Congressional Research Service
Informing the legislative debate since 1914

# Cybersecurity: Selected Issues for the 115th Congress

**(name redacted), Coordinator**
Analyst in Cybersecurity Policy

March 9, 2018

**Congressional Research Service**
7-....
www.crs.gov
R45127

**CRS REPORT**
Prepared for Members and
Committees of Congress

# Summary

Cybersecurity has been gaining attention as a national issue for the past decade. During this time, the country has witnessed cyber incidents affecting both public and private sector systems and data. These incidents have included attacks in which data was stolen, altered, or access to it was disrupted or denied. The frequency of these attacks, and their effects on the U.S. economy, national security, and people's lives have driven cybersecurity issues to the forefront of congressional policy conversations. This report provides an overview of selected cybersecurity concepts and a discussion of cybersecurity issues that are likely to be of interest during the 115th Congress.

From a policymaking standpoint, cybersecurity includes the security of the devices, infrastructure, data, and users that make up cyberspace. The elements of ensuring cybersecurity involve policies spanning a range of fields, including education, workforce management, investment, entrepreneurship, and research and development. Software development, law enforcement, intelligence, incident response, and national defense are involved in the response when something goes awry in cyberspace.

To help secure and respond to incidents in cyberspace federal departments and agencies carry out their authorized responsibilities, run programs, and work with the private sector. While every federal agency has a role in protecting its own data and systems, certain agencies have significant responsibilities with regard to national cybersecurity. The Department of Defense supports domestic efforts on cybersecurity with its capabilities and capacity, and deploys military assets to protect American critical infrastructure from a cyberattack when directed to do so. The Department of Homeland Security secures federal networks, coordinates critical infrastructure protection efforts, responds to cyber threats, investigates cybercrimes, funds cybersecurity research and development, and promotes cybersecurity education and awareness. The Department of Justice investigates and prosecutes a variety of cyber threats, which range from computer hacking and intellectual property rights violations to fraud, child exploitation, and identity theft.

Congress passed five laws related to cybersecurity during the 113th Congress and an additional law during the 114th Congress. Congress also held 119 hearings on cybersecurity-related issues during the 114th Congress. The White House issued presidential actions on cybersecurity related to critical infrastructure cybersecurity, information sharing, and sanctions in retaliation for malicious cyber activities.

Cybersecurity policy has continued to hold congressional interest during the 115th Congress. Recent congressional hearings have examined several cybersecurity issues, including data breaches, critical infrastructure protection, education and training, and the security of federal information technology. Other issues discussed during the 114th Congress continue to hold stakeholder interest, including debates concerning government access to encrypted data.

This report covers a variety of topics related to cybersecurity in order to provide context and a framework for further discussion on selected policy areas. These topics include cybersecurity incidents, major federal agency roles and responsibilities, recent policy actions by Congress and the White House, and descriptions of policy issues that may be of interest in the 115th Congress.

# Contents

Introduction ..... 1
Cybersecurity Overview ..... 1
Attacks ..... 2
Terrorist Use of Cyberspace ..... 4
Selected Federal Roles and Responsibilities ..... 6
Department of Defense ..... 6
Department of Homeland Security (DHS) ..... 7
Department of Justice ..... 8
Selected Policy Issues ..... 9
Critical Infrastructure ..... 9
Data Breaches and Data Security ..... 10
Education and Training ..... 11
Encryption ..... 12
Encryption as a Cybersecurity Tool ..... 12
Encryption and Law Enforcement Investigations ..... 13
Information Sharing ..... 14
Insurance ..... 15
International Issues ..... 16
Trade ..... 16
Internet of Things Security ..... 18
Oversight of Federal Agency Information Technology Security ..... 18
Response to Cybersecurity Incidents ..... 19
Previous Policy Action ..... 21
Recent Legislative Action ..... 21
Recent Executive Action ..... 23
Selected Hearings ..... 28

## Tables

Table 1. 114th Congress Cybersecurity Public Laws ..... 22
Table 2. 113th Congress Cybersecurity Public Laws ..... 22
Table 3. Executive Orders and Presidential Directives ..... 24

## Contacts

Author Contact Information ..... 29

# Introduction

Cybersecurity issues are gaining national prominence, generating extensive media coverage, and affecting constituents nationwide. The frequency of cybersecurity incidents and their effects on the U.S. economy and national security have elevated congressional interest in cybersecurity issues.

This report provides an overview of cybersecurity concepts, the role of selected federal agencies in addressing cybersecurity threats, and a discussion of cybersecurity issues that may be of interest to Congress, including the following:

- protecting critical infrastructure;
- data breaches and data security;
- education and training;
- encryption;
- information sharing;
- insurance;
- international issues;
- the Internet of Things;
- oversight of federal agency information technology; and
- incident response.

This is a coordinated report with multiple authors, who are listed with their contact information in footnotes at the beginning of the section(s) they authored as well as at the end of the report.

# Cybersecurity Overview

Essentially, *cybersecurity* is the security of cyberspace. Cyberspace can be considered to be the services that use the infrastructure of the internet to deliver information to users through their devices.

In practical terms, a person becomes a *user* of cyberspace when they use *devices* to access *services*, such as access to online banking, shopping, email, streaming video, social media, or the news. Those services do not exist independently, but rather rely on a common *infrastructure* of servers and switches; cable and wireless spectrum; and routers to ensure that a user has access to the service. That same infrastructure is used by other services too, such as utilities and shipping companies to ensure that products arrive as intended—or by businesses to develop new products more efficiently and to manage their operations.

Therefore, for policymaking purposes, each of those elements (i.e., the services, infrastructure, devices, and user) are parts of cyberspace. The internet is a publicly accessible network within cyberspace, but cyberspace also contains private networks used by businesses and other users to help obtain greater confidentiality of their communications.

The United States government does not have a single definition of cybersecurity. However, the *Report on Securing and Growing the Digital Economy* by the U.S. Commission on Enhancing National Cybersecurity offers the following definition of cybersecurity:

> The process of protecting information and information systems by preventing, detecting, and responding to unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.[1]

The concepts of "confidentiality," "integrity," and "availability" are defined in U.S. Code as part of the "information security" triad.[2] "Confidentiality" refers to the attribute that data are known only to authorized parties and not made available or disclosed to unauthorized parties. "Integrity" refers to the attribute that data have not been altered or destroyed in an unauthorized manner. "Availability" refers to the attribute that data are available for access by an authorized party when they choose. These terms apply to the data stored, processed, and transmitted by information technology (IT) systems, but also to the IT systems themselves. A fourth term for information security is gaining prominence in discussions on cybersecurity: "authentication," or the ability to confirm that parties using a system and accessing data are who they claim to be and have legitimate access to that data and system.

Elements to ensure cybersecurity involve policies spanning a range of fields, including education, workforce management, investment, entrepreneurship, and research and development. Software development, law enforcement, intelligence, incident response, and national defense may be involved in the response when something goes awry in cyberspace.

## Attacks[3]

Attacks against data and systems are possible because IT systems are large and complex. Through their size and complexity, vulnerabilities exist which can be exploited. Consider a single smartphone. That smartphone may have been designed by a company in the United States, but built abroad by another company using material from yet another country. It runs on software built by one company, but modern operating systems borrow code from other companies. All that complexity exists before the device gets to the user. Once the user has the device it will likely be connected to a variety of networks such as a home wireless network, a corporate network, or a cellular network—each with its own infrastructure, and which share common internet infrastructure. The interconnected nature of all these services necessary to ensure the smartphone works further contributes to the breadth and complexity of the IT system, which is where vulnerabilities may lie.

There are many ways to attack an IT system. Some of the commonly seen attacks are described below.

- *Denial of Service (DOS):* A DOS attack compromises the availability of data. In this attack, a network or website with information is overloaded with information, monopolizing the system's bandwidth and preventing legitimate users from getting their requests for service through, resulting in the user experiencing the system as unavailable. A DOS attack itself does not constitute an intrusion into the network or website, but it may be combined with other forms of attack to compromise the confidentiality or integrity of the network or its data. A distributed denial of service attack (DDOS) occurs when many

[1] U.S. Commission on Enhancing National Cybersecurity, "Report on Security and Growing the Digital Economy," December 1, 2016, at https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf.

[2] These definitions are at 44 U.S.C. §3552.

