Congressional Research Service
Informing the legislative debate since 1914

Cybersecurity Issues and Challenges: In Brief

Updated August 12, 2016

Congressional Research Service
https://crsreports.congress.gov
R43831

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

The information and communications technology (ICT) industry has evolved greatly over the last half century. The technology is ubiquitous and increasingly integral to almost every facet of modern society. ICT devices and components are generally interdependent, and disruption of one may affect many others. Over the past several years, experts and policymakers have expressed increasing concerns about protecting ICT systems from cyberattacks, which many experts expect to increase in frequency and severity over the next several years.

The act of protecting ICT systems and their contents has come to be known as cybersecurity. A broad and arguably somewhat fuzzy concept, cybersecurity can be a useful term but tends to defy precise definition. It is also sometimes inappropriately conflated with other concepts such as privacy, information sharing, intelligence gathering, and surveillance. However, cybersecurity can be an important tool in protecting privacy and preventing unauthorized surveillance, and information sharing and intelligence gathering can be useful tools for effecting cybersecurity.

The management of risk to information systems is considered fundamental to effective cybersecurity. The risks associated with any attack depend on three factors: threats (who is attacking), vulnerabilities (the weaknesses they are attacking), and impacts (what the attack does). Most cyberattacks have limited impacts, but a successful attack on some components of critical infrastructure (CI)—most of which is held by the private sector—could have significant effects on national security, the economy, and the livelihood and safety of individual citizens. Reducing such risks usually involves removing threat sources, addressing vulnerabilities, and lessening impacts.

The federal role in cybersecurity involves both securing federal systems and assisting in protecting nonfederal systems. Under current law, all federal agencies have cybersecurity responsibilities relating to their own systems, and many have sector-specific responsibilities for CI. On average, federal agencies spend more than 10% of their annual ICT budgets on cybersecurity.

More than 50 statutes address various aspects of cybersecurity. Five bills enacted in the 113th Congress and another in the 114th address the security of federal ICT and U.S. CI, the federal cybersecurity workforce, cybersecurity research and development, information sharing in both the public and private sectors, and international aspects of cybersecurity. Other bills considered by Congress have addressed a range of additional issues, including data breach prevention and response, cybercrime and law enforcement, and the Internet of Things, among others.

Among actions taken by the Obama Administration during the 114th Congress are promotion and expansion of nonfederal information sharing and analysis organizations; announcement of an action plan to improve cybersecurity nationwide; proposed increases in cybersecurity funding for federal agencies of more than 30%, including establishment of a revolving fund for modernizing federal ICT; and a directive laying out how the federal government will respond to both government and private-sector cybersecurity incidents.

Those recent legislative and executive-branch actions are largely designed to address several well-established needs in cybersecurity. However, those needs exist in the context of difficult long-term challenges relating to design, incentives, consensus, and environment. Legislation and executive actions in the 114th and future Congresses could have significant impacts on those challenges.

Contents

The Concept of Cybersecurity 1
Management of Cybersecurity Risks 2
What Are the Threats? 2
What Are the Vulnerabilities? 2
What Are the Impacts? 2
Federal Role 3
Federal Spending 5
Legislative Proposals and Actions 5
Executive Branch Actions 8
Long-Term Challenges 9

Figures

Figure 1. Simplified Schematic Diagram of Federal Agency Cybersecurity Roles 4

Tables

Table 1. Federal FISMA and IT Spending 5
Table 2. Cybersecurity Bills Enacted in the 113th and 114th Congresses 6

Contacts

Author Information 9

The information technology (IT) industry has evolved greatly over the last half century. Continued, exponential progress in processing power and memory capacity has made IT hardware not only faster but also smaller, lighter, cheaper, and easier to use.

The original IT industry has also increasingly converged with the communications industry into a combined sector commonly called information and communications technology (ICT). This technology is ubiquitous and increasingly integral to almost every facet of modern society. ICT devices and components are generally interdependent, and disruption of one may affect many others.

