



**Congressional
Research Service**

Informing the legislative debate since 1914

Cybersecurity: Legislation, Hearings, and Executive Branch Documents

Rita Tehan

Information Research Specialist

September 8, 2015

Congressional Research Service

7-5700

www.crs.gov

R43317

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, in the last days of the 113th Congress, five cybersecurity bills were signed by the President. These bills change 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.

In April 2011, the Obama Administration sent Congress legislative proposals that would have given the federal government new authority to ensure that corporations owning assets most critical to the nation’s security and economic prosperity adequately addressed risks posed by cybersecurity threats. This report provides links to cybersecurity legislation in the 112th, 113th, and 114th Congresses.

- 114th Congress Legislation, House, **Table 1**
- 114th Congress Legislation, Senate, **Table 2**
- 113th Congress, Major Legislation, **Table 3** and **Table 4**
- 112th Congress, Major Legislation, **Table 5** and **Table 7**
- 112th Congress, Senate Floor Debate: S. 3414, **Table 6**
- 112th Congress, House Floor Debate: H.R. 3523, **Table 8**

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

- 114th Congress, Senate Hearings, **Table 9** and **Table 10**
- 114th Congress, House Hearings, **Table 11** and **Table 12**
- 113th Congress, House Hearings, **Table 14** and **Table 15**
- 113th Congress, House Committee Markups, **Table 16**
- 113th Congress, Senate Hearings, **Table 17** and **Table 19**
- 113th Congress, Other Hearings, **Table 18** and **Table 20**

- 112th Congress, House Hearings, **Table 21** and **Table 22**
- 112th Congress, House Markups, **Table 23**
- 112th Congress, Senate Hearings, **Table 24** and **Table 25**
- 112th Congress, Congressional Committee Investigative Reports, **Table 26**

For a discussion of selected legislative proposals in the 112th and 113th Congresses, see CRS Report R42114, *Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation*, by Eric A. Fischer.

For a comparison of House and Senate information-sharing legislation in the 114th Congress, see CRS Report R44069, *Cybersecurity and Information Sharing: Comparison of House and Senate Bills in the 114th Congress*, by Eric A. Fischer and Stephanie M. Logan.

For a side-by-side comparison of cybersecurity and information legislation in the 114th Congress, see 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.

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.

- Executive Orders and Presidential Directives, **Table 27**

For a selected list of authoritative reports and resources on cybersecurity, see CRS Report R42507, *Cybersecurity: Authoritative Reports and Resources, by Topic*, by Rita Tehan. For selected cybersecurity data, statistics, and glossaries, see CRS Report R43310, *Cybersecurity: Data, Statistics, and Glossaries*, by Rita Tehan.

Contents

| | |
|---|----|
| Legislation | 1 |
| CRS Reports and Other CRS Products: Legislation | 3 |
| Hearings in the 114 th Congress..... | 10 |
| Hearings in the 113 th Congress..... | 20 |
| Hearings in the 112 th Congress..... | 30 |
| Executive Orders and Presidential Directives | 40 |
| CRS Reports on Executive Orders and Presidential Directives | 40 |

Tables

| | |
|---|----|
| Table 1. 114 th Congress Legislation: House | 4 |
| Table 2. 114 th Congress Legislation: Senate..... | 6 |
| Table 3. 113 th Congress, Major Legislation: Senate | 7 |
| Table 4. 113 th Congress, Major Legislation: House..... | 8 |
| Table 5. 112 th Congress, Major Legislation: Senate | 9 |
| Table 6. 112 th Congress, Senate Floor Debate: S. 3414..... | 9 |
| Table 7. 112 th Congress, Major Legislation: House..... | 10 |
| Table 8. 112 th Congress, House Floor Debate: H.R. 3523 | 10 |
| Table 9. 114 th Congress, Senate Hearings, by Date | 11 |
| Table 10. 114 th Congress, Senate Hearings, by Committee..... | 12 |
| Table 11. 114 th Congress, House Hearings, by Date..... | 14 |
| Table 12. 114 th Congress, House Hearings, by Committee | 17 |
| Table 13. 114 th Congress, Other Hearings | 19 |
| Table 14. 113 th Congress, House Hearings, by Date | 21 |
| Table 15. 113 th Congress, House Hearings, by Committee | 23 |
| Table 16. 113 th Congress, House Committee Markups, by Date | 26 |
| Table 17. 113 th Congress, Senate Hearings, by Date | 26 |
| Table 18. 113 th Congress, Other Hearings, by Date..... | 28 |
| Table 19. 113 th Congress, Senate Hearings, by Committee..... | 28 |
| Table 20. 113 th Congress, Other Hearings, by Committee | 29 |
| Table 21. 112 th Congress, House Hearings, by Date | 31 |
| Table 22. 112 th Congress, House Hearings, by Committee | 33 |
| Table 23. 112 th Congress, House Markups, by Date..... | 36 |
| Table 24. 112 th Congress, Senate Hearings, by Date | 36 |
| Table 25. 112 th Congress, Senate Hearings, by Committee..... | 37 |
| Table 26. 112 th Congress, Congressional Committee Investigative Reports | 39 |
| Table 27. Executive Orders and Presidential Directives | 41 |

Contacts

| | |
|----------------------------------|----|
| Author Contact Information | 44 |
| Key CRS Policy Staff..... | 44 |

Legislation

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

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.

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 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.

¹ The White House, Complete Cybersecurity Proposal, 2011, <http://www.whitehouse.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.

In February 2015, the White House issued Executive Order 13691³, 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 memorandum⁵, 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 the sharing of information with the Department of Homeland Security by protecting entities from civil liabilities.