[3] Section written by (name redacted), Analyst in Cybersecurity Policy ([redacted]@crs.loc.gov, 7-....).

disparate devices are used in the attack, as is the case when a botnet is employed for a DOS attack.[4] DOS attacks are illegal under the Computer Fraud and Abuse Act.[5]

- *Ransomware:* Ransomware is a specific form of malware (or malicious computer software) that installs itself on a user's computer and encrypts the user's hard drive so that the user cannot access her own files. The attacker then typically provides instructions to the victim to provide payment, payable via a cryptocurrency, usually Bitcoin.[6] Upon receipt of payment, the attacker promises to provide the encryption key to the victim so that the victim may decrypt the attacked hard drive and access her files. However, the payment does not constitute a guarantee that the victim will receive the encryption key. Ransomware is illegal under the Computer Fraud and Abuse Act.[7]
- *Data Breaches:* A data breach is a form of an attack against a computer system, but not all attacks are breaches. A data breach has the potential to compromise the confidentiality, integrity, and availability of an information system, and at a minimum violates the confidentiality of that system by exposing it to an unintended third party. In this sense, a breach is "an incident that results in the disclosure or potential exposure of data."[8] Disclosure is different from exposure: disclosure entails a confirmation that an unauthorized third party read the data, while exposure means that a third party merely has the opportunity to do so. Data breaches are illegal under the Computer Fraud and Abuse Act.[9]
- *Attacks against data and system integrity:* The previous three types of attack attempt to disrupt the availability and confidentiality of data on a system. Integrity attacks attempt to disrupt trust in the data or the system itself. In an integrity attack on data, a file is accessed without authorization and altered to reflect some information other than what authorized users intend. An example of an integrity attack is someone accessing a system without authorization to change information in a file. Additionally, an entire system may have its integrity compromised by having unauthorized commands executed on that system. An example might be malware that tells a computer to perform an operation without the authorized user's knowledge, while giving the authorized user feedback that the computer is operating as normal.[10] These types of attack are illegal under the Computer Fraud and Abuse Act.[11]

[4] A botnet is a network of computers or other internet-connected devices that an attacker has infected with malicious software (malware) that grants him control and use of the resources of the devices (i.e., the processing power, network access, microphone and camera, etc.). A single device in that network is called a "bot."

[5] 18 U.S.C. §1030(a)(5)(A).

[6] CRS Report R43339, *Bitcoin: Questions, Answers, and Analysis of Legal Issues*, by (name redacted) and (name redacted) .

[7] 18 U.S.C. §1030(a)(7).

[8] Verizon Enterprise Solutions, *2014 Data Breach Investigations Report*, April 2014, p. 8, at http://www.verizonenterprise.com/resources/reports/rp_Verizon-DBIR-2014_en_xg.pdf.

[9] 18 U.S.C. §1030.

[10] Stuxnet was an attack against the integrity of a system. For more information, see CRS Report R41524, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*, by (name redacted), (name redacted), and (name redacted) .

[11] 18 U.S.C. §1030.

The data and information technology systems of any entity, regardless of size, may be the targets of a cyber incident. Attackers may develop tools and techniques for a specific target and then reuse that tool or technique multiple times to attack other targets. Targets can include countries, multinational corporations, the federal government, large businesses, critical infrastructure entities, state and local governments, nonprofit organizations, academia, small businesses, and individuals. Additionally, attackers may have a particular target in mind, but penetrate their target by going through another entity. As such, partner entities, whether companies or other entities, may face an unforeseen risk of cyberattack based on their relationship to a targeted entity.[12]

## Terrorist Use of Cyberspace[13]

Terrorist use of cyberspace is growing both in terms of reliance for supporting organizational activities and for gaining expertise to achieve operational goals. While no publicly accessible report has been published regarding a confirmed cyberterrorist attack against the United States, the possibility of one exists. Tighter physical and border security may encourage terrorists and extremists to try to use novel weapons to attack the United States. Persistent internet and computer security vulnerabilities, which have been widely publicized, may gradually encourage terrorists to continue to enhance their computer skills, or develop alliances with criminal organizations and consider attempting a cyberattack against U.S. critical infrastructure, facilities, and activities that support global security interests.

Cyberterrorists are state-sponsored and nonstate actors who engage in cyberattacks to pursue their objectives. Transnational terrorist organizations have used the internet as a tool for planning attacks, for radicalization and recruitment, as a method of propaganda distribution, as a means of communication, and for disruptive purposes.

The vulnerability of critical life-sustaining control systems being accessed and destroyed via the internet has been demonstrated. In 2009, the Department of Homeland Security (DHS) conducted an experiment that revealed some of the vulnerabilities to the nation's control systems that manage electric power generators and grids. The experiment, known as the Aurora Project, entailed a computer-based attack on a power generator's control system that caused operations to cease and the equipment to be destroyed. Cyberterrorists may be seeking a destructive capability to exploit these types of vulnerabilities in critical infrastructure but progress toward this goal is uncertain. As noted in March 2017 by then-Federal Bureau of Investigation (FBI) Director James Comey, "terrorists have not yet figured out how to use the Internet as an instrument of destruction ... eventually these knuckleheads will."[14]

There is no consensus definition of what constitutes cyberterrorism. The closest in law is found in the USA PATRIOT Act statute governing "acts of terrorism transcending national boundaries," which includes in its definition of a "federal crime of terrorism" some violations of the Computer Fraud and Abuse Act (CFAA).[15] One portion of the CFAA referenced by the USA PATRIOT Act makes it illegal for an entity to do the following:

[12] For a case example of this type of breach, see CRS Report R43496, *The Target and Other Financial Data Breaches: Frequently Asked Questions*, by (name redacted) and (name redacted)

[13] Section written by John Rollins, Specialist in Terrorism and National Security ([redacted]@crs.loc.gov, ....).

[14] James Comey, "Using Intelligence to Disrupt National Security Threats," remarks as delivered, March 23, 2017, at https://www.fbi.gov/news/speeches/using-intelligence-to-disrupt-national-security-threats.

[15] 18 U.S.C. §2332b(g)(5).; 18 U.S.C. §1030.

> knowingly [access] a computer without authorization or exceeding authorized access, and by means of such conduct … [obtain] information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data … with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation….[16]

The other CFAA provision referenced in the USA PATRIOT Act prohibits transmitting "a program, information, code, or command" to certain computers (including all government computers and most private ones) and thereby intentionally causing unauthorized damage.[17]

Some cyberwarfare experts define cyberterrorism as "the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives."[18] The USA PATRIOT Act's definition of "federal crime of terrorism," with its inclusion of certain CFAA violations as predicate acts, has some similarities to this definition, though the statute is limited to only those attacks with political objectives.[19] However, these provisions are also criminal statutes and generally refer to individuals or organizations rather than state actors. Naval Post Graduate School defense analyst Dorothy Denning's definition of cyberterrorism focuses on the distinction between destructive and disruptive action. Terrorism generates fear comparable to that of physical attack, and is not just a "costly nuisance." Though a DDOS attack itself does not yield this kind of fear or destruction, the broader issue is the potential for second- or third-order effects. For example, if telecommunications and emergency services were completely dismantled in a time of crisis, the effects of that sort of infrastructure attack could potentially be catastrophic. If an attack on the emergency services system were to coincide with a planned real-world event, then cyberterror may be an appropriate metaphor. However, in this case, the emergency service system itself would most likely not be a target, but rather the result of collateral damage to a vulnerable telecommunications network.

There are a number of reasons that may explain why the term "cyberterrorism" has not been statutorily defined, including the difficulty in identifying applicable activities, whether articulating clear red lines would demand a response for lower-level incidents, and retaining strategic maneuverability so as not to bind future U.S. activities in cyberspace.

[16] 18 U.S.C. §1030(a)(1).

[17] 18 U.S.C. § 1030(a)(5)(A).

[18] Kevin Coleman, "Cyber Terrorism," *Directions Magazine*, October 11, 2003, at https://www.directionsmag.com/article/3655.

[19] 18 U.S.C. §2332b(g)(5)(A) (requiring that the offense be "calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct").

# Selected Federal Roles and Responsibilities

## Department of Defense[20]

The Department of Defense (DOD) is responsible for defending the nation and supporting the Department of Homeland Security's (DHS's) coordination of efforts for cyber defense, for protecting the defense industrial base (DIB), and for securing the DOD information networks (DODIN). Both DOD and DHS are charged with defending the U.S. homeland and U.S. national interests against cyberattacks of significant consequence. Military cyber assets may be deployed in the event of a major cyberattack on U.S. critical infrastructure only when directed to do so.[21]

DOD's cyberspace operations are composed of the military, intelligence, and ordinary business operations of the DOD in and through cyberspace. Military cyberspace operations use cyberspace capabilities to create effects that support operations across the physical domains and cyberspace. Cyberspace operations differ from information operations (IO), which may use cyberspace as a medium, but may also employ capabilities from the physical domains.[22]

Cyberspace operations are categorized into the following.

- **Offensive Cyberspace Operations**, intended to project power by the application of force in and through cyberspace. These operations are authorized like operations in the physical domains.
- **Defensive Cyberspace Operations**, to defend DOD or other friendly cyberspace. These are both passive and active defense operations and are conducted inside and outside of DODIN.
- **DODIN Operations**, to design, build, configure, secure, operate, maintain, and sustain DOD communications systems and networks across the entire DODIN.

In 2012, President Obama directed DOD to organize and plan to defend the nation against cyberattacks of significant consequence, in concert with other U.S. government agencies. The resulting DOD Cyber Strategy focuses on three primary cyber missions:[23]

- Defend DOD networks, systems, and information.
- Defend the U.S. homeland and U.S. national interests against cyberattacks of significant consequence.
- Provide cyber support to military operational and contingency plans.

---

[20] Section written by (name redacted), Specialist in Nati onal Security Policy Cyber and Information Operations ([redacted]@crs.loc.gov, 7-....).

For more information on the DOD role in security cyberspace, see CRS Report R43955, *Cyberwarfare and Cyberterrorism: In Brief*, by (name redacted) and (name redacted) ; and CRS In Focus IF10537, *Defense Primer: Cyberspace Operations*, by (name redacted) .