The Concept of Cybersecurity

Over the past several years, experts and policymakers have expressed increasing concerns about protecting ICT systems from *cyberattacks*—deliberate attempts by unauthorized persons to access ICT systems, usually with the goal of theft, disruption, damage, or other unlawful actions. Many experts expect the number and severity of cyberattacks to increase over the next several years.[1]

The act of protecting ICT systems and their contents has come to be known as *cybersecurity*. A broad and arguably somewhat fuzzy concept, cybersecurity can be a useful term but tends to defy precise definition. It usually refers to one or more of three things:

- A set of activities and other measures intended to protect—from attack, disruption, or other threats—computers, computer networks, related hardware and devices, software, and the information they contain and communicate, including software and data, as well as other elements of cyberspace.[2]
- The state or quality of being protected from such threats.
- The broad field of endeavor aimed at implementing and improving those activities and quality.[3]

It is related to but not generally regarded as identical to the concept of *information security*, which is defined in federal law (44 U.S.C. §3552(b)(3)) as

> protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide-
>
> (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
>
> (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
>
> (C) availability, which means ensuring timely and reliable access to and use of information.

Cybersecurity is also sometimes conflated inappropriately in public discussion with other concepts such as privacy, information sharing, intelligence gathering, and surveillance. Privacy is associated with the ability of an individual person to control access by others to information about

[1] See, for example, Lee Rainie, Janna Anderson, and Jennifer Connolly, *Cyber Attacks Likely to Increase* (Pew Research Internet Project, October 2014), http://www.pewInternet.org/2014/10/29/cyber-attacks-likely-to-increase/.

[2] The term *cyberspace* usually refers to the worldwide collection of connected ICT components, the information that is stored in and flows through those components, and the ways that information is structured and processed.

[3] For a more in-depth discussion of this concept, see CRS Report RL32777, *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options*, by Eric A. Fischer.

that person. Thus, good cybersecurity can help protect privacy in an electronic environment, but information that is shared to assist in cybersecurity efforts might sometimes contain personal information that at least some observers would regard as private. Cybersecurity can be a means of protecting against undesired surveillance of and gathering of intelligence from an information system. However, when aimed at potential sources of cyberattacks, such activities can also be useful to help effect cybersecurity. In addition, surveillance in the form of monitoring of information flow within a system can be an important component of cybersecurity.[4]

Management of Cybersecurity Risks

The risks associated with any attack depend on three factors: *threats* (who is attacking), *vulnerabilities* (the weaknesses they are attacking), and *impacts* (what the attack does). The management of risk to information systems is considered fundamental to effective cybersecurity.[5]

What Are the Threats?

People who actually or potentially perform cyberattacks are widely cited as falling into one or more of five categories: *criminals* intent on monetary gain from crimes such as theft or extortion; *spies* intent on stealing classified or proprietary information used by government or private entities; *nation-state warriors* who develop capabilities and undertake cyberattacks in support of a country's strategic objectives; "*hacktivists*" who perform cyberattacks for nonmonetary reasons; and *terrorists* who engage in cyberattacks as a form of non-state or state-sponsored warfare.

What Are the Vulnerabilities?

Cybersecurity is in many ways an arms race between attackers and defenders. ICT systems are very complex, and attackers are constantly probing for weaknesses, which can occur at many points. Defenders can often protect against weaknesses, but three are particularly challenging: inadvertent or intentional acts by *insiders* with access to a system; *supply chain* vulnerabilities, which can permit the insertion of malicious software or hardware during the acquisition process; and previously unknown, or *zero-day*, vulnerabilities with no established fix. Even for vulnerabilities where remedies are known, they may not be implemented in many cases because of budgetary or operational constraints.

What Are the Impacts?

A successful attack can compromise the confidentiality, integrity, and availability of an ICT system and the information it handles. *Cybertheft* or *cyberespionage* can result in exfiltration of financial, proprietary, or personal information from which the attacker can benefit, often without the knowledge of the victim. *Denial-of-service* attacks can slow or prevent legitimate users from accessing a system. *Botnet* malware can give an attacker command of a system for use in cyberattacks on other systems. Attacks on *industrial control systems* can result in the destruction or disruption of the equipment they control, such as generators, pumps, and centrifuges.

[4] See, for example, Department of Homeland Security, "Continuous Diagnostics and Mitigation (CDM)," June 24, 2014, http://www.dhs.gov/cdm.

[5] See, for example, National Institute of Standards and Technology, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011, http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.

