



**Statement of Eric A. Fischer
Senior Specialist in Science and Technology
Congressional Research Service**

Before

**Committee on Oversight and Government Reform
U.S. House of Representatives**

April 22, 2015

on

“Enhancing Cybersecurity of Third-Party Contractors and Vendors”

Chairman Chaffetz, Ranking Member Cummings, and distinguished Members of the Committee:

Thank you for the opportunity to discuss issues related to cybersecurity with you today. As the Committee requested, my testimony will provide an overview of the federal role in cybersecurity, current issues and needs, and long-term challenges the federal government faces in this area, including with respect to the roles of third parties.

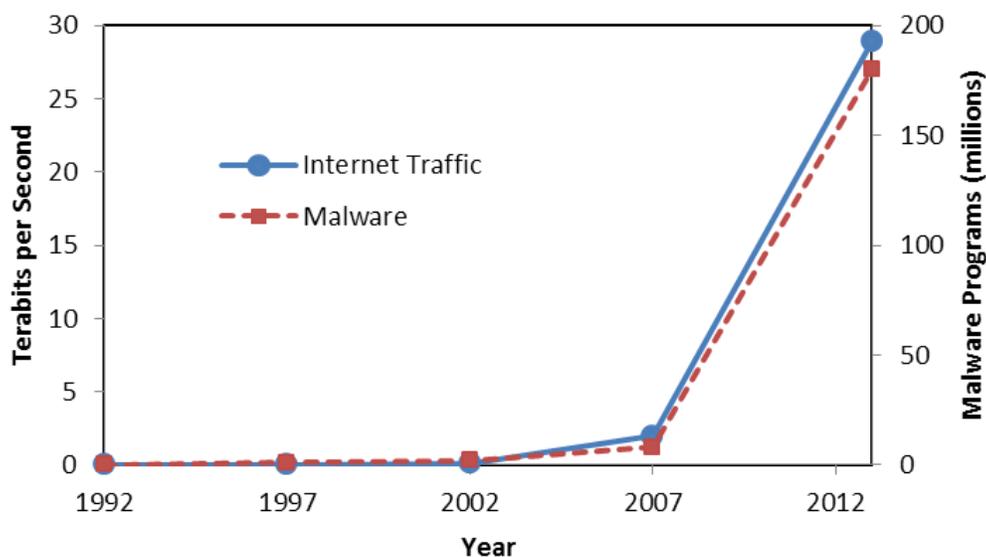
Both the responsibilities and the needs of the federal government with respect to cybersecurity have changed over the last several decades in response to the rapid expansion and evolution of the information technology (IT) industry over that period. The era of mainframe computers began in the 1950s. It was not until the mid-1970s, more than 25 years later, that personal computers began to see widespread use. Internet browser programs and the world-wide web did not appear until the 1990s. Since then, 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. As a result of that and other factors, the last 15 years has seen the rise of cloud computing, big-data analytics, social media, mobile computing, and the Internet of Things.

The original IT industry has also increasingly converged with the communications industry into what is 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.

Over the past several years, experts and policy makers have expressed increasing concerns about protecting ICT systems from *cyberattacks*—deliberate, unauthorized attempts to access the 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. In

fact, over the past ten years, both the amount of global Internet traffic and the number of malicious software programs have grown exponentially (**Figure 1**).

Figure 1. Internet Traffic and Malware



Sources: Internet traffic: Cisco, *The Zettabyte Era: Trends and Analysis*, June 10, 2014, http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.pdf. Malware programs: AV-TEST, "Malware Statistics & Trends Report," April 9, 2015, <http://www.av-test.org/en/statistics/malware/>.

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 umbrella term but tends to defy precise consensus definition. Generally speaking, it refers to various measures intended to protect ICT components and content—collectively known as *cyberspace*¹—from cyberattacks. Cyberspace includes computers and other ICT devices, related hardware and software, the networks that connect them, and the information they contain and communicate. Cybersecurity can also refer to the state or quality of being protected from such attacks, or to the broad field of endeavor aimed at implementing and improving protection.