[21] Section 954 of the National Defense Authorization Act for Fiscal Year 2012 affirms that " ... the Department of Defense has the capability, and upon direction by the President may conduct offensive operations in cyberspace to defend our Nation, Allies and interests, subject to—(1) the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict and (2) the War Powers Resolution (50 U.S.C. §1541 et seq.)."

[22] See Joint Publication 3-13, *Information Operations*, and Joint Publication 3-12, *Cyberspace Operations*, both available at http://www.dtic.mil.

[23] Available at https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

Guided by this strategy document, DOD began to build a Cyber Mission Force (CMF) in 2012 to carry out DOD's cyber missions. The CMF consists of 133 teams that are organized to meet DOD's three cyber missions. Specifically, CMF teams support the following mission sets though their respective assignments.

- **Cyber National Mission Force** teams defend the nation by seeing adversary activity, blocking attacks, and maneuvering in cyberspace to defeat them.
- **Cyber Combat Mission Force** teams conduct military cyber operations in support of combatant commands.
- **Cyber Protection Force** teams defend the DOD information networks, protect priority missions, and prepare cyber forces for combat.
- **Cyber Support Teams** provide analytic and planning support to National Mission and Combat Mission teams.

Cyber Mission Force teams reached initial operating capability in October 2016. Currently comprising around 5,000 individuals, the cyber mission force is expected to grow to 6,200 by the end of 2018. Organizationally, the Cyber Mission Force is an entity of the United States Cyber Command.

### *United States Cyber Command*

In response to the growing cyber threat, in 2009 the Secretary of Defense directed the establishment of a new military command devoted to cyber activities. The United States Cyber Command (USCYBERCOM) is currently a subunified command, under the U.S. Strategic Command, whose stated mission is to "direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries."[24] Previously existing components, such as the Joint Task Force for Global Network Operations (JTF-GNO) and the Joint Functional Component Command for Network Warfare (JFCC-NW), were absorbed by USCYBERCOM and reorganized to provide centralized planning for cyberspace operations. USCYBERCOM is commanded by a four-star general, who is also the director of the National Security Agency (NSA) and chief of the Central Security Service (CSS). The commander manages day-to-day global cyberspace operations and leads defense and protection of DODIN. Each of the military services provides support to USCYBERCOM.

## Department of Homeland Security (DHS)[25]

DHS serves a variety of roles for ensuring cybersecurity, both in the federal government and the private sector. DHS secures federal networks, coordinates critical infrastructure protection efforts, responds to cyber threats, investigates cybercrimes, funds cybersecurity research and development, and promotes cybersecurity education and awareness. In order to accomplish these roles, DHS collects information on cybersecurity threats and shares that information across the

[24] U.S. Strategic Command, "U.S. Cyber Command (USCYBERCOM)," http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/. Section 923 of S. 2943, The National Defense Authorization Act for Fiscal Year 2017, authorized DOD to establish USCYBERCOM as a full unified combatant command.

[25] Section written by (name redacted), Analyst in Cybersecurity Policy ([redacted]@crs.loc.gov, 7-....).

federal government and with the private sector so others may be able to better protect themselves.[26]

In working to secure federal government networks, DHS deploys tools at the gateway between the internet and agency networks to identify and stop known threats before they are able to access the agencies.[27] DHS also deploys tools on agency networks to continuously identify risks and help to prioritize risk mitigation.[28] Working with all federal agencies, DHS also assists in the implementation of and adherence to the Federal Information Security Management Act (FISMA, P.L. 107-347, as amended), which, among other provisions, requires the head of each federal agency to take responsibility for managing risks to information security.[29]

Pursuant to Presidential Policy Directive 41 (PPD-41) and the National Cyber Incident Response Plan (NCIRP), DHS serves as the federal lead for asset response activities. Asset response activities are those which provide technical assistance to victim entities. The assistance may be for mitigating vulnerabilities, reducing the impacts cyber incidents may cause, identifying other entities that may have been impacted by an incident, assessing risks related to an incident, and coordinating the response delivered by federal agencies to victim entities.

DHS's agencies also carry out other cybersecurity responsibilities. The Science and Technology Directorate funds research into cybersecurity threats and invests in mitigating technologies. The U.S. Secret Service and Immigration and Customs Enforcement have authorities to investigate crimes targeting network infrastructure and crimes committed through information and communications technology. DHS serves as the sector-specific agency for 10 of the 16 critical infrastructure sectors, defined by presidential policy, and assists with the cybersecurity of the sectors through threat analysis and the promulgation of mitigating guidance.[30]

## Department of Justice[31]

Combatting malicious actors who exploit cyberspace is a mission that cuts across the Department of Justice's (DOJ's) investigative, intelligence, prosecutorial, and technological components. DOJ is responsible for investigating and prosecuting a range of modern-day cyber threats. It is also responsible for protecting its own critical information systems from cyber intrusions.

The Obama Administration, through PPD-41, outlined how the government responds to significant cyber incidents.[32] It specified that DOJ, through the Federal Bureau of Investigation (FBI) and the National Cyber Investigative Joint Task Force (NCIJTF), is the designated lead on cyber threat response.[33] This involves "conducting appropriate law enforcement and national

[26] For more information see CRS In Focus IF10683, *DHS's Cybersecurity Mission—An Overview*, by (name redacted)

[27] https://www.dhs.gov/einstein.

[28] https://www.dhs.gov/cdm.

[29] 44 U.S.C. §§3551-3558.

[30] The 16 critical infrastructure sectors are available at https://www.dhs.gov/critical-infrastructure-sectors. The sectors are (with their lead agency in parenthesis): chemical (DHS); commercial facilities (DHS); communications (DHS); critical manufacturing (DHS); dams (DHS); defense industrial base (DOD); emergency services (DHS); energy (Energy); financial services (Treasury); food and agriculture (USDA and HHS); healthcare and public health (HHS); information technology (DHS); nuclear reactors, materials, and waste (DHS); transportation systems (DHS and DOT); water and wastewater systems (EPA).

[31] Section written by (name redacted), Specialist in Domestic Security ([redacted]@crs.loc.gov, 7-....).

[32] The White House, *Presidential Policy Directive/PPD-41: United States Cyber Incident Coordination*, Presidential Memoranda, July 26, 2016.

[33] Asset response and intelligence support responsibilities are led by other federal agencies.

security investigative activity at the affected entity's site; collecting evidence and gathering intelligence; providing attribution; linking related incidents; identifying additional affected entities; identifying threat pursuit and disruption opportunities; developing and executing courses of action to mitigate the immediate threat; and facilitating information sharing and operational coordination with asset response."[34]

The FBI pursues cybercrime cases ranging from computer hacking and intellectual property rights violations to child exploitation, fraud, and identity theft. Its top priorities involve combating computer and network intrusions and investigating ransomware.[35] Specifically, the FBI's Cyber Division focuses on "high-level intrusions by state-sponsored hackers and global cyber syndicates, and the most prolific botnets."[36] Further, with respect to prosecuting cyber threat actors, the U.S. Attorneys and the Criminal Division at DOJ are both centrally involved.

# Selected Policy Issues

Below is a list of selected policy issues related to cybersecurity which may be of interest to Congress. These issues are organized alphabetically rather than by theme or priority.

## Critical Infrastructure[37]

Critical infrastructure (CI) is defined in 42 U.S.C. §5195c(e) as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Most U.S. CI is controlled by the private sector. Under the Homeland Security Act of 2002, as amended, DHS coordinates CI security, including cybersecurity.

CI is classified into sectors, most recently 16 under Presidential Policy Directive 21, issued in 2013, with each sector having a designated sector-specific agency. Some agencies have cross-sector responsibilities, such as DHS, DOJ, and the Federal Trade Commission (FTC).[38]

The increasing potential for attacks that might cripple components of CI or otherwise damage the national economy has led to debate about the best ways to protect those sectors. Some, such as the chemical and financial sectors, are subject to federal regulation. The protection of others, such as information technology, relies largely on voluntary efforts. The efficacy of that mix of voluntary and regulatory efforts has long been a source of controversy.

In 2013, Executive Order 13636 established an alternative approach, in which the National Institute of Standards and Technology (NIST) facilitated a public-private effort to develop a cybersecurity framework for CI sectors. Subsequently, Congress authorized the framework process in the Cybersecurity Enhancement Act of 2014 (P.L. 113-274). Issued in 2014, the framework consists of three parts: (1) a core set of activities and outcomes applicable to all the sectors, organized into five functions (identify, protect, detect, respond, and recover); (2) a profile

[34] Ibid.

[35] Federal Bureau of Investigation, *What We Investigate: Cyber*, https://www.fbi.gov/investigate/cyber.

[36] U.S. Congress, Senate Committee on Homeland Security and Governmental Affairs, *Fifteen Years After 9/11: Threats to the Homeland*, 114th Cong., 1st sess., September 27, 2016, S.Hrg. 114-729 (Washington: GPO, 2018), p. 77.

[37] Section written by (name redacted), Senior Specialist in Science and Technology [redacted]@crs.loc.gov, 7-....) .

[38] For a list of the critical infrastructure sectors and corresponding Sector Specific Agency, see https://www.dhs.gov/sector-specific-agencies.

describing an entity's current and target cybersecurity postures; and (3) implementation tiers that characterize the entity's current and intended practices. The DHS C[3] (for Critical infrastructure Cyber Community) program works to facilitate its voluntary adoption, and NIST released a draft update in January 2017.

