Congress.gov.

Hearings in the 114th Congress

The following tables list cybersecurity hearings in the 114th Congress. The tables contain identical content but are organized differently.

Table 11 lists Senate hearings arranged by date. **Table 12** lists Senate hearings arranged by committee. **Table 13** lists House hearings arranged by date (most recent first), and **Table 14** lists House hearings arranged by committee. When viewed in HTML, the document titles are active links to the committee's website for that particular hearing.

Table 11. 114th Congress, Senate Hearings, by Date

Title	Date	Committee	Subcommittee
Encryption and Cyber Matters	September 13, 2016	Armed Services	
Cybersecurity and U.S. National Security	July 14, 2016	Armed Services	
How the Internet of Things (IoT) Can Bring U.S. Transportation and Infrastructure into the 21st Century	June 28, 2016	Commerce, Science and Transportation	Surface Transportation and Merchant Marine Infrastructure, Safety, and Security
International Cybersecurity Strategy: Deterring Foreign Threats and Building Global Cyber Norms	May 25, 2016	Foreign Relations	East Asia, the Pacific, and International Cybersecurity Policy
Assessing the Security of Critical Infrastructure: Threat, Vulnerabilities, and Solutions	May 18, 2016	Homeland Security and Governmental Affairs	
Ransomware: Understanding the Threat and Exploring Solutions	May 18, 2016	Judiciary	
CLOSED: Cybersecurity and United States Cyber Command	April 19, 2016	Armed Services	
Cybersecurity and Protecting Taxpayer Information	April 12, 2016	Finance	
U.S. Cyber Command	April 5, 2016	Armed Services	
Data Brokers – Is Consumers' Information Secure?	November 3, 2015	Judiciary	Privacy, Technology and the Law
Threats to the Homeland	October 8, 2015	Homeland Security and Governmental Affairs	
The Changing Landscape of U.S.-China Relations: What's Next?	September 29, 2015	Foreign Relations	East Asia, The Pacific, and International Cybersecurity Policy
United States Cybersecurity Policy and Threats	September 29, 2015	Armed Services	
Intelligence Issues	September 24, 2015	Intelligence	
Protecting the Electric Grid from the Potential Threats of Solar Storms and Electromagnetic Pulse	July 22, 2015	Homeland Security and Governmental Affairs	

Title	Date	Committee	Subcommittee
Counterterrorism, Counterintelligence, and the Challenges of "Going Dark"	July 8, 2015	Intelligence	
Cyber Crime: Modernizing our Legal Framework for the Information Age	July 8, 2015	Judiciary	
Under Attack: Federal Cybersecurity and the OPM Data Breach	June 25, 2015	Homeland Security and Governmental Affairs	
OPM Information Technology Spending & Data Security	June 23, 2015	Appropriations	Financial Services and General Government
Hearing on Energy Accountability and Reform Legislation (including S. 1241, Enhanced Grid Security Act of 2015)	June 9, 2015	Energy and Natural Resources	
The IRS Data Breach: Steps to Protect Americans' Personal Information	June 2, 2015	Homeland Security and Governmental Affairs	
Cybersecurity: Setting the Rules for Responsible Global Cyber Behavior	May 14, 2015	Foreign Relations	East Asia, The Pacific, And International Cybersecurity Policy
Military Cyber Programs and Posture	April 15, 2015	Armed Services	Emerging Threats and Capabilities
From Protection to Partnership: Funding the DHS role in Cybersecurity	April 15, 2015	Appropriations	Homeland Security
Examining the Evolving Cyber Insurance Marketplace	March 19, 2015	Commerce, Science and Transportation	Consumer Protection, Product Safety, Insurance and Data Security
U.S. Strategic Command, U.S. Transportation Command, and U.S. Cyber Command in review of the Defense Authorization Request for Fiscal Year 2016 and the Future Years Defense Program	March 19, 2015	Armed Services	
The Connected World: Examining the Internet of Things	February 11, 2015	Commerce, Science & Transportation	
Getting it Right on Data Breach and Notification Legislation in the 114th Congress	February 5, 2015	Commerce, Science & Transportation	Consumer Protection, Product Safety, Insurance, and Data Security

Title	Date	Committee	Subcommittee
Building a More Secure Cyber Future: Examining Private Sector Experience with the NIST Framework	February 4, 2015	Commerce, Science & Transportation	
Protecting America from Cyber Attacks: The Importance of Information Sharing	January 28, 2015	Homeland Security and Governmental Affairs	

Source: Compiled by CRS from Congress.gov.

Table 12. 114th Congress, Senate Hearings, by Committee

Committee	Subcommittee	Title	Date
Appropriations	Financial Services and General Government	OPM Information Technology Spending & Data Security	June 23, 2015
Appropriations	Homeland Security	From Protection to Partnership: Funding the DHS role in Cybersecurity	April 15, 2015
Armed Services		Encryption and Cyber Matters	September 13, 2016
Armed Services		Cybersecurity and U.S. National Security	July 14, 2016
Armed Services		CLOSED: Cybersecurity and United States Cyber Command	April 19, 2016
Armed Services		U.S. Cyber Command	April 5, 2016
Armed Services		United States Cybersecurity Policy and Threats	September 30, 2015
Armed Services	Emerging Threats and Capabilities	Military Cyber Programs and Posture	April 15, 2015
Armed Services		U.S. Strategic Command, U.S. Transportation Command, and U.S. Cyber Command in review of the Defense Authorization Request for Fiscal Year 2016 and the Future Years Defense Program	March 19, 2015

Committee	Subcommittee	Title	Date
Commerce, Science and Transportation	Surface Transportation and Merchant Marine Infrastructure, Safety, and Security	How the Internet of Things (IoT) Can Bring U.S. Transportation and Infrastructure into the 21st Century	June 28, 2016
Commerce, Science and Transportation	Consumer Protection, Product Safety, Insurance and Data Security	Examining the Evolving Cyber Insurance Marketplace	March 19, 2015
Commerce, Science & Transportation		The Connected World: Examining the Internet of Things	February 11, 2015
Commerce, Science & Transportation		Getting it Right on Data Breach and Notification Legislation in the 114th Congress	February 5, 2015
Commerce, Science & Transportation		Building a More Secure Cyber Future: Examining Private Sector Experience with the NIST Framework	February 4, 2015
Energy and Natural Resources		Hearing on Energy Accountability and Reform Legislation (including S. 1241, Enhanced Grid Security Act of 2015)	June 9, 2015
Financial Services		A Global Perspective on Cyber Threats	June 16, 2015
Finance		Cybersecurity and Protecting Taxpayer Information	April 12, 2016
Foreign Relations	East Asia, The Pacific, And International Cybersecurity Policy	The Changing Landscape of U.S.-China Relations: What's Next?	September 29, 2015
Foreign Relations	East Asia, The Pacific, And International Cybersecurity Policy	Cybersecurity: Setting the Rules for Responsible Global Cyber Behavior	May 14, 2015
Homeland Security and Governmental Affairs		Assessing the Security of Critical Infrastructure: Threat, Vulnerabilities, and Solutions	May 18, 2016
Homeland Security and Governmental Affairs		Threats to the Homeland	October 8, 2015
Homeland Security and Governmental Affairs		Protecting the Electric Grid from the Potential Threats of Solar Storms and Electromagnetic Pulse	July 22, 2015