Most cyberattacks have limited impacts, but a successful attack on some components of critical infrastructure (CI)—most of which is held by the private sector—could have significant effects on national security, the economy, and the livelihood and safety of individual citizens. Thus, a rare successful attack with high impact can pose a larger risk than a common successful attack with low impact.

While it is widely recognized that cyberattacks can be costly to individuals and organizations, economic impacts can be difficult to measure, and estimates of those impacts vary widely. An often cited figure for annual cost to the global economy from cybercrime is $400 billion, with some observers arguing that costs are increasing substantially, especially with the continued expansion of ICT infrastructure through the Internet of Things and other new and emerging platforms.[6] The costs of cyberespionage can be even more difficult to quantify but are considered to be substantial.[7]

Managing the risks from cyberattacks usually involves (1) removing the threat source (e.g., by closing down botnets or reducing incentives for cybercriminals); (2) addressing vulnerabilities by hardening ICT assets (e.g., by patching software and training employees); and (3) lessening impacts by mitigating damage and restoring functions (e.g., by having back-up resources available for continuity of operations in response to an attack). The optimal level of risk reduction will vary among sectors and organizations. For example, the level of cybersecurity that customers expect may be lower for a company in the entertainment sector than for a bank, a hospital, or a government agency.

Federal Role

The federal role in cybersecurity involves both securing federal systems and assisting in protecting nonfederal systems. Under current law, all federal agencies have cybersecurity responsibilities relating to their own systems, and many have sector-specific responsibilities for CI. More than 50 statutes address various aspects of cybersecurity.

Figure 1 is a simplified schematic diagram of major agency responsibilities in cybersecurity. In general, the National Institute of Standards and Technology (NIST) develops standards that apply to federal civilian ICT under the Federal Information Security Modernization Act (FISMA), and the Office of Management and Budget (OMB) is responsible for overseeing their implementation. The Department of Defense (DOD) is responsible for military ICT, defense of the nation in cyberspace, and, through the National Security Agency (NSA), security of national security systems (NSS), which handle classified information. NSA is also part of the Intelligence Community (IC). The Department of Homeland Security (DHS) has operational responsibility for protection of federal civilian systems and is the lead agency coordinating federal efforts assisting the private sector in protecting CI assets. It is also the main federal focus of information sharing for civilian systems through its National Cybersecurity and Communications Integration Center (NCCIC). The Department of Justice (DOJ) is the lead agency for enforcement of relevant laws.

[6] See, for example, Center for Strategic and International Studies, "Net Losses: Estimating the Global Cost of Cybercrime" (McAfee, June 2014), http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf?cid=BHP028; Cybersecurity Ventures, "Cybersecurity Market Report, Q2 2016," 2016, http://cybersecurityventures.com/cybersecurity-market-report/. For more information on the Internet of Things, see CRS Report R44227, *The Internet of Things: Frequently Asked Questions*, by Eric A. Fischer.

[7] Office of the National Counterintelligence Executive, "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011," October 2011, https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf.

Figure 1. Simplified Schematic Diagram of Federal Agency Cybersecurity Roles

Source: CRS.

Notes: DHS: Department of Homeland Security; DOD: Department of Defense; DOJ: Department of Justice; FISMA: Federal Information Security Management Act; IC: Intelligence Community; NIST: National Institute of Standards and Technology; NSA: National Security Agency; OMB: Office of Management and Budget; R&D: Research and development.

In February 2015, the Obama Administration also established, via presidential memorandum, the Cyber Threat Intelligence Integration Center (CTIIC) under the Director of National Intelligence (DNI). Its purposes are to provide integrated analysis on cybersecurity threats and incidents affecting national interests across the federal government and to support relevant government entities, including the NCCIC and others at DOD and DOJ.

Federal Spending

Federal agencies spend a significant part of their annual IT funding on cybersecurity, which currently constitutes 16-17% (about one in every seven dollars) of agency IT budgets overall (**Table 1**). However, DOD spending accounts for a large proportion of that expenditure, ranging from 22% to 30% of the DOD IT budget from FY2010 to FY2015. The median proportion for other agencies has been 6%-7% during that period. That is roughly equivalent to spending patterns for businesses of 4%-9% reported in a recent survey.[8]

The FY2017 budget request includes over $19 billion altogether for cybersecurity. With a total requested IT investment of $81.6 billion, that would amount to a proportion of 23.3%, or about one in every four dollars, to be spent on cybersecurity. For more information on federal cybersecurity spending, see CRS Report R44404, *Perspectives on Federal Cybersecurity Spending*, by William L. Painter and Chris Jaikaran.