Before the development of the voluntary cybersecurity framework, debate about the role of federal regulation appeared to be a significant factor impeding the enactment of cybersecurity legislation. However, events associated with the rapidly evolving threat environment continue to draw attention to the question of the appropriate federal role in protecting CI. Attacks such as the ones in 2016 using the Mirai botnet have led to renewed calls by some observers for broad security regulations. Attempts attributed to Russia at interfering with the November 2016 federal election have renewed concerns about the security of the U.S. election infrastructure, leading to the controversial designation by DHS of state and local election systems as a subsector under the government facilities CI sector. The 115th Congress may be faced with the need to address such problems and resolve the controversies, which may be made more urgent by the expected continued evolution of cyberspace and more difficult by the unpredictable nature of emerging threats.[39]

## Data Breaches and Data Security[40]

Congress has sought policy responses to the loss of data by both private sector companies and government agencies, prompted by high-profile breaches such as those at Equifax and the Securities and Exchange Commission (SEC).[41] Breaches frequently occur because of the reliance of modern business practices on IT. An increasingly used catchphrase among industry analysts is that today "all companies are technology companies," or "all companies are data companies." This concept reflects the role that IT and data play in enabling modern business practices that allow companies to compete and thrive in the marketplace. However, this reliance on IT and data also creates risk for corporate leadership to manage. Cybersecurity initiatives seek to control that risk.

Congress has held hearings to examine individual instances of breaches and encourage the breached entities to assist those whose data has been compromised.[42] Additionally, some Members have introduced legislation to address a variety of elements around a data breach, such as standards for securing sensitive data, data breach notification requirements, and the responsibilities affected entities have to those whose data has been breached.[43]

---

[39] For further information contact (name redacted), Analyst in Cybersecurity Policy ([redacted]@crs.loc.gov, 7-....), (name redacted), Specialist in Science and Technology Policy ([redacted]@crs.loc.gov, 7-....), or (name redacted), Senior Specialist in Science and Technology ([redacted]@crs.loc.gov, 7-....). For further reading, see CRS Report R43831, *Cybersecurity Issues and Challenges: In Brief*, by (name redacted); and CRS Report RS20898, *The Help America Vote Act and Election Administration: Overview and Selected Issues for the 2016 Election*, by (name redacted) and (name redacted).

[40] Section written by (name redacted), Analyst in Cybersecurity Policy ([redacted]@crs.loc.gov, 7-....). For more information see CRS Testimony TE10021, *Consumer Data Security and the Credit Bureaus*, by (name redacted)

[41] U.S. Congress, House Committee on Financial Services, *Examining the Equifax Data Breach*, 115th Cong., 1st sess., October 5, 2017. U.S. Congress, Senate Committee on Banking, Housing, and Urban Affairs, *Oversight of the U.S. Securities and Exchange Commission*, 115th Cong., 1st sess., September 26, 2017.

[42] Ibid.

[43] Such bills from the 115th Congress include S. 770, H.R. 3806, and H.R. 3896.

## Education and Training[44]

Increasing awareness of cyberattacks—and the increasing connectedness of cyber and cyber-physical systems—have raised concerns about whether U.S. homes, businesses, and government are prepared to secure themselves in our digitally integrated world. Some of this attention to preparedness has focused on the sufficiency of cybersecurity education, training, and workforce development in the United States. Federal policymakers have grappled with questions about both the quality and the quantity of U.S. postsecondary education graduates with cybersecurity credentials (in general) and the civilian and military workforce needs of the federal government (in particular). Federal programs and policies have also sought to increase awareness of secure computing practices (e.g., do not reuse passwords); and policymakers and agency officials often view educational benefits (e.g., scholarships, training) as a tool for attracting and retaining federal military and civilian cybersecurity workers.

The federal effort in cybersecurity education, training, and workforce development has not been comprehensively inventoried. However, federal funding supports a wide variety of activities in this area. These activities, which are sometimes offered in partnership with multiple federal and nonfederal entities, include cybersecurity awareness (StaySafeOnline.org), summer camps (GenCyber) and student competitions (CyberPatriot and the National Collegiate Cyber Defense Competition), scholarships for cybersecurity postsecondary students who agree to serve in government after graduation (CyberCorps), and professional development for federal personnel in specialized cybersecurity positions (College of Cyber and the Federal Virtual Training Environment).[45] Federal programs not specifically designed to provide cybersecurity education and training—such as the TechHire and Advanced Technological Education programs—may also provide grants for these purposes.

Over the past decade, analysts seeking to document the scope and scale of the U.S. cybersecurity workforce came to realize that the federal government, private employers, and academics were not using the same language to describe cybersecurity jobs or the knowledge, skills, and abilities necessary to hold those positions. This lack of a common language was perceived as a potential barrier in the cybersecurity labor market and an impediment in federal hiring. In response, the National Initiative for Cybersecurity Education (NICE)—the federal coordinating body for cybersecurity education, training, and workforce development—undertook a multiyear effort to develop standard terms and uses. When finalized, the *NICE Cybersecurity Workforce Framework* (*Framework*) is to provide a standard vocabulary that can be used to better align education and employment in cybersecurity fields.[46] Among its many other cybersecurity education-related activities, NICE also provides grants to regional education-employment partnerships for the purpose of aligning academic pathways with cybersecurity occupations.

One key policy issue for the 115th Congress may relate to the *Framework*'s implementation. Although the central issue for the *Framework* is its use as a cybersecurity workforce management

[44] Section written by Heather Gonzalez, former Specialist in Education Policy. For further information, contact (name redacted), Analyst in Education Policy ( [redacted]@crs.loc.gov , 7-....), and see CRS In Focus IF10654, *Challenges in Cybersecurity Education and Workforce Development*, by (name redacted) .

[45] For more information, see GenCyber at https://www.gen-cyber.com/; CyberPatriot at https://www.uscyberpatriot.org/; the National Collegiate Cyber Defense Competition at http://www.nationalccdc.org/; and the CyberCorps/Scholarship for Service program at https://www.sfs.opm.gov/.

[46] William Newhouse, Stephanie Keith, Benjamin Scribner, and Greg Witte, "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework," NIST Special Publication 800-181, August 2017, at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.

tool in federal agencies, cybersecurity education programs may begin to adopt the language (and align curriculum and grantee requirements) during the next few years as well. Other policy topics that may be addressed during the 115th Congress include the role or expansion of educational benefits as tools for attracting and retaining federal cybersecurity personnel, as well as funding for federal cybersecurity education, training, and workforce development programs. Longer-term policy issues in cybersecurity education may include the ongoing challenge of ensuring that educational content evolves in tandem with the rapidly changing cyber defense and operations landscape; continued training of incumbent workers in the federal government in secure computing practices; and, potentially, the continuing development of existing certifications, or the creation of new, nontraditional educational credentials, such as microcredentialing and digital badging.

# Encryption[47]

Encryption is a process to secure information from unwanted access or use. Encryption uses the art of cryptography to change information which can be read (plaintext) and make it so that it cannot be read (ciphertext). Decryption uses the same art of cryptography to change that ciphertext back to plaintext. Data that are in a state of being stored or transmitted are eligible for encryption. However, data that are in a state of being processed—that is, being generated, altered, or otherwise used—are unable to be encrypted and remain in plaintext and vulnerable to unauthorized access.[48]

## Encryption as a Cybersecurity Tool[49]

Encryption is used by a variety of users for a variety of purposes. Fundamentally, encryption enables information to remain confidential to a single user or between a user and multiple users. Encryption also enables a level of certainty that the communicating parties are who they say they are and that the communication is only available to intended recipients.

Individuals use encryption to keep aspects of their lives that are held on digital platforms private on their devices and among those with whom they share information.[50] Businesses use encryption to ensure that their research is kept confidential from their competitors, and to ensure that their transactions with their suppliers and customers are authentic.[51] Governments use encryption to assure their information is kept and handled in confidence.[52] Even without a user's interaction, devices may use encryption when communicating to other devices to ensure that commands received from one device are authentic and safe to execute.[53] However, those seeking to obscure

[47] Introduction written by (name redacted), Analyst in Cybersecurity Policy ([redacted]@crs.loc.gov, 7-....).

[48] For further information on and analysis of encryption, see CRS Report R44642, *Encryption: Frequently Asked Questions*, by (name redacted)

[49] Section written by (name redacted), Analyst in Cybersecurity Policy ([redacted]@crs.loc.gov, 7-....).

[50] Bruce Schneier, "Why We Encrypt," *Schneier on Security*, June 23, 2015, at https://www.schneier.com/blog/archives/2015/06/why_we_encrypt.html.

[51] Federal Trade Commission, "Start with Security: A Guide for Business," guidance, June 2015, at https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.

[52] Office of Management and Budget, "Protection of Sensitive Agency Information," M-06-16, June 23, 2006, at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2006/m06-16.pdf.