In the Senate, S. 754, the Cybersecurity Information Sharing Act of 2015 (CISA), which was reported in March, was proposed to be considered as an amendment to H.R. 1735, the National Defense Authorization Act (NDAA). More than 70 amendments to CISA have been submitted and a managers' amendment has been circulated. A cloture motion was filed on August 5, 2015.

For a comparison of House and Senate information-sharing legislation in the 114th Congress, see CRS Report R44069, *Cybersecurity and Information Sharing: Comparison of House and Senate Bills in the 114th Congress*, by Eric A. Fischer and Stephanie M. Logan.

For a side-by-side comparison of cybersecurity and information legislation in the 114th Congress, see 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.

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>

CRS Reports and Other CRS Products: Legislation

- CRS Report R43831, *Cybersecurity Issues and Challenges: In Brief*, by Eric A. Fischer
- CRS Report R44069, *Cybersecurity and Information Sharing: Comparison of House and Senate Bills in the 114th Congress*, by Eric A. Fischer and Stephanie M. Logan
- 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 Insight IN10186, *Cybersecurity: FISMA Reform*, by Eric A. Fischer
- CRS Report R42474, *Selected Federal Data Security Breach Legislation*, by Kathleen Ann Ruane
- CRS Report R42475, *Data Security Breach Notification Laws*, by Gina Stevens
- CRS Legal Sidebar WSLG480, *Privacy and Civil Liberties Issues Raised by CISPA*, by Andrew Nolan
- CRS Legal Sidebar WSLG478, *House Intelligence Committee Marks Up Cybersecurity Bill CISPA*, by Richard M. Thompson II
- CRS Legal Sidebar CRS Legal Sidebar WSLG481, *CISPA, Private Actors, and the Fourth Amendment*, by Richard M. Thompson II
- CRS Legal Sidebar WSLG483, *Obstacles to Private Sector Cyber Threat Information Sharing*, by Edward C. Liu and Edward C. Liu

Table I. 114th Congress Legislation: House

| Bill No. | Title | Committee(s) | Date Introduced | Latest Major Action | Date |
|-----------------|--|--|------------------------|---|------------------|
| H.R. 53 | Cyber Security Education and Federal Workforce Enhancement Act | Education and the Workforce; Homeland Security; Science, Space, and Technology | January 6, 2015 | Referred to Subcommittee of Higher Education and Workforce Training | April 29, 2015 |
| H.R. 60 | Cyber Defense National Guard Act | Committee on Intelligence (Permanent Select) | January 6, 2015 | Referred to committee | January 6, 2015 |
| H.R. 104 | Cyber Privacy Fortification Act of 2015 | Judiciary | January 6, 2015 | Referred to Subcommittee on Crime, Terrorism, Homeland Security, and Investigations | January 22, 2015 |
| H.R. 234 | Cyber Intelligence Sharing and Protection Act | Armed Services, Homeland Security, Intelligence (Permanent), Judiciary | January 8, 2015 | Referred to the Subcommittee on the Constitution and Civil Justice | February 2, 2015 |
| H.R. 451 | Safe and Secure Federal Websites Act of 2015 | Oversight and Government Reform | January 21, 2015 | Ordered to be Reported (Amended) by Voice Vote | May 19, 2015 |
| H.R. 580 | Data Accountability and Trust Act | Energy and Commerce | January 28, 2015 | Referred to subcommittee | January 30, 2015 |
| H.R. 1073 | Critical Infrastructure Protection Act (CIPA) | Homeland Security | February 25, 2015 | Placed on the Union Calendar | August 4, 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 27, 2015 |
| H.R. 1584 | Cybercrime Anti-Resale Deterrent Extraterritoriality Revision (CARDER) Act | Judiciary | March 24, 2015 | Referred to Subcommittee on Crime, Terrorism, Homeland Security, and Investigations | April 21, 2015 |

| Bill No. | Title | Committee(s) | Date Introduced | Latest Major Action | Date |
|-----------------|---|--|------------------------|--|----------------|
| H.R. 1704 | Personal Data Notification and Protection Act | Judiciary, Energy and Commerce | March 26, 2015 | Referred to Subcommittee on the Constitution and Civil Justice | April 29, 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. 1753 | Executive Cyberspace Coordination Act | Oversight and Government Reform | April 13, 2015 | Referred to committee | April 13, 2015 |
| H.R. 1770 | Data Security and Breach Notification Act of 2015 | Energy & Commerce | April 14, 2015 | Referred to the Subcommittee on Commerce, Manufacturing, and Trade | April 17, 2015 |
| H.R. 3305 | EINSTEIN Act of 2015 | Oversight and Government Reform; Homeland Security | July 29, 2015 | Referred to committees | July 29, 2015 |

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

Table 2. 114th Congress Legislation: Senate

| Bill No. | Title | Committee(s) | Date Introduced | Latest Major Action | Date |
|-----------------|---|--|------------------------|---|-------------------|
| 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 | Cloture motion on the motion to proceed to the measure withdrawn by unanimous consent in Senate | August 5, 2015 |
| S. 1027 | Cybersecurity Information Sharing Credit Act | 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.

Table 3 and **Table 4** provide lists of Senate and House legislation under consideration in the 113th Congress.

Table 3. 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 4. 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.

Table 5 and **Table 7** list major Senate and House legislation considered by the 112th Congress. The tables include bills with committee action, floor action, or significant legislative interest. **Table 6** provides *Congressional Record* links to Senate floor debate of S. 3414, the Cybersecurity Act of 2012. **Table 8** provides *Congressional Record* links to House floor debate of H.R. 3523, the Cyber Intelligence Sharing and Protection Act.