Cybersecurity is also sometimes conflated 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 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 data 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,

¹ 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 (CRS Report RL32777, *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options*, by Eric A. Fischer).

when aimed at potential sources of cyberattacks, such surveillance and information-gathering 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.²

Overview of Federal Agency Cybersecurity Activities

The federal role in cybersecurity is complex. It involves both securing federal systems and assisting in the protection of nonfederal systems. No single overarching framework legislation is in place, but many enacted statutes—more than 50—address various aspects of cybersecurity.³ Under the Federal Information Security Management Act (FISMA, 44 U.S.C. Chapter 35, Subchapter II, as amended by P.L. 113-256), all federal agencies have cybersecurity responsibilities relating to their own systems. Responsibility for other cybersecurity functions is distributed among several federal agencies under FISMA and other statutes. Among those functions⁴ are the following:

- performing and supporting *research and development* (R&D);
- developing *technical standards*;
- providing *technical support* in cybersecurity to government and private-sector entities, especially critical infrastructure (CI) entities;
- engaging in electronic surveillance and other *intelligence-gathering* activities to detect cyberthreats;
- performing and coordinating *information sharing* to facilitate protection and mitigate the impacts of incidents;
- engaging in investigations of cybercrime and other *law enforcement* activities;
- developing and enforcing federal *cybersecurity* regulations; and
- preparing for and engaging in *cybercombat*.

Figure 2 provides a simplified schematic diagram of major agency responsibilities in cybersecurity. Below is a brief description of roles for selected agencies that may be of interest to the committee, especially agencies with activities that go beyond the requirements of each to secure its own systems. The description is a highly simplified overview of major roles, drawn from various sources. It is intended to provide a basic sketch of functions and responsibilities. Because of the increasing ubiquity of information technology and its merger with communications technology, the increasing complexity of cyberspace, the continuing evolution of agency roles, and the lack of consensus about what specifically constitutes cybersecurity,

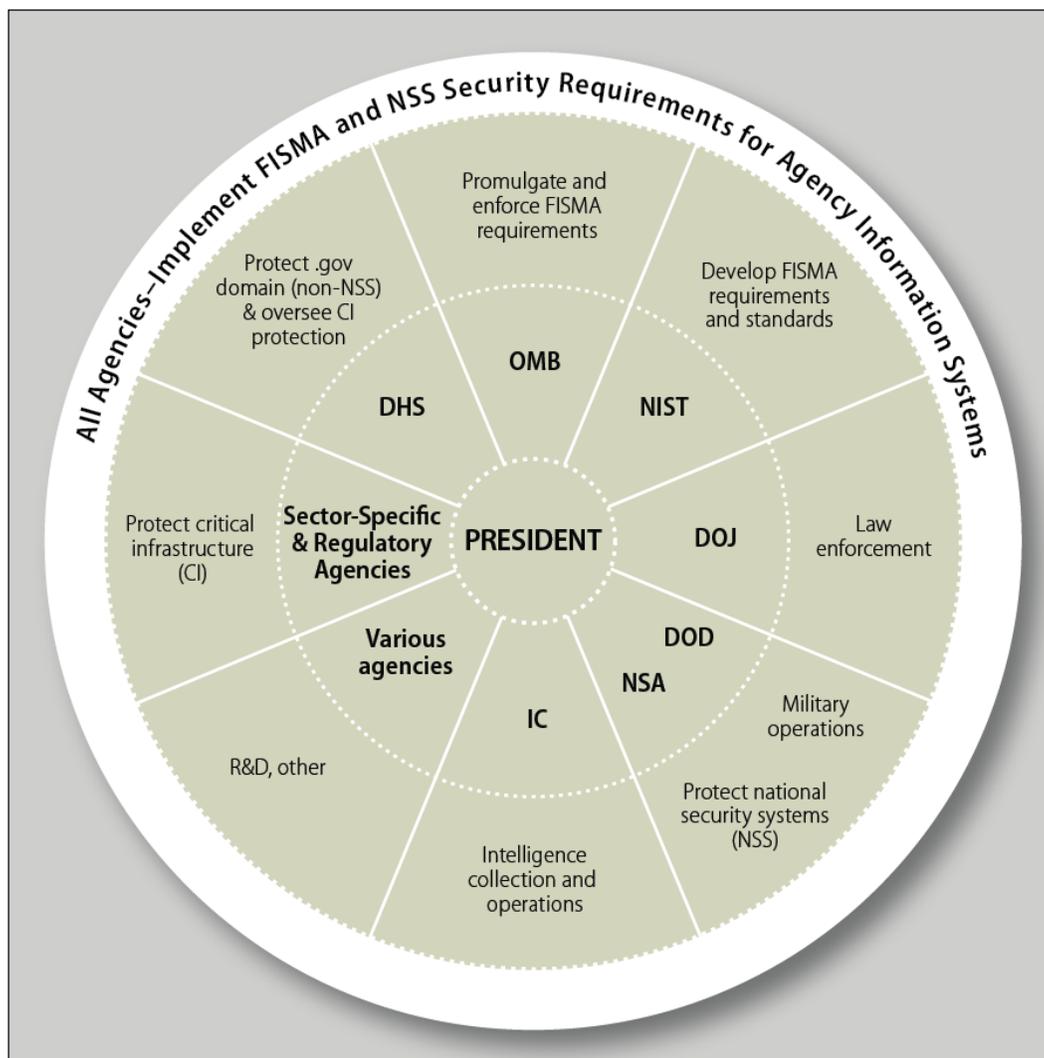
² See, for example, Department of Homeland Security, “Continuous Diagnostics and Mitigation (CDM),” June 24, 2014, <http://www.dhs.gov/cdm>.