[53] U.S. Department of Energy, "Secure Data Transfer Guidance for Industrial Control and SCADA Systems," PNNL-20776, September 2011, at http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-20776.pdf.

their malicious activities from legal authorities may also employ encryption to thwart opportunities to disrupt their malicious activity.[54]

## Encryption and Law Enforcement Investigations[55]

Changing technology presents opportunities and challenges for U.S. law enforcement. While some feel that law enforcement now has more information available to them than ever before, others contend that law enforcement is "going dark" as their investigative capabilities are outpaced by the speed of technological change.[56] As such, law enforcement cannot access certain information they otherwise may be authorized to obtain. One such technology-related hurdle for law enforcement is strong, end-to-end (or what law enforcement has sometimes called "warrant-proof") encryption.[57]

The tension between law enforcement capabilities and technological change has received congressional attention for several decades. For instance, in the 1990s the "crypto wars" pitted the government against technology companies, and this tension was highlighted by proposals to build in vulnerabilities, or "back doors," to certain encrypted communications devices as well as to restrict the export of strong encryption code.[58] In addition, Congress passed the Communications Assistance for Law Enforcement Act (CALEA; P.L. 103-414) in 1994 to help law enforcement maintain their ability to execute authorized electronic surveillance as telecommunications providers turned to digital and wireless technology.

There has been previous executive and congressional action aimed at helping law enforcement conduct investigations of cybercrimes in the face of changing technology that can hamper such investigations. The going dark debate originally focused on data in motion, or law enforcement's ability to intercept real-time communications. However, more recent technology changes have affected law enforcement's capacity to access not only communications but also stored content, or data at rest. The Obama Administration urged the technology community to develop a means to assist law enforcement in accessing encrypted data and took steps to bolster law enforcement's technology capabilities to do so. In addition, policymakers have been evaluating whether legislation may be an appropriate response to the problem of going dark—particularly with regards to encryption. The Encryption Working Group in the 114th Congress made several observations to set up the going dark discussion for the 115th Congress. It noted that (1) any measure to weaken encryption would work against the nation's interest, (2) encryption technology is widely used and increasingly available worldwide, (3) there is no one-size-fits-all

[54] James Comey, "Remarks to the 2016 Symantec Government Symposium," August 30, 2016, at https://www.c-span.org/video/?414522-1/fbi-director-james-comey-addresses-concerns-voter-database-breaches.

[55] Section written by (name redacted), Specialist in Domestic Security ([redacted]@crs.loc.gov, 7-....). For more information on this issue, see CRS Report R44481, *Encryption and the "Going Dark" Debate*, by (name redacted).

[56] See Peter Swire and Kenesa Ahmad, *"Going Dark" Versus a "Golden Age for Surveillance,"* Center for Democracy and Technology, November 28, 2011, as well as Federal Bureau of Investigation, *Going Dark*, at https://www.fbi.gov/services/operational-technology/going-dark.

[57] See, for example, International Association of Chiefs of Police, *Data, Privacy, and Public Safety: A Law Enforcement Perspective on the Challenges of Gathering Electronic Evidence*, November 2015. See also testimony before U.S. Congress, House Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, *Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives*, 114th Cong., 2nd sess., April 19, 2016.

[58] See Philip Elmer-DeWitt, "Apple and the FBI Re-Enact the '90s Crypto Wars," *Fortune*, September 27, 2014; and Todd Lappin, "Winning the Crypto Wars," *Wired*, May 1, 1997. The term "crypto wars" has been used by the Electronic Frontier Foundation and others to describe this debate.

solution to the encryption and going dark challenge, and (4) Congress should promote cooperation between the law enforcement and technology communities.[59]

## Information Sharing[60]

Cyberspace evolves at a rapid pace. That exacerbates the speed and intensity of the cybersecurity arms race between attackers and defenders. As a result, having timely, accurate information is essential for effective cybersecurity—not only threat information, but also defenses, best practices, and other things. Such information sharing is generally considered an important tool for protecting information systems from unauthorized access.

However, barriers to information sharing—both within and across sectors—have long been considered by many to be a significant hindrance, especially with respect to critical infrastructure (CI) sectors. Private-sector entities have often asserted a reluctance to share such information among themselves because of concerns about legal liability, antitrust violations, and potential misuse, especially of intellectual property, including trade secrets and other proprietary business information.

Legislation focusing specifically on alleviating such obstacles to information sharing in cybersecurity was first considered in the 112th Congress, but debate about issues such as regulation and privacy continued until enactment in the 114th. In December 2015, the Cybersecurity Information Sharing Act (CISA) was signed into law as part of the Cybersecurity Act of 2015 (Division N of P.L. 114-113). CISA takes steps to facilitate public- and private-sector sharing of information on cybersecurity threats and defensive measures and to permit private-sector entities to monitor and operate defenses on their information systems. It includes procedures for sharing of classified information; protections for security, privacy, nondisclosure, and correction of errors in shared information; exemptions from liability and antitrust actions for covered activities; and limitations on the uses of shared information by both public and private entities. The Cybersecurity Act of 2015 also makes the DHS National Cybersecurity and Communications Integration Center (NCCIC) the lead agency for federal information sharing.

In overseeing implementation of CISA, Congress might consider a number of factors that might affect its successful application:

- Information that may be usefully shared can be complex in type and purpose, which may complicate determining the best methods and criteria for sharing.
- The timescale during which shared information will be most useful varies with the kind of information shared and its purpose.
- A large increase in information sharing could potentially lead to information overload, reducing the effectiveness of the sharing in reducing cybersecurity risks.
- Protection of confidentiality, privacy, and civil liberties in information sharing remains an area of controversy.

[59] House Judiciary Committee and House Energy and Commerce Committee, Encryption Working Group, *Encryption Working Group Year-End Report*, December 20, 2016. Members of the House Judiciary Committee and Energy and Commerce Committee established this Working Group to "identify potential solutions that preserve the benefits of strong encryption—including the protection of Americans' privacy and information security—while also ensuring law enforcement has the tools needed to keep us safe and prevent crime." House Judiciary Committee, "Goodlatte, Conyers, Upton, and Pallone Announce Bipartisan Encryption Working Group," press release, March 21, 2016.

[60] Section written by (name redacted), Senior Specialist in Science and Technology ([redacted]@crs.loc.gov, 7-....).

- The complexity of the current structure for information sharing may complicate implementation and assessment of effectiveness. It includes not only federal agencies and end users such as businesses but also private-sector information sharing and analysis entities (centers called information sharing and analysis centers, or ISACs, established pursuant to Presidential Decision Directive 63 in 1998, and organizations called information sharing and analysis organizations, or ISAOs, established under the Homeland Security Act of 2002 and Executive Order 13691 of 2015), trade and professional associations, and other mechanisms.
- Sharing of information among private-sector entities might not be substantially improved by CISA. Even if it is successful, information sharing is only one facet of cybersecurity, and the changes made by CISA might by themselves be of limited effectiveness in improving cybersecurity. Information sharing tends to focus on immediate concerns such as cyberattacks and imminent threats. While those must be addressed, that does not diminish the importance of other issues such as education and training, workforce, acquisition, or cybercrime law, or major long-term challenges such as building security into the design of hardware and software, changing the incentive structure for cybersecurity, developing a broad consensus about cybersecurity needs and requirements, and otherwise adapting to the rapid evolution of cyberspace.[61]

## Insurance[62]

Businesses and individuals often use insurance for financial risks that they are unwilling or unable to bear on their own. With the uncertainty and potential size of damages from cyberattacks, entities' interest in insurance against such attacks has been growing in the past few years. Although policies covering cyber risk have been offered for over a decade, the market in general is still largely in its infancy. Much of the coverage is offered outside the regular *admitted* market made up of insurers fully licensed by the state in which they are operating. The National Association of Insurance Commissioners (NAIC) has estimated premiums for cyber insurance at approximately $1.5 billion but recognizes that "a significant amount of premium" is missing from this estimate since it is being offered by non-U.S. companies who do not file information with the states.[63] The actuarial data regarding loss probabilities and severities upon which insurers depend to set premiums are still scarce, and policy language is not standardized, with policies generally including low dollar limits and "a whole slew of exclusions" to limit insurer risk.[64]

The immaturity of the cyber insurance market could be seen as purely a matter of private concern bearing mainly on who may suffer losses from a particular cyberattack. In some circumstances, however, insurance may also be seen to have a public policy purpose. Insurance premiums can cause someone to internalize a risk or a benefit that otherwise might go unrecognized. With security on the internet, for example, being such an interdependent system, such recognition can

[61] For further information see CRS Report R43831, *Cybersecurity Issues and Challenges: In Brief*, by (name redacted).

[62] Section written by (name redacted), Specialist in Financial Economics ([redacted]@crs.loc.gov, 7-....).

[63] National Association of Insurance Commissioners, *Report on the Cybersecurity Insurance Coverage Supplement*, August 16, 2007, p. 5, at http://www.naic.org/documents/committees_ex_cybersecurity_tf_report_cyber_supplement.pdf.

[64] S&P Global Market Intelligence, "Looking Before They Leap: U.S. Insurers Dip Their Toes in the Cyber-Risk Pool," June 9, 2015, at https://www.globalcreditportal.com/ratingsdirect/renderArticle.do?articleId=1403078.

be particularly important and increase security for everyone.[65] Insurers also often act to transmit valuable information on avoiding and mitigating losses.

In the 114th Congress, a Senate subcommittee hearing on cyber insurance was held[66] and legislation was introduced in the House (H.R. 6032) which would have provided a business tax credit for the purchase of "data breach insurance." In addition to the incentive for purchasing cyber insurance inherent in the tax credit, H.R. 6032 would also have required compliance with NIST standards on cybersecurity to be eligible for the credit.