Committee	Subcommittee	Title	Date
Homeland Security and Governmental Affairs		Under Attack: Federal Cybersecurity and the OPM Data Breach	June 25, 2015
Homeland Security and Governmental Affairs		The IRS Data Breach: Steps to Protect Americans' Personal Information	June 2, 2015
Homeland Security and Governmental Affairs		Protecting America from Cyber Attacks: The Importance of Information Sharing	January 28, 2015
Intelligence		Intelligence Issues	September 24, 2015
Intelligence		Counterterrorism, Counterintelligence, and the Challenges of "Going Dark"	July 8, 2015
Judiciary		Ransomware: Understanding the Threat and Exploring Solutions	May 18, 2016
Judiciary		Data Brokers – Is Consumers' Information Secure?	November 3, 2015
Judiciary		Cyber Crime: Modernizing our Legal Framework for the Information Age	July 8, 2015

Source: Compiled by CRS from Congress.gov.

Table 13. 114th Congress, House Hearings, by Date

Title	Date	Committee	Subcommittee
Cybersecurity: Ensuring the Integrity of the Ballot Box	September 28, 2016	Oversight and Government Reform	Information Technology
Protecting the 2016 Elections from Cyber and Voting Machine Attacks	September 13, 2016	Science, Space & Technology	
Evaluating FDIC's Response to Major Data Breaches: Is the FDIC Safeguarding Consumers' Banking Information?	July 14, 2016	Science	
Digital Acts of War: Evolving the Cybersecurity Conversation	July 13, 2016	Oversight and Government Reform	National Security and Information Technology (Joint)
The Value of DHS's Vulnerability Assessments in Protecting Our Nation's Critical Infrastructure	July 12, 2016	Homeland Security	Cybersecurity, Infrastructure Protection and Security Technologies
Foreign Cyber Threats: Small Business, Big Target	July 7, 2016	Small Business	
Military Cyber Operations	June 22, 2016	Armed Services	
Federal Efforts to Improve Cybersecurity (Field Hearing: Chicago)	June 20, 2016	Oversight and Government Reform	Information Technology
Oversight of the Cybersecurity Act of 2015	June 15, 2016	Homeland Security	Cybersecurity, Infrastructure Protection and Security Technologies
Examining Cybersecurity Responsibilities at HHS	May 25, 2016	Energy and Commerce	
Enhancing Preparedness and Response Capabilities to Address Cyber Threats	May 24, 2016	Homeland Security	Emergency Preparedness, Response and Communications AND Cybersecurity, Infrastructure Protection and Security Technologies
FDIC Data Breaches: Can Americans Trust that Their Private Banking Information Is Secure?	May 12, 2016	Science, Space & Technology	Oversight
Federal Cybersecurity Detection, Response, and Mitigation	April 20, 2016	Oversight and Government Reform	Information Technology

Title	Date	Committee	Subcommittee
Small Business and the Federal Government: How Cyber-Attacks Threaten Both	April 20, 2016	Small Business	
Hearing on Tax Return Filing Season (focusing on efforts to protect Americans from identity theft related tax fraud and cybersecurity attacks)	April 19, 2016	Ways and Means	Oversight
Blackout! Are We Prepared to Manage the Aftermath of a Cyber-Attack or Other Failure of the Electrical Grid?	April 14, 2016	Transportation and Infrastructure	Economic Development, Public Buildings and Emergency Management
Can the IRS Protect Taxpayers' Personal Information?	April 14, 2016	Science, Space and Technology	Research and Technology
Cyber Preparedness and Response at the Local Level (Field Hearing)	April 7, 2016	Homeland Security	Cybersecurity, Infrastructure Protection and Security Technologies
Fiscal Year 2017 Information Technology and Cyber Programs: Foundations for a Secure Warfighting Network	March 23, 2016	Armed Services	Emerging Threats and Capabilities
The Role of Cyber Insurance in Risk Management	March 22, 2016	Homeland Security	Cybersecurity, Infrastructure Protection and Security Technologies
VA Cybersecurity and IT Oversight	March 16, 2016	Oversight and Government Reform	Information Technology
Fiscal 2017 Budget Request for the Department of Homeland Security and Readiness	March 16, 2016	Homeland Security	
Fiscal Year 2017 Budget Request for U.S. Cyber Command: Preparing for Operations in the Cyber Domain	March 16, 2016	Armed Services	Emerging Threats and Capabilities
FY 2017 Budget Hearing - Office of Personnel Management	March 14, 2016	Appropriations	Financial Services and General Government
Emerging Cyber Threats to the United States	February 25, 2016	Homeland Security	Cybersecurity, Infrastructure Protection, and Security Technologies

Title	Date	Committee	Subcommittee
U.S. Department of Education: Investigation of the CIO	February 2, 2016	Oversight and Government Reform	
Wassenaar: Cybersecurity and Export Control	January 12, 2016	Oversight and Government Reform	Information Technology
Cyber Security: What the Federal Government Can Learn from the Private Sector	January 8, 2016	Science, Space & Technology	Research and Technology
Document Production Status Update (OPM data breaches)	January 7, 2016	Oversight and Government Reform	
The Internet of Cars	November 18, 2015	Oversight and Government Reform	Transportation and Public Assets
U.S. Department of Education: Information Security Review	November 17, 2015	Oversight and Government Reform	
Cybersecurity for Power Systems	October 21, 2015	Science, Space and Technology	Energy Subcommittee and Research and Technology Subcommittee
Protecting Maritime Facilities in the 21st Century: Are Our Nation's Ports at Risk for a Cyber-Attack?	October 8, 2015	Homeland Security	
The EMV Deadline and What it Means for Small Business	October 7, 2015	Small Business	
Examining the Mission, Structure, and Reorganization Effort of the National Protection and Programs Directorate	October 7, 2915	Homeland Security	Cybersecurity, Infrastructure Protection, and Security
Implementing the Department of Defense Cyber Strategy	September 30, 2015	Armed Services	
The State of the Cloud	September 22, 2015	Oversight and Government Reform	Information Technology (field hearing University of Texas-San Antonio)
Examining Vulnerabilities of America's Power Supply	September 10, 2015	Science, Space & Technology	Oversight/Energy
World Wide Cyber Threats	September 10, 2015	Intelligence	
Internet of Things	July 29, 2015	Judiciary	