³ CRS Report R42114, *Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation*, by Eric A. Fischer.

⁴ The functions are not necessarily mutually exclusive. For example, development of technical standards often involves R&D.

among other factors, the actual distribution of responsibilities is far more complex and in some ways may be more ambiguous than what is presented here.

Figure 2. Simplified Schematic Diagram of Federal Agency Cybersecurity Roles



Source: CRS

OMB — Office of Management and Budget. Under current law, in addition to its budgetary role in federal cybersecurity efforts, this White House office is responsible for promulgating and enforcing information security requirements under FISMA for federal information systems other than national security systems (NSS) and information systems in the Department of Defense (DOD) and Intelligence Community (IC) agencies that are crucial to their missions.

NIST — National Institute of Standards and Technology. This bureau within the Department of Commerce develops the standards that OMB promulgates under FISMA. It also performs research relating to cybersecurity, develops voluntary guidance, and works with government and private-sector entities to develop cybersecurity best practices.

DHS — Department of Homeland Security. While federal responsibilities for the cybersecurity of non-NSS systems are distributed among several agencies, FISMA, as amended by P.L. 113-256, provides DHS primary responsibility for coordinating the operational security of federal systems.⁵ In addition, DHS oversees federal efforts to coordinate and improve the protection of U.S. critical infrastructure (CI), most of which is controlled by the private sector. Some notable DHS cybersecurity programs and activities include the following:

- The Cybersecurity Division of the Science and Technology Directorate,⁶ established in 2011, focuses on developing and delivering new cybersecurity technologies and other tools in coordination with public- and private-sector partners.
- The National Cybersecurity and Communications Integration Center (NCCIC),⁷ established administratively in 2009 under existing statutory authority to provide and facilitate information sharing and incident response among public and private-sector CI entities. It received specific statutory authorization in P.L. 113-282, the *National Cybersecurity Protection Act of 2014*.
- The National Cybersecurity Protection System (NCPS) and its EINSTEIN component, which provide capabilities for intrusion prevention and detection, analysis, and information sharing for cybersecurity of federal civilian systems.
- The Enhanced Cybersecurity Services (ECS) program, established pursuant to Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, and through which DHS provides private-sector CI entities with sensitive and classified cyberthreat information either directly or through providers of commercial Internet services.
- The Continuous Diagnostics and Mitigation (CDM) program, which provides products and services to agencies to implement CDM, including sensors, tools, dashboards, and other assistance.