Congress has enacted laws and programs affecting a range of other insurance markets such as health insurance (Medicare, Affordable Care Act), flood insurance (National Flood Insurance Program), and terrorism insurance (Terrorism Risk Insurance Act). Should the 115th Congress seek to encourage cyber insurance, a relatively wide range of approaches from a tax, regulatory, or program perspective could be considered.

## International Issues

### Trade[67]

Cybersecurity poses challenges in the international trade arena as more trade is conducted, or facilitated, online, potentially increasing the susceptibility of commerce to cyberattack and theft of information. Digital trade, including end products like movies and video games, and services such as email and online banking, enhances the productivity and overall competitiveness of an economy, enabling technological shifts that are transforming businesses. According to one study, the global economic impact of the internet is estimated at $4.2 trillion in 2016, and would rank as the fifth-largest national economy in the world.[68] According to the Bureau of Economic Analysis, in 2015, the United States exported $751 billion in services, of which over 60% were information and communication technology (ICT) and potentially ICT-enabled services.[69]

The increase in digital trade also raises new challenges in U.S. trade policy, including how best to address new and emerging trade barriers and risks related to cybersecurity. For example, hacks into company databases and systems could disrupt worldwide business operations and global supply chains, and pose a threat to consumers whose personal information may be stolen or manipulated. Publicized cyberattacks on firms may depress stock values. When governments of U.S. trading partners impose trade barriers, such as data localization measures compelling companies to store data within the country's border, a U.S. firm's data may become fragmented, creating vulnerabilities and increasing the risk of a cyberattack.

---

[65] See, for example, Marc Lelange and Jean Bolot, "Economic Incentives to Increase Security in the Internet: The Case for Insurance," at http://www.di.ens.fr/~lelarge/papiers/2009/infocom09_cr.pdf.

[66] U.S. Congress, Senate Committee on Commerce, Science, and Transportation, Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security, *Examining the Evolving Cyber Insurance Marketplace*, 114th Cong., 2nd sess., March 19, 2015, at http://www.commerce.senate.gov/public/index.cfm/2015/3/examining-the-evolving-cyber-insurance-marketplace.

[67] Section written by Rachel Fefer, Analyst in International Trade and Finance ([redacted]@crs.loc.gov, 7-....).

[68] Paul Zwillenberg, Dominic Field, and David Dean, *Greasing the Wheels of the Internet Economy*, Boston Consulting Group, February 2014, at https://www.bcgperspectives.com/content/articles/digital_economy_telecommunications_greasing_wheels_Internet_economy/.

[69] U.S. Bureau of Economic Analysis, Trade in Goods and Services table at http://www.bea.gov/international/index.htm.

The internet is a key driver of intellectual property-related trade. However, it can make infringement of intellectual property rights (IPR) easier, and identifying those responsible for IPR infringement more challenging. Cyber theft of trade secrets can wipe out the value and competitive advantage of a firm's long-term research, presenting additional, increasingly prominent, barriers to digital trade. In May 2014, DOJ indicted five Chinese individuals for government-sponsored cyber espionage against U.S. companies and theft of proprietary information to aid the competitiveness of Chinese state-owned enterprises (SOEs).

U.S. companies see potential challenges as countries develop new cyber regimes, such as China's new cybersecurity law, passed in November 2016. The law imposes several restrictions on internet firms including requiring operators of critical information infrastructure (defined as sectors such as telecommunications, energy, and finance) to store certain data in China, and requiring companies to assist Chinese police and national security agencies. The law's security reviews may force companies to disclose source code, a concern of many U.S. firms who are hesitant to reveal proprietary information about their business intellectual property that could potentially expose them to further cyberattacks. The law states that a key goal is "secure and controllable" technology, a term some see as an attempt to promote local ICT providers and lock out foreign firms. U.S. companies and various U.S. officials, such as former National Security Adviser Susan Rice, have raised U.S. concerns about the potential impact of the law.[70]

The United States holds high-level cyber dialogues with multiple bilateral partners, such as China, India, and the European Union, to focus on cybersecurity efforts. Recent bilateral and plurilateral agreements have begun to address digital trade rules and barriers more explicitly.[71] For example, the proposed Trans-Pacific Partnership (TPP) promoted cooperation among the parties on cybersecurity issues and has new enforceable commitments to combat cyber theft of trade secrets and localization barriers. The United States also discusses digital trade and cybersecurity norms in forums such as the Group of 20 (G-20), the Organization for Economic Co-operation and Development (OECD), and the Asia-Pacific Economic Cooperation (APEC). The 2016 G-7 Joint Declaration endorsed the "G7 Principles and Actions on Cyber."[72]

Congress has an interest in ensuring the global rules and norms of the internet economy align with U.S. laws and norms, and that U.S. trade policy on digital trade and cybersecurity advances U.S. interests. Congress may consider specific actions to uphold the G-7 commitments to serve as a model for other countries; hold hearings on trade barriers, negotiations, or international forums in relation to cybersecurity; conduct oversight of the relevant executive branch agencies; or consider legislation to respond to cybersecurity threats to U.S. trade and businesses, including the imposition of sanctions.[73]

[70] Reuters, "White House Voices Concerns About China Cyber Law," December 8, 2016, at http://www.reuters.com/article/us-usa-china-cyber-idUSKBN13X2NO?mod=djemCIO_h.

[71] Bilateral agreements involve two parties. Plurilateral agreements are agreements among a group of parties that are part of a larger coalition. Multilateral agreements are agreements among all members of a coalition.

[72] U.S. Department of State, "G7 Principles and Actions on Cyber," fact sheet, March 13, 2016, at https://2009-2017.state.gov/s/cyberissues/releasesandremarks/258028.htm.

[73] For more information on cybersecurity and trade, see CRS In Focus IF10030, *U.S.-China Trade Issues*, by (name red acted) ; CRS In Focus IF10033, *Intellectual Property Rights (IPR) and International Trade*, by (name redacted) and (name redacted) ; and CRS Report R44565, *Digital Trade and U.S. Trade Policy*, coordinated by (name reda cted).

## Internet of Things Security[74]

"Internet of Things" (IoT) refers to networks of objects that communicate with other objects and with computers through the internet. "Things" may include virtually any object for which remote communication, data collection, or control might be useful, such as vehicles, appliances, medical devices, electric grids, transportation infrastructure, manufacturing equipment, or building systems. In other words, the IoT potentially includes huge numbers and kinds of interconnected, "smart" objects. It is often considered the next major stage in the evolution of cyberspace.

Smart devices can form systems that communicate among themselves, usually in concert with computers, allowing automated and remote control of many independent processes and potentially transforming them into integrated systems. Those systems can potentially impact homes and communities, factories and cities, and every sector of the economy, both domestically and globally. The IoT can contribute to more integrated and functional infrastructure, especially in "smart cities," with projected improvements in transportation, utilities, and other municipal services.

Although the full extent and nature of the IoT's impacts remain uncertain, economic analyses predict that it will contribute trillions of dollars to economic growth over the next decade. Sectors that may be particularly affected include agriculture, energy, government, health care, manufacturing, and transportation.

IoT objects are potentially vulnerable targets for hackers. As the number of connected objects in the IoT grows, so will the potential risk of successful intrusions into IoT devices and increases in costs from those incidents. Economic and other factors may reduce the degree to which such objects are designed with adequate cybersecurity capabilities built in. IoT devices are small, are often built to be disposable, and may have limited capacity for software updates to address vulnerabilities that come to light after deployment.

The interconnectivity of IoT devices may also provide entry points through which hackers can access other parts of a network. Control of a set of smart objects could permit hackers to use their computing power in malicious networks called botnets to perform various kinds of cyberattacks, such as the 2016 attack using the Mirai botnet that interrupted the internet services of several companies. Access could also be used for destruction, such as by modifying the operation of industrial control systems, as with the Stuxnet malware that caused centrifuges to self-destruct at Iranian nuclear plants.[75]

## Oversight of Federal Agency Information Technology Security[76]

The Federal Information Security Management Act (FISMA, P.L. 107-347, as amended) places the responsibility for the information security of a federal agency with the agency head. Specifically, 44 U.S.C. §3554 states the following:

> The head of each agency shall—
>
> (1) be responsible for—

[74] Section written by (name redacted), Senior Specialist in Science and Technology ([redacted]@crs.loc.gov, 7-....).

[75] For further information, contact (name redacted), Analyst in Cybersecurity Policy ([redacted]@crs.loc.gov, 7-....) or (name redacted), Senior Specialist in Science and Technology ([redacted]@crs.loc.gov, 7-....). For further reading, see CRS Report R44227, *The Internet of Things: Frequently Asked Questions*, by (name redacted).

[76] Section written by (name redacted), Analyst in Cybersecurity Policy ([redacted]@crs.loc.gov, 7-....).

> (A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—
>
> (i) information collected or maintained by or on behalf of the agency; and
>
> (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency[.]

In executing this responsibility, each agency head shall also ensure the agency has senior officials who can operationally oversee the management and security of agency information technology. Congress requested an annual, independent evaluation of agency information security performance, conducted by the agency inspector general, to assist in Congress's oversight of the agency's IT management and security of its systems and data.