Title	Date	Committee	Subcommittee
Promoting and Incentivizing Cybersecurity Best Practices	July 28, 2015	Homeland Security	Cybersecurity, Infrastructure Protection, and Security Technologies
Cybersecurity: The Department of the Interior	July 15, 2015	Oversight and Government Reform	Information Technology AND Subcommittee on Interior (Joint hearing)
Is the OPM [Office of Personnel Management] Data Breach the Tip of the Iceberg?	July 8, 2015	Science, Space and Technology	Research and Technology
DHS' Efforts to Secure.Gov	June 24, 2015	Homeland Security	Cybersecurity, Infrastructure Protection and Security Technology
OPM Data Breach: Part II	June 24, 2015	Oversight and Government Reform	
Evaluating the Security of the U.S. Financial Sector (Task Force to Investigate Terrorism Financing)	June 24, 2015	Financial Services	
OPM Data Security Review	June 23, 2015	Appropriations	Financial Services and General Government
OPM: Data Breach	June 16, 2015	Oversight and Government Reform	
A Global Perspective on Cyber Threats	June 16, 2015	Financial Services	
Protecting Critical Infrastructure: How the Financial Sector Addresses Cyber Threats	May 19, 2015	Financial Services	Financial Institutions and Consumer Credit
Protecting Consumers: Financial Data Security in the Age of Computer Hackers	May 14, 2015	Financial Services	
Enhancing Cybersecurity of Third-Party Contractors and Vendors	April 22, 2015	Oversight and Government Reform	
Small Business, Big Threat: Protecting Small Businesses from Cyber Attacks	April 22, 2015	Small Business	
Full committee meets to formulate a rule on H.R. 1560, the "Protecting Cyber Networks Act"; and H.R. 1731, the "National Cybersecurity Protection Advancement Act of 2015"	April 21, 2015	Rules	

Title	Date	Committee	Subcommittee
[CLOSED] Special Activities	April 15, 2015	Intelligence	National Security Agency and Cybersecurity
The Internet of Things: Exploring the Next Technology Frontier	March 24, 2015	Energy and Commerce	Commerce, Manufacturing and Trade
The Growing Cyber Threat and its Impact on American Business	March 19, 2015	Intelligence	
Discussion Draft of H.R. 1704, Data Security and Breach Notification Act of 2015	March 18, 2015	Energy and Commerce	Commerce, Manufacturing, and Trade
Cybersecurity: The Evolving Nature of Cyber Threats Facing the Private Sector	March 18, 2015	Oversight and Government Reform	Information Technology
Industry Perspectives on the President's Cybersecurity Information Sharing Proposal	March 4, 2015	Homeland Security	Cybersecurity, Infrastructure Protection and Security Technologies
Cyber Operations: Improving the Military Cyber Security Posture in an Uncertain Threat Environment	March 4, 2015	Armed Services	Emerging Threats and Capabilities
Understanding the Cyber Threat and Implications for the 21st Century Economy	March 3, 2015	Energy and Commerce	Oversight and Investigations
Examining the President's Cybersecurity Information Sharing Proposal	February 25, 2015	Homeland Security	
Emerging Threats and Technologies to Protect the Homeland	February 12, 2015	Homeland Security	Cybersecurity, Infrastructure Protection, and Security Technologies
The Expanding Cyber Threat	January 27, 2015	Science, Space & Technology	Research and Technology
What are the Elements of Sound Data Breach Legislation?	January 27, 2015	Energy and Commerce	
Briefing: The North Korean Threat: Nuclear, Missiles and Cyber	January 13, 2015	Foreign Affairs	

Source: Compiled by CRS from Congress.gov.

Table 14. 114th Congress, House Hearings, by Committee

Committee	Subcommittee	Title	Date
Appropriations	Financial Services and General Government	FY 2017 Budget Hearing - Office of Personnel Management	March 14, 2016
Armed Services		Military Cyber Operations	June 22, 2016
Armed Services	Emerging Threats and Capabilities	Fiscal Year 2017 Information Technology and Cyber Programs: Foundations for a Secure Warfighting Network	March 23, 2016
Armed Services	Emerging Threats and Capabilities	Fiscal Year 2017 Budget Request for U.S. Cyber Command: Preparing for Operations in the Cyber Domain	March 16, 2016
Armed Services		Implementing the Department of Defense Cyber Strategy	September 30, 2015
Armed Services	Emerging Threats and Capabilities	Cyber Operations: Improving the Military Cyber Security Posture in an Uncertain Threat Environment	March 4, 2015
Energy and Commerce		Examining Cybersecurity Responsibilities at HHS	May 25, 2016
Energy and Commerce	Commerce, Manufacturing, and Trade	The Internet of Things: Exploring the Next Technology Frontier	March 24, 2015
Energy and Commerce	Commerce, Manufacturing, and Trade	Discussion Draft of H.R. 1704, Data Security and Breach Notification Act	March 18, 2015
Energy and Commerce	Oversight and Investigations	Understanding the Cyber Threat and Implications for the 21st Century Economy	March 3, 2015
Energy and Commerce		What are the Elements of Sound Data Breach Legislation?	January 27, 2015
Financial Services		Evaluating the Security of the U.S. Financial Sector (Task Force to Investigate Terrorism Financing)	June 24, 2015

Committee	Subcommittee	Title	Date
Financial Services	Financial Institutions and Consumer Credit	Protecting Critical Infrastructure: How the Financial Sector Addresses Cyber Threats	May 19, 2015
Financial Services		Protecting Consumers: Financial Data Security in the Age of Computer Hackers	May 14, 2015
Foreign Affairs		Briefing: The North Korean Threat: Nuclear, Missiles and Cyber	January 13, 2015
Homeland Security	Cybersecurity, Infrastructure Protection and Security Technologies	The Value of DHS's Vulnerability Assessments in Protecting Our Nation's Critical Infrastructure	July 12, 2016
Homeland Security	Cybersecurity, Infrastructure Protection and Security Technologies	Oversight of the Cybersecurity Act of 2015	June 15, 2016
Homeland Security	Cybersecurity, Infrastructure Protection and Security Technologies	Enhancing Preparedness and Response Capabilities to Address Cyber Threats	May 24, 2016
Homeland Security	Cybersecurity, Infrastructure Protection and Security Technologies	Cyber Preparedness and Response at the Local Level (Field Hearing)	April 7, 2016
Homeland Security	Cybersecurity, Infrastructure Protection and Security Technologies	The Role of Cyber Insurance in Risk Management	March 22, 2016
Homeland Security		Fiscal 2017 Budget Request for the Department of Homeland Security and Readiness	March 16, 2016
Homeland Security	Cybersecurity, Infrastructure Protection and Security Technologies	Emerging Cyber Threats to the United States	February 25, 2016
Homeland Security		Protecting Maritime Facilities in the 21st Century: Are Our Nation's Ports at Risk for a Cyber-Attack?	October 8, 2015
Homeland Security	Cybersecurity, Infrastructure Protection and Security Technologies	Examining the Mission, Structure, and Reorganization Effort of the National Protection and Programs Directorate	October 7, 2015