Table 5. 112th Congress, Major Legislation: Senate

| Bill No. | Title | Committee(s) | Date Introduced |
|----------|--|--|-------------------|
| S. 3414 | Cybersecurity Act of 2012 | N/A (Placed on Senate Legislative Calendar under Read the First Time) | July 19, 2012 |
| S. 3342 | SECURE IT | N/A (Placed on Senate Legislative Calendar under General Orders. Calendar No. 438) | June 27, 2012 |
| S. 3333 | Data Security and Breach Notification Act of 2012 | Commerce, Science, and Transportation | June 21, 2012 |
| S. 2151 | SECURE IT | Commerce, Science, and Transportation | March 1, 2012 |
| S. 2105 | Cybersecurity Act of 2012 | Homeland Security and Governmental Affairs | February 14, 2012 |
| S. 2102 | Cybersecurity Information Sharing Act of 2012 | Homeland Security and Governmental Affairs | February 13, 2012 |
| S. 1535 | Personal Data Protection and Breach Accountability Act of 2011 | Judiciary | September 8, 2011 |
| S. 1342 | Grid Cyber Security Act | Energy and Natural Resources | July 11, 2011 |
| S. 1151 | Personal Data Privacy and Security Act of 2011 | Judiciary | June 7, 2011 |
| S. 413 | Cybersecurity and Internet Freedom Act of 2011 | Homeland Security and Governmental Affairs | February 17, 2011 |

Source: LIS.

Table 6. 112th Congress, Senate Floor Debate: S. 3414

| Title | Date | Congressional Record Pages |
|---|-------------------|----------------------------|
| Cybersecurity Act of 2012: Motion to Proceed | July 26, 2012 | S5419-S5449 |
| Cybersecurity Act of 2012: Motion to Proceed—Continued and Cloture Vote | July 26, 2012 | S5450-S5467 |
| Cybersecurity Act of 2012 | July 31, 2012 | S5694-S5705 |
| Cybersecurity Act of 2012: Continued | July 31, 2012 | S5705-S5724 |
| Cybersecurity Act of 2012: Debate and Cloture Vote | August 2, 2012 | S5907-S5919 |
| Cybersecurity Act of 2012: Motion to Proceed | November 14, 2012 | S6774-S6784 |

Source: *Congressional Record*, Government Publishing Office (GPO).

Table 7. 112th Congress, Major Legislation: House

| Bill No. | Title | Committee(s) | Date Introduced |
|-----------|---|--|-------------------|
| H.R. 4257 | Federal Information Security Amendments Act of 2012 | Oversight and Government Reform | March 26, 2012 |
| H.R. 3834 | Advancing America's Networking and Information Technology Research and Development Act of 2012 | Science, Space, and Technology | January 27, 2012 |
| H.R. 4263 | SECURE IT Act of 2012 Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology | Oversight and Government Reform; Judiciary; Armed Services; Intelligence (Permanent Select) | March 27, 2012 |
| H.R. 3674 | PRECISE Act of 2012 | Homeland Security; Oversight and Government Reform; Science, Space, and Technology; Judiciary; Intelligence (Permanent Select) | December 15, 2011 |
| H.R. 3523 | Cyber Intelligence Sharing and Protection Act | Committee on Intelligence (Permanent Select) | November 30, 2011 |
| H.R. 2096 | Cybersecurity Enhancement Act of 2012 | Science, Space, and Technology | June 2, 2011 |
| H.R. 174 | Homeland Security Cyber and Physical Infrastructure Protection Act of 2011 | Technology; Education and the Workforce; Homeland Security | January 5, 2011 |
| H.R. 76 | Cybersecurity Education Enhancement Act of 2011 | Homeland Security; House Oversight and Government Reform | January 5, 2011 |

Source: LIS.

Table 8. 112th Congress, House Floor Debate: H.R. 3523

| Title | Date | Congressional Record Pages |
|---|----------------|----------------------------|
| Cyber Intelligence Sharing and Protection Act: Providing for Consideration of Motion to Suspend the Rules | April 26, 2012 | H2147-2156 |
| Cyber Intelligence Sharing and Protection Act: Consideration of the Bill | April 26, 2012 | H2156-2186 |

Source: *Congressional Record* (GPO).

Hearings in the 114th Congress

The following tables list cybersecurity hearings in the 114th Congress. **Table 9** and **Table 10** contain identical content but are organized differently. **Table 11** lists House hearings arranged by date (most recent first), and **Table 12** 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 9. 114th Congress, Senate Hearings, by Date

| 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 | |
| [CLOSED] Markup of the “Cybersecurity Information Sharing Act of 2015” | March 12, 2015 | Intelligence | |

| Title | Date | Committee | Subcommittee |
|--|-------------------|--|---|
| 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 114 th Congress | February 5, 2015 | Commerce, Science & Transportation | Consumer Protection, Product Safety, Insurance, and Data Security |
| 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 10. 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 | 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 |
| 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 |

| Committee | Subcommittee | Title | Date |
|--|--|---|------------------|
| Commerce, Science & Transportation | | Getting it Right on Data Breach and Notification Legislation in the 114 th 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 |
| 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 | | 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 | | Counterterrorism, Counterintelligence, and the Challenges of "Going Dark" | July 8, 2015 |
| Intelligence | | [CLOSED] Markup of the "Cybersecurity Information Sharing Act of 2015" | March 12, 2015 |
| Judiciary | | Cyber Crime: Modernizing our Legal Framework for the Information Age | July 8, 2015 |

Source: Compiled by CRS from Congress.gov.