DOD — Department of Defense. DOD is responsible for military operations in cyberspace. That includes both defensive and offensive operations, with the U.S. Cyber Command, under the U.S. Strategic Command, serving as the main focus for coordinating and conducting such activities.⁸ DOD agencies such as the Defense Advanced Research Projects Agency (DARPA) and the National Security Agency (NSA) also engage in cybersecurity research and development (R&D). NSA and other DOD agencies also provide assistance upon request to DHS, other civilian

⁵ The Obama administration had delegated such responsibilities to DHS in 2010 (Peter R. Orszag and Howard A. Schmidt, “Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS),” Office of Management and Budget, Memorandum for Heads of Executive Departments and Agencies M-10-28, July 6, 2010, http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-28.pdf).

⁶ Department of Homeland Security, “Cyber Security Division,” January 22, 2015, <http://www.dhs.gov/science-and-technology/cyber-security-division>.

⁷ NCCIC is usually pronounced “En-kick.”

⁸ CRS Report R43848, *Cyber Operations in DOD Policy and Plans: Issues for Congress*, by Catherine A. Theohary and Anne I. Harrington.

agencies, and private sector entities under various agreements. DOD also offers scholarship opportunities in cybersecurity at selected institutions to recruit and retain qualified personnel.

IC — Intelligence Community. The IC consists of 17 federal agencies and other entities responsible for various forms of intelligence collection and operations, including those relating to cybersecurity.⁹ The Director of National Intelligence sets standards for mission-critical IC systems other than NSS.

*NSA — National Security Agency.*¹⁰ While NSA is a major component of the IC, it also has a significant cybersecurity mission, serving as the designated manager of national security systems (NSS), which are information and telecommunications systems that are used in military, intelligence, and other national security activities or that handle classified information. This includes the development of security standards. NSA, along with DHS, is also involved in designation of academic centers of excellence in cybersecurity.

DOE—Department of Energy. DOE supports cybersecurity efforts in the energy sector, including electricity and nuclear, for example by assisting private-sector energy companies in developing cybersecurity capabilities for energy-delivery systems. It also provides some cybersecurity services to other agencies and private-sector entities through the DOE National Laboratories and other means. Several of DOE's 17 national laboratories also engage in cybersecurity R&D, education and training, and other activities. These include such things as modeling and simulation of systems and networks, forensic analyses, and providing test beds for investigating and improving the security of industrial control systems.

DOJ — Department of Justice. Most enforcement of federal criminal laws relating to cybersecurity, including investigation and prosecution, is carried out by DOJ. However, some entities within other departments also have enforcement responsibilities, such as the Secret Service in the Department of Homeland Security (DHS), and the Defense Criminal Investigative Organizations within DOD. The duties of law-enforcement agencies often involve computer forensics, electronic surveillance, and other technological activities. The Federal Bureau of Investigation (FBI) leads the multiagency National Cyber Investigative Joint Task Force (NCIJTF), which focuses on information sharing and analysis relating to cyberthreats for law enforcement purposes.

OSTP—Office of Science and Technology Policy. This White House office coordinates and facilitates interagency and multiagency cybersecurity activities, especially R&D.

NSF—National Science Foundation. This independent agency funds research and education in cybersecurity, largely through academic and nonprofit institutions. NSF also provides scholarships to train cybersecurity professionals through its Scholarship-for-Service program, established administratively in 2001 under existing statutory authority and receiving specific statutory authorization in P.L. 113-274.

⁹ See CRS Report RL33539, *Intelligence Issues for Congress*, by John W. Rollins.

¹⁰ Administratively, NSA is part of DOD but is listed separately because of its unique cybersecurity responsibilities.