Committee	Subcommittee	Title	Date
Homeland Security	Cybersecurity, Infrastructure Protection, and Security Technologies	Promoting and Incentivizing Cybersecurity Best Practices	July 28, 2015
Homeland Security	Cybersecurity, Infrastructure Protection and Security Technologies	Oversight and Government Reform	June 24, 2015
Homeland Security	Cybersecurity, Infrastructure Protection and Security Technologies	Industry Perspectives on the President's Cybersecurity Information Sharing Proposal	March 4, 2015
Homeland Security		Examining the President's Cybersecurity Information Sharing Proposal	February 25, 2015
Homeland Security	Cybersecurity, Infrastructure Protection, and Security Technologies	Emerging Threats and Technologies to Protect the Homeland	February 12, 2015
Intelligence		World Wide Cyber Threats	September 10, 2015
Intelligence	National Security Agency and Cybersecurity	[CLOSED] Special Activities	April 15, 2015
Intelligence		The Growing Cyber Threat and its Impact on American Business	March 19, 2015
Judiciary		Internet of Things	July 29, 2015
Oversight and Government Reform	Information Technology	Cybersecurity: Ensuring the Integrity of the Ballot Box	September 28, 2016
Oversight and Government Reform	Information Technology and National Security (Joint)	Digital Acts of War: Evolving the Cybersecurity Conversation	July 13, 2016
Oversight and Government Reform	Information Technology	Federal Efforts to Improve Cybersecurity (Field Hearing: Chicago)	June 20, 2016
Oversight and Government Reform	Information Technology	Federal Cybersecurity Detection, Response, and Mitigation	April 20, 2016
Oversight and Government Reform	Information Technology	VA Cybersecurity and IT Oversight	March 16, 2016
Oversight and Government Reform		U.S. Department of Education: Investigation of the CIO	February 2, 2016

Committee	Subcommittee	Title	Date
Oversight and Government Reform	Information Technology	Wassenaar: Cybersecurity and Export Control	January 12, 2016
Oversight and Government Reform		Document Production Status (OPM data breaches)	January 7, 2016
Oversight and Government Reform	Transportation and Public Assets	The Internet of Cars	November 18, 2015
Oversight and Government Reform		U.S. Department of Education: Information Security Review	November 17, 2105
Oversight and Government Reform	Information Technology (field hearing University of Texas-San Antonio)	The State of the Cloud	September 22, 2015
Oversight and Government Reform	Information Technology AND Subcommittee on Interior (Joint hearing	Cybersecurity: The Department of the Interior	July 15, 2015
Oversight and Government Reform		OPM Data Breach: Part II	June 24, 2015
Oversight and Government Reform		OPM: Data Breach	June 16, 2015
Oversight and Government Reform		Enhancing Cybersecurity of Third-Party Contractors and Vendors	April 22, 2015
Oversight and Government Reform	Information Technology	Cybersecurity: The Evolving Nature of Cyber Threats Facing the Private Sector	March 18, 2015
Rules		Full committee meets to formulate a rule on H.R. 1560, the "Protecting Cyber Networks Act"; and H.R. 1731, the "National Cybersecurity Protection Advancement Act of 2015"	April 21, 2015
Science, Space & Technology		Protecting the 2016 Elections from Cyber and Voting Machine Attacks	September 13, 2016
Science, Space & Technology		Evaluating FDIC's Response to Major Data Breaches: Is the FDIC Safeguarding Consumers' Banking Information?	July 14, 2016
Science, Space & Technology	Oversight and Energy (Joint)	Examining Vulnerabilities of America's Power Supply	September 10, 2015

Committee	Subcommittee	Title	Date
Science, Space & Technology	Oversight	FDIC Data Breaches: Can Americans Trust that Their Private Banking Information Is Secure?	May 12, 2016
Science, Space & Technology	Research and Technology	Can the IRS Protect Taxpayers' Personal Information?	April 14, 2016
Science, Space & Technology	Research and Technology	Cyber Security: What the Federal Government Can Learn from the Private Sector	January 8, 2016
Science, Space & Technology	Research and Technology and Energy (Joint)	Cybersecurity for Power Systems	October 21, 2015
Science, Space & Technology	Research and Technology	The Expanding Cyber Threat	January 27, 2015
Small Business		Foreign Cyber Threats: Small Business, Big Target	July 7, 2016
Small Business		Small Business and the Federal Government: How Cyber-Attacks Threaten Both	April 19, 2016
Small Business		The EMV Deadline and What it Means for Small Business	October 7, 2015
Small Business		Small Business, Big Threat: Protecting Small Businesses from Cyber Attacks	April 22, 2015
Transportation and Infrastructure	Economic Development, Public Buildings and Emergency Management	Blackout! Are We Prepared to Manage the Aftermath of a Cyber-Attack or Other Failure of the Electrical Grid?	April 14, 2016
Ways and Means	Oversight	Hearing on Tax Return Filing Season (focusing on efforts to protect Americans from identity theft related tax fraud and cybersecurity attacks)	April 19, 2016

Source: Compiled by CRS from Congress.gov.

Table 15. 114th Congress, Other Hearings

Committee	Subcommittee	Title	Date
U.S.-China Economic and Security Review Commission		Commercial Cyber Espionage and Barriers to Digital Trade in China	June 15, 2015

Source: Compiled by CRS.

Hearings in the 113th Congress

The following tables list cybersecurity hearings in the 113th Congress. The tables contain identical content but are organized differently. **Table 16** lists House hearings arranged by date (most recent first), and **Table 17** lists House hearings arranged by committee. **Table 18** lists Senate hearings arranged by date. **Table 20** lists Senate hearings arranged by committee. When viewed in HTML, the document titles are active links to the committee's website for that particular hearing.