Table 1. Federal FISMA and IT Spending

Billions of Dollars, FY2006 to FY2015

Fiscal Year	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
FISMA Spending	5.5	5.9	6.2	6.8	12.0	13.3	14.6	10.3	12.7	13.1
Total IT Spending	66.2	68.2	72.8	76.1	80.7	76.0	75.0	73.2	75.6	80.4
FISMA Proportion of Total IT Spending (%)	*8.3*	*8.7*	*8.5*	*8.9*	*14.9*	*17.5*	*19.3*	*14.1*	*16.8*	*16.3*

Source: Data on FISMA spending are from annual reports on implementation of FISMA from the Office of Management and Budget (OMB), many of which are available at http://www.whitehouse.gov/omb/e-gov/docs. Data on total IT spending are from OMB Exhibit 53 spreadsheets (see Office of Management and Budget, "Exhibit 53 Archive," Federal IT Dashboard, August 31, 2014, https://itdashboard.gov/exhibit53report, for recent documents).

Notes: FISMA data for FY2006-FY2009 are not comparable to later data, and data from 2013-2015 are not comparable to earlier data, because of changes in how OMB collected the information implemented in 2010 and again in 2013. Amounts for both FISMA and IT spending are reported in the documents as "actual" expenditures and therefore probably consist mostly of obligated funds. Federal documents provide data as IT, not ICT, spending, but include investments in activities such as telecommunications (Office of Management and Budget, "Guidance on Exhibit 53—Information Technology and E-Government," August 5, 2011, http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy13_guidance_for_exhibit_53-a-b_20110805.pdf). FISMA spending may not fully account for all agency investment in cybersecurity. Agencies might not report funds spent on cybersecurity beyond what FISMA requires in their submissions that are summarized in the annual FISMA reports. Therefore, the total amounts spent on cybersecurity might exceed the amounts presented in the table.

Legislative Proposals and Actions

Since at least the 111th Congress, many bills have been introduced that would address a range of cybersecurity issues:

- **Cybercrime Laws**—updating criminal statutes and law-enforcement authorities relating to cybersecurity.

[8] Barbara Filkins, "IT Security Spending Trends" (SANS Institute, February 2016), https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697. The results are from a survey of 169 organizations across several sectors that found median proportions of 4%-6% for FY2014 and 7%-9% for FY2016.

- **Data-Breach Notification**—requiring notification to victims and other responses after data breaches involving personal or financial information of individuals.
- **FISMA Reform**—updating the law to reflect changes in ICT and the threat landscape.
- **Information Sharing**—easing access of the private sector to classified and unclassified threat information and removing barriers to sharing within the private sector and with the federal government.
- **Internet of Things**—addressing a range of cybersecurity issues arising from the proliferation of devices and objects (such as home appliances, automobiles, medical devices, factories, and infrastructure) connected to the Internet.
- **Privately Held CI**—improving protection of private sector CI from attacks with major impacts.
- **R&D**—updating agency authorizations and strategic planning requirements.
- **Workforce**—improving the size, skills, and preparation of the federal and private sector cybersecurity workforce.

Table 2. Cybersecurity Bills Enacted in the 113th and 114th Congresses

Public Law	Bill No.	Title
P.L. 113-246	H.R. 2952	Cybersecurity Workforce Assessment Act
P.L. 113-274	S. 1353	Cybersecurity Enhancement Act of 2014
P.L. 113-277	S. 1691	Border Patrol Agent Pay Reform Act of 2014
P.L. 113-282	S. 2519	National Cybersecurity Protection Act of 2014
P.L. 113-283	S. 2521	Federal Information Security Modernization Act of 2014
P.L. 114-113	H.R. 2029	Cybersecurity Act of 2015 (Division N), including Cybersecurity Information Sharing Act (Title I) National Cybersecurity Protection Advancement Act of 2015 (Subtitle A of Title II) Federal Cybersecurity Enhancement Act of 2015 (Subtitle B of Title II) Federal Cybersecurity Workforce Assessment Act of 2015 (Title III) Title IV—Other Cyber Matters

Source: CRS.