Congress has also passed additional legislation regarding the management of federal information technology. The Federal Information Technology Acquisition Reform Act (FITARA, P.L. 113-291, Title VIII) expanded the role of the chief information security officer (CIO) in the financial management of planning, programming, and execution of IT acquisitions for agencies. It also requires the Office of Management and Budget (OMB) to report to Congress on the net performance of capital investments. In addition, FISMA 2014 (P.L. 113-283) specifies some operational roles for DHS and the Office of the Director of National Intelligence (DNI) in IT security. It also directs OMB to provide additional reports to Congress on the adoption of security technologies by federal agencies and sets out the guidance for agencies to directly report to Congress when they experience a data breach. Also, the Cybersecurity Act of 2015 (P.L. 114-113, Division N) requires the inspectors general of each agency with a national security system or a system that has access to personally identifiable information to report to Congress on the security policies and practices of those systems.

The OMB reports to Congress on annual FISMA performance usually arrive in the spring of each calendar year, and agency IG reports on annual information security evaluations or periodic information systems security reports are released throughout the year. These reports, along with those from the Government Accountabily Office (GAO), can assist Congress in executing oversight over agency operations, and can inform Congress on agency performance.[77]

## Response to Cybersecurity Incidents[78]

Presidential Policy Directive 41 (PPD-41), issued on July 26, 2016, by the Obama Administration, outlines guiding principles and the government's policy response to a cyber incident. The National Cyber Incident Response Plan (NCIRP) elaborates on those principles by delineating responsibilities and outlining the coordinating of federal agencies. PPD-41 states that

- response is a shared responsibility among the victims, private sector, and the government;
- responses must be risk-based to determine which resources to bring to bear;

[77] An example of the annual FISMA report to Congress may be found online at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/egov/documents/omb-fy-2016-egov-act-report.pdf.

[78] Section written by (name redacted), Analyst in Cybersecurity Policy ([redacted]@crs.loc.gov, 7-....).

- any response must respect the affected entities and must require a unity of effort across federal agencies; and
- any response should be done in a manner that enables restoration and recovery of operations to the victim, not just retaliation against the hacker.

The policy also dictates that a government response is to have concurrent lines of effort. Threat response activities are to be led by the FBI and involve seeking out and delivering a response against the hacker. Asset response activities, as prescribed in PPD-41, are to be led by DHS and involve efforts to help victims mitigate the effects of an attack. The intelligence community is to provide assistance to both lines of effort.[79]

Following the release of PPD-41, the government adopted the NCIRP.[80] The NCIRP follows a model developed to support conventional emergency management in the National Preparedness System, especially the National Response Framework. In doing so, it borrows the use of a core capability approach and adopts key aspects of the National Incident Management System (NIMS).[81] Instead of prescribing specific actions for agencies to take, the NCIRP outlines how the government is to activate a Cyber Unified Coordination Group to address the specific incidents. This is similar to how the government activates a multiagency group at a Joint Field Office to deliver federal resources in response to a natural disaster.

Lacking specific responses, or even a menu of options for the Cyber Unified Coordination Group to consider, the NCIRP is not an operational plan, and as such may not have a deterrent effect on adversaries.

PPD-41 describes two sides to a response: efforts directed at providing support for the victim and efforts directed at tracking down and punishing the aggressor. Similar to how the fire department will put out the fire and get people to safety while the police department pursues the arson, the federal government's response activities are directed toward both the victim and the attacker.

Response focusing on victims seeks to remediate the attack's effects. Such activities endeavor to remove any malware installed on systems, repair damaged systems, and work with incident response teams to restore unadulterated operations. Although DHS is the lead federal agency for such activities, it also relies on capabilities from partner agencies such as the DOD or the intelligence community in providing a response, as well as a critical infrastructure sector-specific agency. The federal government may provide resources to victims, but the victim is not under any obligation to accept federal resources. Victims may opt to respond to incidents with in-house teams, or by retaining cybersecurity firms. If the federal government is invited to assist with incident response, its work may only be made public with the victim's consent, by matter of administrative policy. However, the very action of federal resources being delivered to assist with response to a cyber incident can act as an overt federal reaction, signaling to both other victims and adversaries the options the federal government will pursue for cybersecurity.

Frequently concurrent to a response directed at helping victims, response focused on attackers seeks to determine who committed the attack and deliver some form of retaliation. Such activities endeavor to attribute the attack to a group or an individual, and develop options which will both

[79] The White House, "Presidential Policy Directive—United States Cyber Incident Coordination," presidential directive, July 26, 2016, at https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

[80] Department of Homeland Security, "National Cyber Incident Response Plan," December 2016, at https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf.

[81] For details on the National Response Framework, see https://www.fema.gov/media-library/assets/documents/32230.

punish the attacker and seek to deter additional adversarial action. Options may include an overt cyber-based response, a covert cyber-based attack against the adversary, announcing sanctions against the group or individual, indicting or arresting those responsible, or using some other form of national power. Although the FBI is the lead federal agency for responding domestically in this line of effort, it will also rely on the capabilities of partner agencies, such as DOD for a cyberattack, the intelligence community for attribution, the Department of the Treasury for sanctions, or the Department of State for diplomatic options.

# Previous Policy Action[82]

## Recent Legislative Action

A complete list of bills considered during the 115th Congress may be found in CRS Report R43317, *Cybersecurity: Legislation, Hearings, and Executive Branch Documents*, by (name redacted)

More than 10 bills received consideration and action during the first session of the 115th Congress to address several issues, including management of federal IT, assisting state and local governments investigate cybercrimes, improving information sharing, and the development of voluntary guidelines on ways to reduce cyber risks.

More than 30 bills were introduced in the 114th Congress that would have addressed 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 released proposals for three bills—on information sharing, data-breach notification, and revision of cybercrime laws. Several bills received committee or floor action.

On December 18, 2015, H.R. 2029, the Consolidated Appropriations Act, 2016, was signed into public law (P.L. 114-113). The omnibus law's cybersecurity provisions are located in Division N (Cybersecurity Act of 2015), including Title I, Cybersecurity Information Sharing; Title II, National Cybersecurity Advancement; Title III, Federal Cybersecurity Workforce Assessment; and Title IV, Other Cyber Matters. The bill encourages private companies to voluntarily share information about cyber threats with each other as well as the government. Firms that participate in the information sharing are to receive liability protection.

In the 113th Congress, five cybersecurity-focused bills were signed into law on December 18, 2014:

- H.R. 2952, the Cybersecurity Workforce Assessment Act, which requires the DHS to develop a cyber-workforce strategy (P.L. 113-246);
- S. 1353, the Cybersecurity Enhancement Act of 2014, which codifies the National Institute of Standards and Technology's (NIST's) role in cybersecurity (P.L. 113-274);
- S. 1691, the Border Patrol Agent Pay Reform Act of 2014, which gives DHS new authorities for cybersecurity hiring (P.L. 113-277);
- S. 2519, the National Cybersecurity Protection Act of 2014, which codifies DHS's cybersecurity center (P.L. 113-282); and

[82] Section written by (name redacted), Senior Research Librarian, ([redacted]@crs.loc.gov, 7-....).

- S. 2521, the Federal Information Security Modernization Act of 2014, which reforms federal IT security management (P.L. 113-283).

The National Defense Authorization Act for Fiscal Year 2014, which became P.L. 113-66 on December 26, 2013, included a variety of cybersecurity-related provisions.

The below tables summarize recent legislative actions.

**Table 1. 114th Congress Cybersecurity Public Laws**

| Bill No. | Title | Committee(s) | Date Introduced | Public Law | Date Enacted |
|---|---|---|---|---|---|
| H.R. 2029[83] | Consolidated Appropriations Act, 2016 | Appropriations | April 24, 2015 | P.L. 114-113 | December 18, 2015 |

**Table 2. 113th Congress Cybersecurity Public Laws**

| Bill No. | Title | Committee(s) | Date Introduced | Public Law | Date Enacted |
|---|---|---|---|---|---|
| S. 2521 | Federal Information Security Modernization Act of 2014 | Senate Homeland Security and Government Affairs | June 24, 2014 | P.L. 113-283 | December 18, 2014 |
| S. 2519 | National Cybersecurity Protection Act of 2014 | Senate Homeland Security and Governmental Affairs | June 24, 2014 | P.L. 113-282 | December 18, 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 Enhancement Act of 2014 | Senate Commerce, Science, and Transportation | July 24, 2013 | P.L. 113-274 | December 18, 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. 2952 | Critical Infrastructure Research and Development Advancement Act of 2013 | House Homeland Security | August 1, 2013 | P.L. 113-246 | December 18, 2014 |

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

## Recent Executive Action

The White House has taken actions independent of Congress to address a variety of cybersecurity issues. Recent executive actions are described below in reverse chronological order, starting with the most recent action.

In May 2017, the Trump Administration issued an executive order (E.O. 13800) designed to improve the cybersecurity of both federal networks and critical infrastructure.[84] It requires federal agencies to manage cybersecurity risks holistically across the government. It also directs federal agencies to take specific steps to assist the private sector in managing cyber risks.

Previously, the Obama Administration issued an executive order (E.O. 13757) amending E.O. 13694 to allow for the imposition of sanctions on individuals and entities determined to be responsible for tampering, altering, or causing the misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions. Five entities and four individuals were identified in the Annex of the amended Executive Order and added to the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) list of Specially Designated Nationals and Blocked Persons (SDN List).