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

| Title | Date | Committee | Subcommittee |
|--|--------------------|---------------------------------|---|
| 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 | |
| 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 | |
| [CLOSED] Special Activities | April 15, 2015 | Intelligence | National Security Agency and Cybersecurity |
| Markup: H.R. 1731, the National Cybersecurity Protection Advancement Act of 2015 | April 14, 2015 | Homeland Security | |
| Markup of H.R. 1770, The Data Security and Breach Notification Act of 2015 | April 14, 2015 | Energy and Commerce | |
| [CLOSED] Markup of "Protecting Cyber Networks Act" | March 26, 2015 | Intelligence | |
| The Internet of Things: Exploring the Next Technology Frontier | March 24, 2015 | Energy and Commerce | Commerce, Manufacturing and Trade |
| [MARKUP] H.R. 1704, Data Security and Breach Notification Act of 2015 | March 24, 2015 | Energy and Commerce | |
| 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 21 st 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 12. 114th Congress, House Hearings, by Committee

| Committee | Subcommittee | Title | Date |
|---------------------|---|--|------------------|
| 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 | | Markup of H.R. 1770, The Data Security and Breach Notification Act of 2015 | April 14, 2015 |
| Energy and Commerce | Commerce, Manufacturing, and Trade | The Internet of Things: Exploring the Next Technology Frontier | March 24, 2015 |
| Energy and Commerce | | [MARKUP] H.R. 1704, Data Security and Breach Notification Act of 2015 | 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 21 st 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 |
| 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 | Promoting and Incentivizing Cybersecurity Best Practices | July 28, 2015 |

| Committee | Subcommittee | Title | Date |
|---------------------------------|---|---|--------------------|
| Homeland Security | Cybersecurity, Infrastructure Protection and Security Technologies | Oversight and Government Reform | June 24, 2015 |
| Homeland Security | | Markup: H.R. 1731, the National Cybersecurity Protection Advancement Act of 2015 | April 14, 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 | | [CLOSED] Markup of "Protecting Cyber Networks Act" | March 26, 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 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 |

| Committee | Subcommittee | Title | Date |
|---|-------------------------|---|--------------------|
| 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 |
| Examining Vulnerabilities of America’s Power Supply | | Examining Vulnerabilities of America's Power Supply | September 10, 2015 |
| Science, Space & Technology | Research and Technology | The Expanding Cyber Threat | January 27, 2015 |
| Small Business | | Small Business, Big Threat: Protecting Small Businesses from Cyber Attacks | April 22, 2015 |

Source: Compiled by CRS from Congress.gov.

Table 13. 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. **Table 14** and **Table 15** contain identical content but are organized differently. **Table 14** lists House hearings arranged by date (most recent first), and **Table 15** 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 14. 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: 21 st 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 21 st 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 15. 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 |
| Energy and Commerce | | Cyber Threats and Security Solutions | May 21, 2013 |

| Committee | Subcommittee | Title | Date |
|--|---|--|--------------------|
| 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 21 st 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 16. 113th Congress, House Committee Markups, by Date

| Committee | Subcommittee | Title | Date |
|-------------------|---|--|--------------------|
| Homeland Security | | H.R. 3696, National Cybersecurity and Critical Infrastructure Protection Act | February 5, 2014 |
| Homeland Security | Cybersecurity, Infrastructure Protection, and Security Technologies | H.R. 3696, National Cybersecurity and Critical Infrastructure Protection Act | January 15, 2014 |
| Homeland Security | Cybersecurity, Infrastructure Protection, and Security Technologies | H.R. 2952, CIRDA Act of 2013, and H.R. 3107, the Homeland Security Cybersecurity Boots-on-the-Ground Act | September 18, 2013 |

Source: Compiled by CRS.

Table 17. 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 | |
| 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 | |

| Title | Date | Committee | Subcommittee |
|---|------------------|--|---|
| 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 |
| 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 18. 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 19. 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 |
| Banking, Housing, and Urban Affairs | National Security and International Trade and Finance | Safeguarding Consumers' Financial Data | February 3, 2014 |

| Committee | Subcommittee | Title | Date |
|--|---------------------|---|------------------|
| 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 20. 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.

Hearings in the 112th Congress

The following tables list cybersecurity hearings in the 112th Congress. **Table 21** and **Table 22** contain identical content but are organized differently. **Table 21** lists House hearings arranged by date (most recent first) and **Table 22** lists House hearings arranged by committee. **Table 23** lists House markups by date; **Table 24** and **Table 25** contain identical content. **Table 24** lists Senate hearings arranged by date and **Table 25** lists Senate hearings arranged by committee. **Table 26** lists two congressional committee investigative reports: the House Permanent Select Committee on Intelligence investigative report into the counterintelligence and security threats posed by Chinese telecommunications companies doing business in the United States, and the Senate Permanent Subcommittee on Investigations' review of U.S. Department of Homeland Security efforts to engage state and local intelligence "fusion centers." When viewed in HTML, the document titles are active links to the committee's website for that particular hearing.