Table 16. 113th Congress, House Hearings, by Date

Title	Date	Committee	Subcommittee
How Data Mining Threatens Student Privacy	June 25, 2014	Homeland Security	Cybersecurity, Infrastructure Protection, and Security Technologies
Assessing Persistent and Emerging Cyber Threats to the U.S. Homeland	May 21, 2014	Homeland Security	Counterterrorism and Intelligence
Electromagnetic Pulse (EMP): Threat to Critical Infrastructure	May 8, 2014	Homeland Security	Cybersecurity, Infrastructure Protection, and Security Technologies
Protecting Your Personal Data: How Law Enforcement Works With the Private Sector to Prevent Cybercrime	April 16, 2014	Homeland Security	Cybersecurity, Infrastructure Protection, and Security Technologies (Field Hearing)
Information Technology and Cyber Operations: Modernization and Policy Issues in a Changing National Security Environment	March 12, 2014	Armed Services	Intelligence, Emerging Threats, and Capabilities
International Cybercrime Protection	March 6, 2014	Science, Space, and Technology	Financial Institutions and Consumer Credit
Data Security: Examining Efforts to Protect Americans' Financial Information	March 5, 2014	Financial Services	
Protecting Consumer Information: Can Data Breaches Be Prevented?	February 5, 2014	Energy and Commerce	Commerce, Manufacturing, and Trade
A Roadmap for Hackers? - Documents Detailing HealthCare.gov Security Vulnerabilities	January 28, 2014	Oversight and Government Reform	
HealthCare.gov: Consequences of Stolen Identity	January 19, 2014	Science, Space, and Technology	
HHS' Own Security Concerns About HealthCare.gov	January 16, 2014	Oversight and Government Reform	
Is My Data on Healthcare.gov Secure?	November 19, 2013	Science, Space, and Technology	
Security of Healthcare.gov	November 19, 2013	Energy and Commerce	
Cyber Side-Effects: How Secure is the Personal Information Entered into the Flawed Healthcare.gov?	November 13, 2013	Homeland Security	
Cyber Incident Response: Bridging the Gap Between Cybersecurity and Emergency Management	October 30, 2013	Homeland Security	Cybersecurity, Infrastructure Protection, and Security Technologies

Title	Date	Committee	Subcommittee
Cybersecurity: 21st Century Threats, Challenges, and Opportunities	October 23, 2013	Permanent Select Committee on Intelligence	
A Look into the Security and Reliability of the Health Exchange Data Hub	September 11, 2013	Homeland Security	Cybersecurity, Infrastructure Protection, and Security Technologies
Asia: The Cyber Security Battleground	July 23, 2013	Foreign Affairs	Asia and the Pacific
Oversight of Executive Order 13636 and Development of the Cybersecurity Framework	July 18, 2013	Homeland Security	Cybersecurity, Infrastructure Protection, and Security Technologies
Reporting Data Breaches: Is Federal Legislation Needed to Protect Consumers?	July 18, 2013	Energy and Commerce	Commerce, Manufacturing, and Trade
Evaluating Privacy, Security, and Fraud Concerns with ObamaCare's Information Sharing Apparatus	July 17, 2013	(Joint Hearing) Homeland Security and Oversight and Government Reform	
Cyber Espionage and the Theft of U.S. Intellectual Property and Technology	July 9, 2013	Energy and Commerce	Oversight and Investigation
Cyber Threats and Security Solutions	May 21, 2013	Energy and Commerce	
Cybersecurity: An Examination of the Communications Supply Chain	May 21, 2013	Energy and Commerce	Communications and Technology
Facilitating Cyber Threat Information Sharing and Partnering with the Private Sector to Protect Critical Infrastructure: An Assessment of DHS Capabilities	May 16, 2013	Homeland Security	Cybersecurity, Infrastructure Protection, and Security Technologies
Striking the Right Balance: Protecting Our Nation's Critical Infrastructure from Cyber Attack and Ensuring Privacy and Civil Liberties	April 25, 2013	Homeland Security	Cybersecurity, Infrastructure Protection, and Security Technologies
Cyber Attacks: An Unprecedented Threat to U.S. National Security	March 21, 2013	Foreign Affairs	Europe, Eurasia, and Emerging Threats
Protecting Small Business from Cyber-Attacks	March 21, 2013	Small Business	Healthcare and Technology
Cybersecurity and Critical Infrastructure [CLOSED hearing]	March 20, 2013	Appropriations	
Cyber Threats from China, Russia and Iran: Protecting American Critical Infrastructure	March 20, 2013	Homeland Security	Cybersecurity, Infrastructure Protection, and Security Technologies

Title	Date	Committee	Subcommittee
DHS Cybersecurity: Roles and Responsibilities to Protect the Nation's Critical Infrastructure	March 13, 2013	Homeland Security	
Investigating and Prosecuting 21st Century Cyber Threats	March 13, 2013	Judiciary	Crime, Terrorism, Homeland Security and Investigations
Information Technology and Cyber Operations: Modernization and Policy Issues to Support the Future Force	March 13, 2013	Armed Services	Intelligence, Emerging Threats, and Capabilities
Cyber R&D Challenges and Solutions	February 26, 2013	Science, Space, and Technology	Technology
Advanced Cyber Threats Facing Our Nation	February 14, 2013	Select Committee on Intelligence	

Source: Compiled by CRS.

Table 17. 113th Congress, House Hearings, by Committee

Committee	Subcommittee	Title	Date
Appropriations		Cybersecurity and Critical Infrastructure [CLOSED hearing]	March 20, 2013
Armed Services	Intelligence, Emerging Threats, and Capabilities	Information Technology and Cyber Operations: Modernization and Policy Issues in a Changing National Security Environment	March 12, 2014
Armed Services	Intelligence, Emerging Threats, and Capabilities	Information Technology and Cyber Operations: Modernization and Policy Issues to Support the Future Force	March 13, 2013
Energy and Commerce	Commerce, Manufacturing, and Trade	Protecting Consumer Information: Can Data Breaches Be Prevented?	February 5, 2014
Energy and Commerce		Security of Healthcare.gov	November 19, 2013
Energy and Commerce	Commerce, Manufacturing, and Trade	Reporting Data Breaches: Is Federal Legislation Needed to Protect Consumers?	July 18, 2013
Energy and Commerce	Oversight and Investigation	Cyber Espionage and the Theft of U.S. Intellectual Property and Technology	July 9, 2013