On April 1, 2015, the Obama Administration issued an executive order (E.O. 13694) placing sanctions on certain persons engaging in significant malicious cyber-enabled activities.[85] The executive order established 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 cyber activity for sanctions that could include freezing their financial assets and barring commercial transactions with them.

In February 2015, the Obama Administration issued Executive Order 13691, which, along with a legislative proposal, is aimed at enhancing information sharing in cybersecurity among private sector entities.[86] 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 to assist in defense against and recovery from incidents.[87] These initiatives broadened the reach of ISAOs beyond CI to any affinity group (e.g., geography, business sector, etc.). 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 created the Cyber Threat Intelligence Integration Center (CTIIC), established by the DNI.[88] Its purposes are to provide integrated

[84] For further information, see CRS Insight IN10707, *A Little Old, a Little New: The Cybersecurity Executive Order*, by (name redacted)

[85] The White House, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," 80 *Federal Register* 18077-18079, April 2, 2015.

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

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

[88] The White House, "Establishment of the Cyber Threat Intelligence Integration Center," Presidential Memorandum, February 25, 2015, at http://www.whitehouse.gov/the-press-office/2015/02/25/presidential-memorandum-

(continued...)

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 DHS, as well as other entities at DOD and DOJ.

In February 2013, the Obama Administration issued an executive order (E.O. 13636) designed to improve the cybersecurity of U.S. critical infrastructure.[89] It 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 cyber threats. 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.[90]

Below is a table of executive action on cybersecurity-related issues.

**Table 3. Executive Orders and Presidential Directives**

(by date of issuance from most recent)

| Title | Date | Notes |
|---|---|---|
| E.O. 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure | May 11, 2017 | Directs agencies to take additional actions to protect federal IT networks and to work with the private sector to develop ways to better protect the nation from cyberattacks. |
| E.O. 13757, Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities | December 29, 2016 | This amends Executive Order 13694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities." E.O. 13694 authorizes the imposition of sanctions on individuals and entities determined to be responsible for or complicit in malicious cyber-enabled activities that result in enumerated harms that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States. The authority has been amended to also allow for the imposition of sanctions on individuals and entities determined to be responsible for tampering, altering, or causing the misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions. Five entities and four individuals are identified in the Annex of |

(...continued)

establishment-cyber-threat-intelligence-integrat.

[89] The White House, "Improving Critical Infrastructure Cybersecurity," 78 *Federal Register* 11739-11744, February 19, 2013.

[90] For further discussion of the executive order, see CRS Report R42984, *The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress*, by (name redacted) et al.

| Title | Date | Notes |
|---|---|---|
| | | the amended Executive Order and added to OFAC's list of Specially Designated Nationals and Blocked Persons (SDN List). OFAC is designating an additional two individuals who also will be added to the SDN List. |
| Presidential Policy Directive 41—United States Cyber Incident Coordination | July 26, 2016 | The PPD sets forth principles governing the federal government's response to any cyber incident, whether involving government or private-sector entities. For significant cyber incidents, the PPD establishes lead federal agencies and an architecture for coordinating the broader federal government response. The PPD also requires the Departments of Justice and Homeland Security to maintain updated contact information for public use to assist entities affected by cyber incidents in reporting those incidents to the proper authorities. |
| Annex for Presidential Policy Directive 41—United States Cyber Incident Coordination | July 26, 2016 | The annex to PPD-41 provides further details concerning the federal government coordination architecture for significant cyber incidents and prescribes certain implementation tasks pertaining to coordination architecture, federal government response to incidents affecting federal networks, and implementation and assessment. |
| E.O. 13718, Commission on Enhancing National Cybersecurity | February 9, 2016 | The commission consists of 12 members appointed by the President, including "top strategic, business, and technical thinkers from outside of Government—including members to be designated by the bi-partisan Congressional leadership." |
| E.O. 13694, Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities | April 1, 2015 | 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 | The CTIIC is 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 is to also assist |

| Title | Date | Notes |
|---|---|---|
| | | 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 | 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 | 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 the Administration authorized 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 | The executive order mandates that government credit and debit cards be enabled with chip and PIN technology and federal facilities accept chip and PIN-enabled cards at retail terminals. |
| E.O. 13636, Improving Critical Infrastructure Cybersecurity | February 12, 2013 | E.O. 13636 addresses cybersecurity threats to critical infrastructure (CI) by, among other things,<br>• expanding to other CI sectors an existing DHS program for information sharing and collaboration between the government and the private sector;<br>• establishing a broadly consultative process for identifying CI with especially high priority for protection;<br>• requiring the National Institute of Standards and Technology to lead in developing a Cybersecurity Framework of standards and best practices for protecting CI; and<br>• requiring regulatory agencies to determine the adequacy of current requirements and their authority to establish requirements to address the risks. |

| Title | Date | Notes |
|---|---|---|
| Presidential Policy Directive (PPD) 21—Critical Infrastructure Security and Resilience | February 12, 2013 | 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. This directive also refines and clarifies the critical infrastructure-related functions, roles, and responsibilities across the federal government, as well as enhances overall coordination and collaboration. The federal government also has a responsibility to strengthen the security and resilience of its own critical infrastructure, for the continuity of national essential functions, and to organize itself to partner effectively with and add value to the security and resilience efforts of critical infrastructure owners and operators. |
| E. O. 13618, Assignment of National Security and Emergency Preparedness Communications Functions | July 6, 2012 | This order addresses the federal government's need and responsibility to communicate during national security and emergency situations and crises by assigning federal national security and emergency preparedness communications functions. EO 13618 is a continuation of older executive orders issued by other presidents and is related to the Communications Act of 1934 (47 U.S.C. §606). This executive order, however, changes federal national security and emergency preparedness communications functions by dissolving the National Communications System, establishing an executive committee to oversee federal national security and emergency preparedness communications functions, establishing a programs office within the DHS to assist the executive committee, and assigning specific responsibilities to federal government entities. |

| Title | Date | Notes |
|---|---|---|
| E.O. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information | October 7, 2011 | 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. |
| Homeland Security Presidential Directive (HSPD)-23/National Security Presidential Directive (NSPD)-54—Cybersecurity Policy | January 8, 2008 | This directive establishes U.S. policy, strategy, guidelines, and implementation actions to secure cyberspace. It strengthens and augments existing policies for protecting the security and privacy of information entrusted to the federal government and clarifies roles and responsibilities of federal agencies relating to cybersecurity. It requires the federal government to integrate many of its technical and organizational capabilities to better address sophisticated cybersecurity threats and vulnerabilities. |

**Source:** Descriptions compiled by CRS from White House documents websites.

## Selected Hearings

The House has held over 30 hearings during the first session of the 115th Congress on cybersecurity issues, and the Senate has held over 25. The House held 84 cybersecurity hearings during the 114th Congress and the Senate held 35.[91] The House committees holding the most hearings during the 114th Congress were Homeland Security (17), Oversight and Government Reform (16), Science, Space, and Technology (8), and Energy and Commerce (7). The Senate committees holding the most hearings were Armed Services (8), Commerce, Science, and Transportation (6), and Homeland Security and Governmental Affairs (6).[92]

[91] Another hearing, Commercial Cyber Espionage and Barriers to Digital Trade in China (see http://www.uscc.gov/Hearings/hearing-commercial-cyber-espionage-and-barriers-digital-trade-china-webcast), was held by the U.S.-China Economic and Security Review Commission on June 15, 2015. The Commission was created by Congress in October 2000 with the legislative mandate to monitor, investigate, and submit to Congress an annual report on the national security implications of the bilateral trade and economic relationship between the United States and the People's Republic of China, and to provide recommendations, where appropriate, to Congress for legislative and administrative action.

[92] For a list of cybersecurity hearings in the 112th-114th Congresses, see CRS Report R43317, *Cybersecurity: Legislation, Hearings, and Executive Branch Documents*, by (name redacted)

A few topics of interest to 114th Congress committees were cybercrime (including privat-sector and federal data breaches and the Office of Personnel Management's 2015 cyber intrusions),[93] critical infrastructure vulnerabilities, oversight of federal and military cybersecurity programs, and the Internet of Things.

## Author Contact Information

(name redacted), Coordinator
Analyst in Cybersecurity Policy
[redacted]@crs.loc.gov, 7-....

(name redacted)
Analyst in International Trade and Finance
[redacted]@crs.loc.gov, 7-....

(name redacted)
Acting Section Research Manager
[redacted]@crs.loc.gov, 7-....

(name redacted)
Senior Specialist in Science and Technology
[redacted]@crs.loc.gov, 7-....

(name redacted)
Specialist in Terrorism and National Security
[redacted]@crs.loc.gov, 7-....

(name redacted)
Senior Research Librarian
[redacted]@crs.loc.gov, 7-....

(name redacted)
Specialist in National Security Policy, Cyber and Information Operations
[redacted]@crs.loc.gov, 7-....

(name redacted)
Specialist in Financial Economics
[redacted]@crs.loc.gov, 7-....

[93] CRS Report R44111, *Cyber Intrusion into U.S. Office of Personnel Management: In Brief*, coordinated by (name re dacted).