Table 21. 112th Congress, House Hearings, by Date

| Title | Date | Committee | Subcommittee |
|--|--------------------|--|---|
| Investigation of the Security Threat Posed by Chinese Telecommunications Companies Huawei and ZTE | September 13, 2012 | Permanent Select Committee on Intelligence | |
| Resilient Communications: Current Challenges and Future Advancements | September 12, 2012 | Homeland Security | Emergency Preparedness, Response, and Communications |
| Cloud Computing: An Overview of the Technology and the Issues facing American Innovators | July 25, 2012 | Judiciary | Intellectual Property, Competition, and the Internet |
| Digital Warriors: Improving Military Capabilities for Cyber Operations | July 25, 2012 | Armed Services | Emerging Threats and Capabilities |
| Cyber Threats to Capital Markets and Corporate Accounts | June 1, 2012 | Financial Services | Capital Markets and Government Sponsored Enterprises |
| Iranian Cyber Threat to U.S. Homeland | April 26, 2012 | Homeland Security | Cybersecurity, Infrastructure Protection, and Security Technologies and Counterterrorism and Intelligence |
| America is Under Cyber Attack: Why Urgent Action is Needed | April 24, 2012 | Homeland Security | Oversight, Investigations and Management |
| The DHS and DOE National Labs: Finding Efficiencies and Optimizing Outputs in Homeland Security Research and Development | April 19, 2012 | Homeland Security | Cybersecurity, Infrastructure Protection, and Security Technologies |
| Cybersecurity: Threats to Communications Networks and Public-Sector Responses | March 28, 2012 | Energy and Commerce | Communications and Technology |
| IT Supply Chain Security: Review of Government and Industry Efforts | March 27, 2012 | Energy and Commerce | Oversight and Investigations |
| Fiscal Year 2013 Budget Request for Information Technology and Cyber Operations Programs | March 20, 2012 | Armed Services | Emerging Threats and Capabilities |
| Cybersecurity: The Pivotal Role of Communications Networks | March 7, 2012 | Energy and Commerce | Communications and Technology |
| NASA Cybersecurity: An Examination of the Agency's Information Security | February 29, 2012 | Science, Space, and Technology | Investigations and Oversight |
| Critical Infrastructure Cybersecurity: Assessments of Smart Grid Security | February 28, 2012 | Energy and Commerce | Oversight and Investigations |
| Hearing on Draft Legislative Proposal on Cybersecurity | December 6, 2011 | Homeland Security and Governmental Affairs | Cybersecurity, Infrastructure Protection, and Security Technologies |

| Title | Date | Committee | Subcommittee |
|---|--------------------|--|---|
| Cyber Security: Protecting Your Small Business | December 1, 2011 | Small Business | Healthcare and Technology |
| Combating Online Piracy (H.R. 3261, Stop the Online Piracy Act) | November 16, 2011 | Judiciary | |
| Cybersecurity: Protecting America's New Frontier | November 15, 2011 | Judiciary | Crime, Terrorism and Homeland Security |
| Institutionalizing Irregular Warfare Capabilities | November 3, 2011 | Armed Services | Emerging Threats and Capabilities |
| Cloud Computing: What are the Security Implications? | October 6, 2011 | Homeland Security | Cybersecurity, Infrastructure Protection, and Security Technologies |
| Cyber Threats and Ongoing Efforts to Protect the Nation | October 4, 2011 | Permanent Select Intelligence | |
| The Cloud Computing Outlook | September 21, 2011 | Science, Space, and Technology | Technology and Innovation |
| Cybersecurity: Threats to the Financial Sector | September 14, 2011 | Financial Services | Financial Institutions and Consumer Credit |
| Cybersecurity: An Overview of Risks to Critical Infrastructure | July 26, 2011 | Energy and Commerce | Oversight and Investigations |
| Cybersecurity: Assessing the Nation's Ability to Address the Growing Cyber Threat | July 7, 2011 | Oversight and Government Reform | |
| Field Hearing: "Hacked Off: Helping Law Enforcement Protect Private Financial Information" | June 29, 2011 | Financial Services (field hearing in Hoover, AL) | |
| Examining the Homeland Security Impact of the Obama Administration's Cybersecurity Proposal | June 24, 2011 | Homeland Security | Cybersecurity, Infrastructure Protection, and Security Technologies |
| Sony and Epsilon: Lessons for Data Security Legislation | June 2, 2011 | Energy and Commerce | Commerce, Manufacturing, and Trade |
| Protecting the Electric Grid: the Grid Reliability and Infrastructure Defense Act | May 31, 2011 | Energy and Commerce | |
| Unlocking the SAFETY Act's [Support Anti-terrorism by Fostering Effective Technologies—P.L. 107-296] Potential to Promote Technology and Combat Terrorism | May 26, 2011 | Homeland Security | Cybersecurity, Infrastructure Protection, and Security Technologies |
| Protecting Information in the Digital Age: Federal Cybersecurity Research and Development Efforts | May 25, 2011 | Science, Space, and Technology | Research and Science Education and Technology and Innovation |
| Cybersecurity: Innovative Solutions to Challenging Problems | May 25, 2011 | Judiciary | Intellectual Property, Competition and the Internet |
| Cybersecurity: Assessing the Immediate Threat to the United States | May 25, 2011 | Oversight and Government Reform | National Security, Homeland Defense and Foreign Operations |

| Title | Date | Committee | Subcommittee |
|---|-------------------|------------------------------------|---|
| DHS Cybersecurity Mission: Promoting Innovation and Securing Critical Infrastructure | April 15, 2011 | Homeland Security | Cybersecurity, Infrastructure Protection, and Security Technologies |
| Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology | April 15, 2011 | Foreign Affairs | Oversight and Investigations |
| Budget Hearing—National Protection and Programs Directorate, Cybersecurity and Infrastructure Protection Programs | March 31, 2011 | Appropriations (closed/classified) | Energy and Power |
| Examining the Cyber Threat to Critical Infrastructure and the American Economy | March 16, 2011 | Homeland Security | Cybersecurity, Infrastructure Protection, and Security Technologies |
| 2012 Budget Request from U.S. Cyber Command | March 16, 2011 | Armed Services | Emerging Threats and Capabilities |
| What Should the Department of Defense’s Role in Cyber Be? | February 11, 2011 | Armed Services | Emerging Threats and Capabilities |
| Preventing Chemical Terrorism: Building a Foundation of Security at Our Nation’s Chemical Facilities | February 11, 2011 | Homeland Security | Cybersecurity, Infrastructure Protection, and Security Technologies |
| World Wide Threats | February 10, 2011 | Permanent Select Intelligence | |

Source: Compiled by CRS.