Committee	Subcommittee	Title	Date
Energy and Commerce		Cyber Threats and Security Solutions	May 21, 2013
Energy and Commerce	Communications and Technology	Cybersecurity: An Examination of the Communications Supply Chain	May 21, 2013
Financial Services	Financial Institutions and Consumer Credit	Data Security: Examining Efforts to Protect Americans' Financial Information	March 5, 2014
Foreign Affairs	Asia and the Pacific	Asia: The Cyber Security Battleground	July 23, 2013
Foreign Affairs	Europe, Eurasia, and Emerging Threats	Cyber Attacks: An Unprecedented Threat to U.S. National Security	March 21, 2013
Homeland Security	Cybersecurity, Infrastructure Protection, and Security Technologies	How Data Mining Threatens Student Privacy	June 25, 2014
Homeland Security	Counterterrorism and Intelligence	Assessing Persistent and Emerging Cyber Threats to the U.S. Homeland	May 21, 2014
Homeland Security	Cybersecurity, Infrastructure Protection, and Security Technologies	Electromagnetic Pulse (EMP): Threat to Critical Infrastructure	May 8, 2014
Homeland Security	Cybersecurity, Infrastructure Protection, and Security Technologies (Field Hearing)	Protecting Your Personal Data: How Law Enforcement Works With the Private Sector to Prevent Cybercrime	April 16, 2014
Homeland Security		Cyber Side-Effects: How Secure is the Personal Information Entered into the Flawed Healthcare.gov?	November 13, 2013
Homeland Security	Cybersecurity, Infrastructure Protection, and Security Technologies	Cyber Incident Response: Bridging the Gap Between Cybersecurity and Emergency Management	October 30, 2013
Homeland Security	Cybersecurity, Infrastructure Protection, and Security Technologies	A Look into the Security and Reliability of the Health Exchange Data Hub	September 11, 2013
Homeland Security	Cybersecurity, Infrastructure Protection, and Security Technologies	Oversight of Executive Order 13636 and Development of the Cybersecurity Framework	July 18, 2013
Homeland Security (Joint Hearing with Oversight and Government Reform)	Cybersecurity, Infrastructure Protection, and Security Technologies, and Energy Policy, Health Care, and Entitlements (Joint Hearing)	Facilitating Cyber Threat Information Sharing and Partnering with the Private Sector to Protect Critical Infrastructure: An Assessment of DHS Capabilities	May 16, 2013

Committee	Subcommittee	Title	Date
Homeland Security	Cybersecurity, Infrastructure Protection, and Security Technologies	Striking the Right Balance: Protecting Our Nation's Critical Infrastructure from Cyber Attack and Ensuring Privacy and Civil Liberties	April 25, 2013
Homeland Security	Cybersecurity, Infrastructure Protection, and Security Technologies	Cyber Threats from China, Russia and Iran: Protecting American Critical Infrastructure	March 20, 2013
Homeland Security	Cybersecurity, Infrastructure Protection, and Security Technologies	DHS Cybersecurity: Roles and Responsibilities to Protect the Nation's Critical Infrastructure	March 13, 2013
Judiciary	Crime, Terrorism, Homeland Security, and Investigations	Investigating and Prosecuting 21st Century Cyber Threats	March 13, 2013
Oversight and Government Reform		A Roadmap for Hackers? - Documents Detailing HealthCare.gov Security Vulnerabilities	January 28, 2014
Oversight and Government Reform		HHS' Own Security Concerns About HealthCare.gov	January 16, 2014
Oversight and Government Reform (Joint Hearing with Homeland Security)	Energy Policy, Health Care, and Entitlements (Joint Hearing with Cybersecurity, Infrastructure Protection, and Security Technologies)	Evaluating Privacy, Security, and Fraud Concerns with ObamaCare's Information Sharing Apparatus	July 18, 2013
Science, Space, and Technology		International Cybercrime Protection	March 6, 2014
Science, Space, and Technology		HealthCare.gov: Consequences of Stolen Identity	January 19, 2014
Science, Space, and Technology		Is My Data on Healthcare.gov Secure?	November 19, 2013
Science, Space, and Technology	Technology	Cyber R&D [Research and Development] Challenges and Solutions	February 26, 2013
Select Committee on Intelligence		Advanced Cyber Threats Facing Our Nation	February 14, 2013
Small Business	Healthcare and Technology	Protecting Small Business from Cyber-Attacks	March 21, 2013

Source: Compiled by CRS.

Table 18. 113th Congress, Senate Hearings, by Date

Title	Date	Committee	Subcommittee
Cybersecurity: Enhancing Coordination to Protect the Financial Sector	December 10, 2014	Banking, Housing, and Urban Affairs	

Title	Date	Committee	Subcommittee
Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks	July 15, 2014	Judiciary	Crime and Terrorism
Investing in Cybersecurity: Understanding Risks and Building Capabilities for the Future	May 7, 2014	Appropriations	Homeland Security
Data Breach on the Rise: Protecting Personal Information from Harm	April 2, 2014	Homeland Security and Governmental Affairs	
Protecting Personal Consumer Information from Cyber Attacks and Data Breaches	March 26, 2014	Commerce, Science, and Transportation	
Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure	March 26, 2014	Homeland Security and Governmental Affairs	
Nomination of Vice Admiral Michael S. Rogers, USN to be admiral and Director, National Security Agency/ Chief, Central Security Services/ Commander, U.S. Cyber Command	March 11, 2014	Armed Services	
U.S. Strategic Command and U.S. Cyber Command in review of the fiscal 2015 Defense Authorization Request and the Future Years Defense Program	February 27, 2014	Armed Services	
Oversight of Financial Stability and Data Security	February 6, 2014	Banking, Housing, and Urban Affairs	
Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime	February 4, 2014	Judiciary	
Safeguarding Consumers' Financial Data, Panel 2	February 3, 2014	Banking, Housing, and Urban Affairs	National Security and International Trade and Finance
The Partnership Between NIST [National Institute of Standards and Technology] and the Private Sector: Improving Cybersecurity	July 25, 2013	Commerce, Science, and Transportation	
Resilient Military Systems and the Advanced Cyber Threat (CLOSED BRIEFING)	June 26, 2013	Armed Services	
Cybersecurity: Preparing for and Responding to the Enduring Threat	June 12, 2013	Appropriations	
Cyber Threats: Law Enforcement and Private Sector Responses	May 8, 2013	Judiciary	Crime and Terrorism

Title	Date	Committee	Subcommittee
Defense Authorization: Cybersecurity Threats: To receive a briefing on cybersecurity threats in review of the Defense Authorization Request for Fiscal Year 2014 and the Future Years Defense Program	March 19, 2013	Armed Services	Emerging Threats and Capabilities
Fiscal 2014 Defense Authorization, Strategic Command: U.S. Cyber Command	March 12, 2013	Armed Services	
The Cybersecurity Partnership Between the Private Sector and Our Government: Protecting Our National and Economic Security	March 7, 2013	(Joint) Homeland Security and Governmental Affairs and Commerce, Science, and Transportation	

Source: Compiled by CRS.

Table 19. 113th Congress, Other Hearings, by Date

Title	Date	Committee	Subcommittee
U.S.-China Cybersecurity Issues	July 11, 2013	Congressional-Executive Commission on China	
Chinese Hacking: Impact on Human Rights and Commercial Rule of Law	June 25, 2013	Congressional-Executive Commission on China	

Source: Compiled by CRS.