Note: The Cybersecurity Act of 2015 is Division N of P.L. 114-113, the Consolidated Appropriations Act, 2016.

Laws enacted in the 113th and 114th Congresses (**Table 2**) have focused on all of those issues to varying degrees:

- **Critical Infrastructure**
  P.L. 113-274 established a process led by the National Institute of Standards and Technology (NIST) similar to one created in Executive Order 13636 to develop a cybersecurity framework, a common set of practices for protection of CI.
  P.L. 113-282 requires DHS to develop and exercise incident-response plans for cybersecurity risks to CI.
  P.L. 114-113, Title IV, requires DHS and NIST to assist states in improving cybersecurity for emergency response networks. It also requires the Department of Health and Human Services to establish a task force and collaboration mechanisms to assist the healthcare sector in reducing cybersecurity risks.

- **Data-Breach Notification**
  P.L. 113-283 requires OMB to establish procedures for notification and other responses to federal agency data breaches of personal information.
- **Federal Information Systems**
  P.L. 113-283 retains, with some amendments, most provisions of FISMA, which was originally enacted in 2002. Changes include providing statutory authority to DHS for overseeing operational cybersecurity of federal civilian information systems, and requiring agencies to implement DHS directives.
  P.L. 114-113, Title II, Subtitle B establishes in statute the DHS intrusion-protection program known as EINSTEIN; requires agencies to adopt it and implement additional cybersecurity measures; gives DHS additional authority in the event of an imminent threat or emergency; and establishes additional reporting requirements.
  P.L. 114-113, Title IV, also requires reports to Congress: from DHS on the security of mobile devices used by federal agencies, and from agency inspectors general on the cybersecurity of NSS and systems providing access to personally identifiable information.
- **Information Sharing**
  P.L. 113-282 provided statutory authority for NCCIC, which had been created by DHS in 2009 under existing statutory authority to provide and facilitate information sharing and incident response among public and private-sector CI entities.
  P.L. 114-113, Title I, facilitates public- and private-sector sharing of information on cyberthreats and defensive measures and permits private-sector entities to monitor and operate defenses on their information systems.
  P.L. 114-113, Title II, Subtitle A, expands the functions and modifies the responsibilities of the NCCIC and establishes additional reporting requirements.
- **International and Cybercrime**
  P.L. 114-113, Title IV, requires, from the Department of State, an international cyberspace policy and international consultations on measures against cybercriminals. It also broadens cybercrime penalties to cover specified offenses occurring outside U.S. territory.
- **R&D**
  P.L. 113-274 requires a multiagency strategic plan for cybersecurity R&D and specifies areas of research for NSF.
- **Workforce**
  P.L. 113-246 requires an assessment by DHS of its cybersecurity workforce and development of a workforce strategy;
  P.L. 113-274 provides statutory authority for an existing NSF scholarship and recruitment program to build the federal cybersecurity workforce, as well as competitions and a study of existing education and certification programs;
  P.L. 113-277 provides additional DHS hiring and compensation authorities and requires a DHS assessment of workforce needs.
  P.L. 114-113, Title III, requires the Office of Personnel Management (OPM) to establish and implement an employment-code structure for federal cybersecurity personnel, and it sets reporting requirements.

With respect to cybercrime and data-breach notification, more comprehensive legislation has been introduced in recent Congresses but has not been enacted. Ongoing controversies relating to

cybercrime include the balance between providing adequate penalties and authorities, on the one hand, and ensuring protection of privacy and civil liberties, on the other (for more information, see CRS Report R44481, *Encryption and the "Going Dark" Debate*, by Kristin Finklea; CRS Report R44036, *Stored Communications Act: Reform of the Electronic Communications Privacy Act (ECPA)*, by Richard M. Thompson II and Jared P. Cole). With respect to data-breach notification, much of the debate involves how best to harmonize federal and state standards, and what precautions and responses should be required from organizations holding sensitive information such as financial or personal data of customers (see CRS Report R44326, *Data Security and Breach Notification Legislation: Selected Legal Issues*, by Alissa M. Dolan). Debate about the cybersecurity of the Internet of Things involves a broad range of issues that vary among sectors and applications (see CRS Report R44227, *The Internet of Things: Frequently Asked Questions*, by Eric A. Fischer).