Table 22. 112th Congress, House Hearings, by Committee

| Committee | Subcommittee | Title | Date |
|------------------------------------|-----------------------------------|---|-------------------|
| Appropriations (closed/classified) | | Budget Hearing—National Protection and Programs Directorate, Cybersecurity and Infrastructure Protection Programs | March 31, 2011 |
| Armed Services | Emerging Threats and Capabilities | Digital Warriors: Improving Military Capabilities for Cyber Operations | July 25, 2012 |
| Armed Services | Emerging Threats and Capabilities | Fiscal 2013 Defense Authorization: IT and Cyber Operations | March 20, 2012 |
| Armed Services | Emerging Threats and Capabilities | Institutionalizing Irregular Warfare Capabilities | November 3, 2011 |
| Armed Services | Emerging Threats and Capabilities | 2012 Budget Request for U.S. Cyber Command | March 16, 2011 |
| Armed Services | Emerging Threats and Capabilities | What Should the Department of Defense’s Role in Cyber Be? | February 11, 2011 |
| Energy and Commerce | Communications and Technology | Cybersecurity: Threats to Communications Networks and Public-Sector Responses | March 28, 2012 |
| Energy and Commerce | Oversight and Investigations | IT Supply Chain Security: Review of Government and Industry Efforts | March 27, 2012 |
| Energy and Commerce | Communications and Technology | Cybersecurity: The Pivotal Role of Communications Networks | March 7, 2012 |

| Committee | Subcommittee | Title | Date |
|---------------------|---|---|--------------------|
| Energy and Commerce | Oversight and Investigations | Critical Infrastructure Cybersecurity: Assessments of Smart Grid Security | February 28, 2012 |
| Energy and Commerce | Oversight and Investigations | Cybersecurity: An Overview of Risks to Critical Infrastructure | July 26, 2011 |
| Energy and Commerce | Commerce, Manufacturing, and Trade | Sony and Epsilon: Lessons for Data Security Legislation | June 2, 2011 |
| Energy and Commerce | Energy and Power | Protecting the Electric Grid: the Grid Reliability and Infrastructure Defense Act | May 31, 2011 |
| Financial Services | Capital Markets and Government Sponsored Enterprises | Cyber Threats to Capital Markets and Corporate Account | June 1, 2012 |
| Financial Services | Financial Institutions and Consumer Credit | Cybersecurity: Threats to the Financial Sector | September 14, 2011 |
| Financial Services | Field hearing in Hoover, AL | Field Hearing: "Hacked Off: Helping Law Enforcement Protect Private Financial Information" | June 29, 2011 |
| Foreign Affairs | Oversight and Investigations | Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology | April 15, 2011 |
| Homeland Security | Emergency Preparedness, Response, and Communications | Resilient Communications: Current Challenges and Future Advancement | September 12, 2012 |
| Homeland Security | Cybersecurity, Infrastructure Protection, and Security Technologies and Counterterrorism and Intelligence | Iranian Cyber Threat to U.S. Homeland | April 26, 2012 |
| Homeland Security | Oversight, Investigations and Management | America is Under Cyber Attack: Why Urgent Action is Needed | April 24, 2012 |
| Homeland Security | Cybersecurity, Infrastructure Protection, and Security Technologies | The DHS and DOE National Labs: Finding Efficiencies and Optimizing Outputs in Homeland Security Research and Development | April 19, 2012 |
| Homeland Security | Cybersecurity, Infrastructure Protection, and Security Technologies | Hearing on Draft Legislative Proposal on Cybersecurity | December 6, 2011 |
| Homeland Security | Cybersecurity, Infrastructure Protection, and Security Technologies | Cloud Computing: What are the Security Implications? | October 6, 2011 |
| Homeland Security | Cybersecurity, Infrastructure Protection, and Security Technologies | Examining the Homeland Security Impact of the Obama Administration's Cybersecurity Proposal | June 24, 2011 |
| Homeland Security | | Unlocking the SAFETY Act's [Support Anti-terrorism by Fostering Effective Technologies—P.L. 107-296] Potential to Promote Technology and Combat Terrorism | May 26, 2011 |
| Homeland Security | Cybersecurity, Infrastructure Protection, and Security Technologies | DHS Cybersecurity Mission: Promoting Innovation and Securing Critical Infrastructure | April 15, 2011 |