Table 20. 113th Congress, Senate Hearings, by Committee

Committee	Subcommittee	Title	Date
Appropriations	Homeland Security	Investing in Cybersecurity: Understanding Risks and Building Capabilities for the Future	May 7, 2014
Appropriations		Cybersecurity: Preparing for and Responding to the Enduring Threat	June 12, 2013
Armed Services		Nomination of Vice Admiral Michael S. Rogers, USN to be admiral and Director, National Security Agency/ Chief, Central Security Services/ Commander, U.S. Cyber Command	March 11, 2014
Armed Services		U.S. Strategic Command and U.S. Cyber Command in review of the Fiscal 2015 Defense Authorization Request and the Future Years Defense Program	February 27, 2014
Armed Services		Resilient Military Systems and the Advanced Cyber Threat (CLOSED BRIEFING)	June 26, 2013
Armed Services	Emerging Threats and Capabilities	Defense Authorization: Cybersecurity Threats	March 19, 2013
Armed Services		Fiscal 2014 Defense Authorization, Strategic Command: U.S. Cyber Command	March 12, 2013
Banking, Housing, and Urban Affairs		Cybersecurity: Enhancing Coordination to Protect the Financial Sector	December 10, 2014
Banking, Housing, and Urban Affairs		Oversight of Financial Stability and Data Security	February 6, 2014

Committee	Subcommittee	Title	Date
Banking, Housing, and Urban Affairs	National Security and International Trade and Finance	Safeguarding Consumers' Financial Data	February 3, 2014
Commerce, Science, and Transportation		Protecting Personal Consumer Information from Cyber Attacks and Data Breaches	March 26, 2014
Commerce, Science, and Transportation		The Partnership Between NIST [National Institute of Standards and Technology] and the Private Sector: Improving Cybersecurity	July 25, 2013
Homeland Security and Governmental Affairs		Data Breach on the Rise: Protecting Personal Information from Harm	April 2, 2014
Homeland Security and Governmental Affairs		Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure	March 26, 2014
(Joint) Homeland Security and Governmental Affairs and Commerce, Science, and Transportation		The Cybersecurity Partnership Between the Private Sector and Our Government: Protecting Our National and Economic Security	March 7, 2013
Judiciary	Crime and Terrorism	Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks	July 15, 2014
Judiciary		Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime	February 4, 2014
Judiciary	Crime and Terrorism	Cyber Threats: Law Enforcement and Private Sector Responses	May 8, 2013

Source: Compiled by CRS.

Table 21. 113th Congress, Other Hearings, by Committee

Committee	Subcommittee	Title	Date
Congressional-Executive Commission on China		U.S.-China Cybersecurity Issues	July 11, 2013
Congressional-Executive Commission on China		Chinese Hacking: Impact on Human Rights and Commercial Rule of Law	June 25, 2013

Source: Compiled by CRS.

Executive Orders and Presidential Directives

Executive orders are official documents through which the President of the United States manages the operations of the federal government. Presidential directives guide the federal rulemaking policy and are signed or authorized by the President.

CRS Reports on Executive Orders and Presidential Directives

The following reports provide additional information on executive orders and presidential directives:

- CRS Report R42984, *The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress*, by Eric A. Fischer et al.
- CRS Report RS20846, *Executive Orders: Issuance, Modification, and Revocation*, by Vivian S. Chu and Todd Garvey
- CRS Report R42740, *National Security and Emergency Preparedness Communications: A Summary of Executive Order 13618*, by Shawn Reese.

Table 22 provides a list of executive orders and presidential directives pertaining to cybersecurity. (Titles are linked to documents.)

Table 22. Executive Orders and Presidential Directives

(by date of issuance)

Title	Date	Source	Notes
E.O. 13801, Expanding Apprenticeships in America	June 20, 2017	White House	The Secretaries of Commerce and Labor shall promote apprenticeships to business leaders across critical industry sectors, including manufacturing, infrastructure, cybersecurity, and health care.
Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure	May 11, 2017	White House	The order requires an assessment of cybersecurity risks at every agency, orders a review of current efforts to protect vital infrastructure like power plants and hospitals, and requires a report on building the cybersecurity workforce.
Amended Executive Order 13694, Cyber-Related Sanctions Designations	December 29, 2016	Treasury Department	Authorizes the imposition of sanctions on individuals and entities determined to be responsible for or complicit in malicious cyber-enabled activities that result in enumerated harms that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States. The authority has been amended to also allow for the imposition of sanctions on individuals and entities determined to be responsible for tampering, altering, or causing the misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions. Five entities and four individuals are identified in the Annex of the amended Executive Order and will be added to OFAC's list of Specially Designated Nationals and Blocked Persons (SDN List). OFAC today is designating an additional two individuals who also will be added to the SDN List.
E.O. 13757, Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities	December 29, 2016	White House	This amends Executive Order 13694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," which authorized the imposition of sanctions on individuals and entities determined to be responsible for or complicit in malicious cyber-enabled activities that result in enumerated harms that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States. The authority has been amended to allow for the imposition of sanctions on individuals and

Title	Date	Source	Notes
			entities determined to be responsible for tampering, altering, or causing the misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions. Five entities and four individuals are identified in the Annex of the amended executive order and will be added to the Office of Foreign Assets Control's (OFAC's) list of Specially Designated Nationals and Blocked Persons (SDN List). At this writing, two additional individuals will be added to the SDN List.
E.O. 13741, Amending Executive Order 13467 To Establish the Roles and Responsibilities of the National Background Investigations Bureau and Related Matters	September 29, 2016	White House	NBIB, established within the Office of Personnel Management, has responsibility for conducting effective, efficient, and secure personnel background investigations. NBIB will partner with the Department of Defense, which will build and manage a new IT platform for the background checks.
Presidential Policy Directive 41—United States Cyber Incident Coordination	July 26, 2016	White House	The PPD sets forth principles governing the federal government's response to any cyber incident, whether involving government or private-sector entities. For significant cyber incidents, the PPD establishes lead federal agencies and architecture for coordinating the broader federal government response. The PPD also requires the Departments of Justice and Homeland Security to maintain updated contact information for public use to assist entities affected by cyber incidents in reporting those incidents to the proper authorities.
Annex for Presidential Policy Directive 41—United States Cyber Incident Coordination	July 26, 2016	White House	The annex to PPD-41 provides further details concerning the federal government coordination architecture for significant cyber incidents and prescribes certain implementation tasks pertaining to coordination architecture, federal government response to incidents affecting federal networks, and implementation and assessment.
E.O. 13718, Commission on Enhancing National Cybersecurity	February 9, 2016	White House	The commission will consist of 12 members appointed by the President, including "top strategic, business, and technical thinkers from outside of Government—including members to be designated by the bi-partisan Congressional leadership."
E.O. 13694, Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities	April 1, 2015	White House	The executive order establishes the first sanctions program to allow the Administration to impose penalties on individuals overseas who engage in destructive attacks or commercial espionage in cyberspace. The order declares "significant