Other legislation with more limited cybersecurity provisions has also been enacted in the 114th Congress. Notably, the annual defense reauthorization act, P.L. 114-92, contains cybersecurity provisions relating to DOD.

Altogether, more than 150 bills have been introduced in the 114th Congress that would address various cybersecurity issues, with more than a dozen receiving committee or floor action. For two of the issues discussed above—data-breach notification and revision of cybercrime laws—in addition to the bills that have been introduced, the Obama Administration has also released legislative proposals.

Executive Branch Actions

Some notable actions have been taken by the Obama Administration during the 114th Congress. Some of the provisions in the enacted legislation provided statutory authority for programs or activities previously established through executive action. In addition to the NCCIC (P.L. 113-282), examples include the Scholarship for Service program and the NIST cybersecurity framework process (P.L. 113-274), as well as the EINSTEIN intrusion-protection program for federal agencies (P.L. 114-113). The Administration has also taken steps to implement enacted provisions.

Additional actions include the following:

- Executive Order 13691 set up mechanisms to promote the widespread use of information sharing and analysis organizations and the development of standards for their establishment and operation.
- Subsequent to significant data breaches, such as the 2015 exfiltration of records from the Office of Personnel Management (see CRS Report R44111, *Cyber Intrusion into U.S. Office of Personnel Management: In Brief*, coordinated by Kristin Finklea), and other concerns, the Administration announced a cybersecurity national action plan to implement strategies to enhance U.S. cybersecurity nationwide. Initiatives in the plan include a proposed revolving fund for modernizing federal IT (see H.R. 4897 and H.R. 5792) and the appointment of a federal chief information security officer, among other actions.
- Presidential Policy Directive 41 describes how the federal government will respond to cybersecurity incidents affecting government and private-sector entities, including principles, kinds of response, a framework of roles and responsibilities, and coordination.

Long-Term Challenges

The legislative and executive-branch actions discussed above are largely designed to address several well-established near-term needs in cybersecurity: preventing cyber-based disasters and espionage, reducing impacts of successful attacks, improving inter- and intrasector collaboration, clarifying federal agency roles and responsibilities, and fighting cybercrime. However, those needs exist in the context of more difficult long-term challenges relating to design, incentives, consensus, and environment (DICE):

Design: Experts often say that effective security needs to be an integral part of ICT design. Yet, developers have traditionally focused more on features than security, for economic reasons. Also, many future security needs cannot be predicted, posing a difficult challenge for designers.

Incentives: The structure of economic incentives for cybersecurity has been called distorted or even perverse. Cybercrime is regarded as cheap, profitable, and comparatively safe for the criminals. In contrast, cybersecurity can be expensive, is by its nature imperfect, and the economic returns on investments are often unsure.

Consensus: Cybersecurity means different things to different stakeholders, often with little common agreement on meaning, implementation, and risks. Substantial cultural impediments to consensus also exist, not only between sectors but within sectors and even within organizations. Traditional approaches to security may be insufficient in the hyperconnected environment of cyberspace, but consensus on alternatives has proven elusive.

Environment: Cyberspace has been called the fastest evolving technology space in human history, both in scale and properties. New and emerging properties and applications—especially social media, mobile computing, big data, cloud computing, and the Internet of Things—further complicate the evolving threat environment, but they can also pose potential opportunities for improving cybersecurity, for example through the economies of scale provided by cloud computing and big data analytics.

Legislation and executive actions in the 114th and future Congresses could have significant impacts on those challenges. For example, cybersecurity R&D may affect the design of ICT, cybercrime penalties may influence the structure of incentives, the NIST framework may facilitate achievement of a consensus on cybersecurity, and federal initiatives in cloud computing and other new components of cyberspace may help shape the evolution of cybersecurity.

Author Information

Eric A. Fischer
Senior Specialist in Science and Technology

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other

than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.