| Committee | Subcommittee | Title | Date |
|---------------------------------|--|--|--------------------|
| Homeland Security | Cybersecurity, Infrastructure Protection, and Security Technologies | Examining the Cyber Threat to Critical Infrastructure and the American Economy | March 16, 2011 |
| Homeland Security | Cybersecurity, Infrastructure Protection, and Security Technologies | Preventing Chemical Terrorism: Building a Foundation of Security at Our Nation's Chemical Facilities | February 11, 2011 |
| Judiciary | Intellectual Property, Competition, and the Internet | Cloud Computing: An Overview of the Technology and the Issues facing American Innovators | July 25, 2012 |
| Judiciary | | Combating Online Piracy (H.R. 3261, Stop the Online Piracy Act) | November 16, 2011 |
| Judiciary | Crime, Terrorism and Homeland Security | Cybersecurity: Protecting America's New Frontier | November 15, 2011 |
| Judiciary | Intellectual Property, Competition, and the Internet | Cybersecurity: Innovative Solutions to Challenging Problems | May 25, 2011 |
| Oversight and Government Reform | | Cybersecurity: Assessing the Nation's Ability to Address the Growing Cyber Threat | July 7, 2011 |
| Oversight and Government Reform | Subcommittee on National Security, Homeland Defense and Foreign Operations | Cybersecurity: Assessing the Immediate Threat to the United States | May 25, 2011 |
| Permanent Select Intelligence | | Investigation of the Security Threat Posed by Chinese Telecommunications Companies Huawei and ZTE | September 13, 2012 |
| Permanent Select Intelligence | | Cyber Threats and Ongoing Efforts to Protect the Nation | October 4, 2011 |
| Permanent Select Intelligence | | World Wide Threats | February 10, 2011 |
| Science, Space, and Technology | Investigations and Oversight | NASA Cybersecurity: An Examination of the Agency's Information Security | February 29, 2012 |
| Science, Space, and Technology | Technology and Innovation | The Cloud Computing Outlook | September 21, 2011 |
| Science, Space, and Technology | Research and Science Education and Technology and Innovation | Protecting Information in the Digital Age: Federal Cybersecurity Research and Development Efforts | May 25, 2011 |
| Small Business | Healthcare and Technology | Cyber Security: Protecting Your Small Business | November 30, 2011 |

Source: Compiled by CRS.

Table 23. 112th Congress, House Markups, by Date

| Title | Date | Committee | Subcommittee |
|---|------------------|--------------------------------|---|
| Consideration and Markup of H.R. 3674 | February 1, 2012 | Homeland Security | Cybersecurity, Infrastructure Protection, and Security Technologies |
| Markup: Draft Bill: Cyber Intelligence Sharing and Protection Act of 2011 | December 1, 2011 | Permanent Select Intelligence | |
| Markup on H.R. 2096, Cybersecurity Enhancement Act of 2011 | July 21, 2011 | Science, Space, and Technology | |
| Discussion Draft of H.R. 2577, a bill to require greater protection for sensitive consumer data and timely notification in case of breach | June 15, 2011 | Energy and Commerce | Commerce, Manufacturing, and Trade |

Source: Compiled by CRS.

Table 24. 112th Congress, Senate Hearings, by Date

| Title | Date | Committee | Subcommittee |
|---|-------------------|--|--|
| State of Federal Privacy and Data Security Law: Lagging Behind the Times? | July 31, 2012 | Homeland Security and Governmental Affairs | Oversight of Government Management, the Federal Workforce and the District of Columbia |
| Cyber Security and the Grid | July 17, 2012 | Energy and Natural Resources Committee | |
| U.S. Strategic Command and U.S. Cyber Command | March 27, 2012 | Armed Services | |
| Cybersecurity Research and Development | March 20, 2012 | Armed Services | Emerging Threats and Capabilities |
| The Freedom of Information Act: Safeguarding Critical Infrastructure Information and the Public's Right to Know | March 13, 2012 | Judiciary | |
| Securing America's Future: The Cybersecurity Act of 2012 | February 16, 2012 | Homeland Security and Governmental Affairs | |
| Cybercrime: Updating the Computer Fraud and Abuse Act to Protect Cyberspace and Combat Emerging Threats | September 7, 2011 | Judiciary | |
| Role of Small Businesses in Strengthening Cybersecurity Efforts in the United States | July 25, 2011 | Small Business and Entrepreneurship | |
| Privacy and Data Security: Protecting Consumers in the Modern World | June 29, 2011 | Commerce, Science, and Transportation | |
| Cybersecurity: Evaluating the Administration's Proposals | June 21, 2011 | Judiciary | Crime and Terrorism |

| Title | Date | Committee | Subcommittee |
|---|-------------------|--|-----------------------------------|
| Cybersecurity and Data Protection in the Financial Sector | June 21, 2011 | Banking, Housing, and Urban Affairs | |
| Protecting Cyberspace: Assessing the White House Proposal | May 23, 2011 | Homeland Security and Governmental Affairs | |
| Cybersecurity of the Bulk-Power System and Electric Infrastructure and for Other Purposes | May 5, 2011 | Energy and Natural Resources | |
| Health and Status of the Defense Industrial Base | May 3, 2011 | Armed Services | Emerging Threats and Capabilities |
| Cyber Security: Responding to the Threat of Cyber Crime and Terrorism | April 12, 2011 | Judiciary | Crime and Terrorism |
| Oversight of the Federal Bureau of Investigation | March 30, 2011 | Judiciary | |
| Cybersecurity and Critical Electric Infrastructure ^a (closed hearing) | March 15, 2011 | Energy and Natural Resources | |
| Information Sharing in the Era of WikiLeaks: Balancing Security and Collaboration | March 10, 2011 | Homeland Security and Governmental Affairs | |
| Homeland Security Department's Budget Submission for Fiscal Year 2012 | February 17, 2011 | Homeland Security and Governmental Affairs | |

Source: Compiled by CRS.

a. The March 15, 2011, hearing before the Committee on Energy and Natural Resources was closed.