Title	Date	Source	Notes
			malicious cyber-enabled activities" a "national emergency" and enables the Treasury Secretary to target foreign individuals and entities that take part in the illicit cyberactivity for sanctions that could include freezing their financial assets and barring commercial transactions with them.
Presidential Memorandum—Establishment of the Cyber Threat Intelligence Integration Center	February 25, 2015	White House	The CTIIC will be a national intelligence center focused on "connecting the dots" regarding malicious foreign cyber threats to the nation and cyber incidents affecting U.S. national interests, and on providing all-source analysis of threats to U.S. policymakers. The CTIIC will also assist relevant departments and agencies in their efforts to identify, investigate, and mitigate those threats
E.O. 13691, Encouraging Private-Sector Cybersecurity Collaboration	February 12, 2015	White House	The executive order calls for establishing new "information sharing and analysis organizations to serve as focal points for cybersecurity information sharing and collaboration within the private sector and between the private sector and government." It also aims to streamline the process companies use to sign agreements with the federal government and grants DHS new powers to approve sharing classified intelligence with the private sector.
E.O. 13687, Imposing Additional Sanctions with Respect to North Korea	January 2, 2015	White House	The executive order states that North Korea engaged in "provocative, destabilizing, and repressive actions and policies," including "destructive, coercive cyber-related actions during November and December 2014," and authorizes sanctions against North Korea. The sanctions prohibit the people and organizations named from accessing the U.S. financial system and forbid any banks or other financial institutions that do business with the U.S. system from doing business with the sanctioned entities.
E.O. 13681, Improving the Security of Consumer Financial Transactions	October 17, 2014	White House	The executive order mandates that government credit and debit cards be enabled with chip and PIN technology and federal facilities accept chip and PIN-enabled cards at retail terminals.
E.O. 13636, Improving Critical Infrastructure Cybersecurity	February 12, 2013	White House	E.O. 13636 addresses cybersecurity threats to critical infrastructure (CI) by, among other things, • expanding to other CI sectors an existing DHS program for information sharing and collaboration between the

Title	Date	Source	Notes
			government and the private sector; • establishing a broadly consultative process for identifying CI with especially high priority for protection; • requiring the National Institute of Standards and Technology to lead in developing a Cybersecurity Framework of standards and best practices for protecting CI; and • requiring regulatory agencies to determine the adequacy of current requirements and their authority to establish requirements to address the risks.
Presidential Policy Directive (PPD) 21 - Critical Infrastructure Security and Resilience	February 12, 2013	White House	This directive establishes national policy on critical infrastructure security and resilience. This endeavor is a shared responsibility among the federal, state, local, tribal, and territorial (SLTT) entities, and public and private owners and operators of critical infrastructure (hereinafter referred to as "critical infrastructure owners and operators"). This directive also refines and clarifies the critical infrastructure-related functions, roles, and responsibilities across the federal government, as well as enhances overall coordination and collaboration. The federal government also has a responsibility to strengthen the security and resilience of its own critical infrastructure, for the continuity of national essential functions, and to organize itself to partner effectively with and add value to the security and resilience efforts of critical infrastructure owners and operators.
E. O. 13618, Assignment of National Security and Emergency Preparedness Communications Functions	July 6, 2012	White House	This order addresses the federal government's need and responsibility to communicate during national security and emergency situations and crises by assigning federal national security and emergency preparedness communications functions. EO 13618 is a continuation of older executive orders issued by other presidents and is related to the Communications Act of 1934 (47 U.S.C. §606). This executive order, however, changes federal national security and emergency preparedness communications functions by dissolving the National Communications System, establishing an executive committee to oversee federal national security and emergency preparedness communications functions, establishing a programs office within the DHS to assist the executive committee, and

Title	Date	Source	Notes
			assigning specific responsibilities to federal government entities.
E.O. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible	October 7, 2011	White House	This order directs structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks that shall be consistent with appropriate protections for privacy and civil liberties. Agencies bear the primary responsibility for meeting these twin goals. These policies and minimum standards will address all agencies that operate or access classified computer networks, all users of classified computer networks (including contractors and others who operate or access classified computer networks controlled by the federal government), and all classified information on those networks.
HSPD-23/NSPD-54 -Cybersecurity Policy	January 8, 2008	White House	This directive establishes U.S. policy, strategy, guidelines, and implementation actions to secure cyberspace. It strengthens and augments existing policies for protecting the security and privacy of information entrusted to the federal government and clarifies roles and responsibilities of federal agencies relating to cybersecurity. It requires the federal government to integrate many of its technical and organizational capabilities to better address sophisticated cybersecurity threats and vulnerabilities.
E.O. 13407, Public Alert and Warning System	June 26, 2006	White House	The order assigns the Secretary of Homeland Security the responsibility to establish or adopt, as appropriate, common alerting and warning protocols, standards, terminology, and operating procedures for the public alert and warning system to enable interoperability and the secure delivery of coordinated messages to the American people through as many communication pathways as practicable, taking account of Federal Communications Commission rules as provided by law.
HSPD-7, Homeland Security Presidential Directive No. 7: Critical Infrastructure Identification, Prioritization, and Protection	December 17, 2003	White House	Assigns the Secretary of Homeland Security the responsibility of coordinating the nation's overall efforts in critical infrastructure protection across all sectors. HSPD-7 also designates the DHS as lead agency for the nation's information and telecommunications sectors.
E.O. 13286, Amendment of Executive Orders, and Other Actions, in Connection With the Transfer of Certain Functions to the Secretary of Homeland Security	February 28, 2003	White House	Designates the Secretary of Homeland Security the Executive Agent of the National Communication System Committee of Principals, which are the agencies, designated by the President,

Title	Date	Source	Notes
			that own or lease telecommunication assets identified as part of the National Communication System, or which bear policy, regulatory, or enforcement responsibilities of importance to national security and emergency preparedness telecommunications.
Presidential Decision Directive/NSC-63	May 22, 1998	White House	Sets as a national goal the ability to protect the nation's critical infrastructure from intentional attacks (both physical and cyber) by the year 2003. According to the PDD, any interruptions in the ability of these infrastructures to provide their goods and services must be "brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States."
NSD-42, National Security Directive 42 - National Policy for the Security of National Security Telecommunications and Information Systems	July 5, 1990	White House	Establishes the National Security Telecommunications and Information Systems Security Committee, now called the Committee on National Security Systems (CNSS). CNSS is an interagency committee, chaired by the Department of Defense. Among other assignments, NSD-42 directs the CNSS to provide system security guidance for national security systems to executive departments and agencies and submit annually to the Executive Agent an evaluation of the security status of national security systems. NSD-42 also directs the CNSS to interact, as necessary, with the National Communications System Committee of Principals.

Source: Descriptions compiled by CRS from government websites.

Author Contact Information

Rita Tehan
Information Research Specialist
rtehan@crs.loc.gov, 7-6739

Key CRS Policy Staff

See CRS Report R42619, *Cybersecurity: CRS Experts*, by Eric A. Fischer, for the names and contact information for CRS experts on policy issues related to cybersecurity bills.