Table 25. 112th Congress, Senate Hearings, by Committee

| Committee | Subcommittee | Title | Date |
|---------------------------------------|-----------------------------------|---|----------------|
| Armed Services | Emerging Threats and Capabilities | Cybersecurity Research and Development | March 20, 2012 |
| Armed Services | | U.S. Strategic Command and U.S. Cyber Command | March 27, 2012 |
| Armed Services | Emerging Threats and Capabilities | Health and Status of the Defense Industrial Base | May 3, 2011 |
| Banking, Housing, and Urban Affairs | | Cybersecurity and Data Protection in the Financial Sector | June 21, 2011 |
| Commerce, Science, and Transportation | | Privacy and Data Security: Protecting Consumers in the Modern World | June 29, 2011 |
| Energy and Natural Resources | | Cybersecurity and the Grid | July 17, 2012 |

| Committee | Subcommittee | Title | Date |
|--|--|---|-------------------|
| Energy and Natural Resources | | Cybersecurity of the Bulk-Power System and Electric Infrastructure and For Other Purposes | May 5, 2011 |
| Energy and Natural Resources (closed) ^a | | Cybersecurity and Critical Electric Infrastructure | March 15, 2011 |
| Homeland Security and Governmental Affairs | Oversight of Government Management, the Federal Workforce and the District of Columbia | State of Federal Privacy and Data Security Law: Lagging Behind the Times? | July 31, 2012 |
| Homeland Security and Governmental Affairs | | Securing America's Future: The Cybersecurity Act of 2012 | February 16, 2012 |
| Homeland Security and Governmental Affairs | | Protecting Cyberspace: Assessing the White House Proposal | May 23, 2011 |
| Homeland Security and Governmental Affairs | | Information Sharing in the Era of WikiLeaks: Balancing Security and Collaboration | March 10, 2011 |
| Homeland Security and Governmental Affairs | | Homeland Security Department's Budget Submission for Fiscal Year 2012 | February 17, 2011 |
| Judiciary | | The Freedom of Information Act: Safeguarding Critical Infrastructure Information and the Public's Right to Know | March 13, 2012 |
| Judiciary | | Cybercrime: Updating the Computer Fraud and Abuse Act to Protect Cyberspace and Combat Emerging Threats | September 7, 2011 |
| Judiciary | Crime and Terrorism | Cybersecurity: Evaluating the Administration's Proposals | June 21, 2011 |
| Judiciary | Crime and Terrorism | Cyber Security: Responding to the Threat of Cyber Crime and Terrorism | April 12, 2011 |
| Judiciary | | Oversight of the Federal Bureau of Investigation | March 30, 2011 |
| Small Business and Entrepreneurship | | Role of Small Business in Strengthening Cybersecurity Efforts in the United States | July 25, 2011 |

Source: Compiled by CRS.

a. The March 15, 2011, hearing before the Committee on Energy and Natural Resources was closed.

Table 26. 112th Congress, Congressional Committee Investigative Reports

| Title | Committee | Date | Pages | Notes |
|--|---|-----------------|--------------|--|
| Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE | House Permanent Select Committee on Intelligence | October 8, 2012 | 60 | The committee initiated this investigation in November 2011 to inquire into the counterintelligence and security threat posed by Chinese telecommunications companies doing business in the United States. |
| Federal Support for and Involvement in State and Local Fusion Centers | U. S. Senate Permanent Subcommittee on Investigations | October 3, 2012 | 141 | A two-year bipartisan investigation found that U.S. Department of Homeland Security efforts to engage state and local intelligence “fusion centers” has not yielded significant useful information to support federal counterterrorism intelligence efforts. In Section VI, “Fusion Centers Have Been Unable to Meaningfully Contribute to Federal Counterterrorism Efforts,” Part G, “Fusion Centers May Have Hindered, Not Aided, Federal Counterterrorism Efforts,” the report discusses the Russian “Cyberattack” in Illinois. |

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.
- CRS Report 98-611, *Presidential Directives: Background and Overview*, by Elaine Halchin.

Table 27 provides a list of executive orders and presidential directives pertaining to cybersecurity. (Titles are linked to documents.)

Table 27. Executive Orders and Presidential Directives
(by date of issuance)

| Title | Date | Source | Notes |
|---|-------------------|-------------|---|
| 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 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- |

| Title | Date | Source | Notes |
|--|-------------------|-------------|--|
| E.O. 13636, Improving Critical Infrastructure Cybersecurity | February 12, 2013 | White House | <p>enabled cards at retail terminals.</p> <p>E.O. 13636 addresses cybersecurity threats to critical infrastructure (CI) by, among other things,</p> <ul style="list-style-type: none"> • expanding to other CI sectors an existing DHS program for information sharing and collaboration between the 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 | <p>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.</p> |
| E. O. 13618, Assignment of National Security and Emergency Preparedness Communications Functions | July 6, 2012 | White House | <p>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,</p> |

| Title | Date | Source | Notes |
|--|-------------------|-------------|--|
| E.O. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible | October 7, 2011 | White House | <p>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 assigning specific responsibilities to federal government entities.</p> <p>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.</p> |
| E.O. 13407, Public Alert and Warning System | June 26, 2006 | White House | <p>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.</p> |
| HSPD-7, Homeland Security Presidential Directive No. 7: Critical Infrastructure Identification, Prioritization, and Protection | December 17, 2003 | White House | <p>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.</p> |
| 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 | <p>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, that own or lease telecommunication assets identified as part of the National Communication System, or which bear policy, regulatory, or enforcement</p> |

| Title | Date | Source | Notes |
|---|-----------------|----------------|--|
| Presidential Decision Directive/NSC-63 | May 22, 1998 | White House | responsibilities of importance to national security and emergency preparedness telecommunications. 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 currently being debated in the 114th Congress.