SSAs — Sector-Specific Agencies. SSAs are those federal agencies responsible for leading public/private collaborative efforts to protect the 16 designated CI sectors.¹¹ A plan has been developed for each sector, and many of those plans include discussion of cybersecurity concerns and activities for the different sectors.¹²

Regulatory Agencies. The regulatory environment for cybersecurity is complex, involving both technical and nontechnical activities by various agencies.¹³

Agency Investment in Cybersecurity

As shown in **Table 1**, federal agencies invested a total of \$66 billion in IT in FY 2006. That investment had grown to \$80 billion in nominal dollars by FY 2014, for an average annual growth rate of 2.7%. The rate of growth in spending on cybersecurity has been several times higher, increasing from \$8.3 billion in FY2006 to \$12.7 billion in FY2014, for an annual growth rate of 11%.

Table 1. Federal FISMA and Information Technology (IT) Spending
Billions of Dollars, FY2006 to FY2014

Fiscal Year	2006	2007	2008	2009	2010	2011	2012	2013	2014
FISMA Spending	5.5	5.9	6.2	6.8	12.0	13.3	14.6	10.3	12.7
Total IT Spending	66.2	68.2	72.8	76.1	80.7	76.0	75.7	73.2	81.9
<i>FISMA as a Proportion of Total IT Spending (%)</i>	8.3	8.7	8.5	8.9	14.9	17.5	19.3	13.8	12.7

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). The first year for which CRS has data on both FISMA spending and IT investment is FY2006, and the most recent is FY2014.

Note: As indicated by the vertical lines, FISMA data for FY2006-FY2009 are not comparable to later data, and data from 2013 are not comparable to earlier data, because of changes in how OMB collected the information (see text). Amounts for both FISMA and IT spending are reported in the documents as “actual” expenditures and therefore probably consist mostly of obligated funds.

¹¹ The White House, “Critical Infrastructure Security and Resilience,” Presidential Policy Directive 21, (February 12, 2013), <http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

¹² See Department of Homeland Security, “Sector-Specific Plans,” 2012, http://www.dhs.gov/files/programs/gc_1179866197607.shtm.

¹³ See, for example, Government Accountability Office, *Information Technology: Federal Laws, Regulations, and Mandatory Standards for Securing Private Sector Information Technology Systems and Data in Critical Infrastructure Sectors*, GAO-08-1075R, (September 16, 2008), <http://www.gao.gov/assets/100/95747.pdf>. The report identified legal cybersecurity requirements associated with specific federal agencies for nine CI sectors, pertaining specifically to securing privately owned information technology systems in those sectors.

The growth rate as shown in the table may be higher than the actual growth because of changes in how data were reported, but it is nevertheless likely that the actual rate of growth in cybersecurity spending has been substantially higher than that in IT investment overall. The large increase from FY2009 to FY2010 and the marked decrease from FY2012 to FY2013 do not appear to reflect actual changes in cybersecurity spending in those years. OMB changed the way it collected the data beginning with FY2010, when it introduced a separate form (Exhibit 53B) on which agencies were required to report detailed FISMA spending.¹⁴ Before that, agencies reported the data as a simple percentage of their overall IT investment.¹⁵ Therefore, data from FY2006 to FY2009 are not comparable to those from FY2010 to FY2013. The amplitude of the reported 75% increase in FISMA spending from FY2009 to FY2010 is almost certainly an artifact of the change in reporting method. It is possible that a real increase occurred, but the size and direction of any change during that period could not be determined. Similarly, the reported decrease of 30% in FISMA spending from FY2012 to FY2013 appears likely to be an artifact largely of additional changes in reporting requirements.¹⁶ According to OMB,

Prior to FY 2013, government-wide information security spending data was collected using a variety of methodologies, resulting in discrepancies in the figures. Based on conversations among the agencies and with the Hill, there was a decision made to streamline and coordinate the collection and presentation mechanisms to ensure uniformity in the final spending figures.¹⁷

OMB further stated that because of those changes, “comparisons cannot be drawn between the FY2012 and FY2013 information security spending figures” but that “the approach used in FY2013 will be used again for FY2014.”¹⁸ Presumably, out-year data can be meaningfully compared to FY2013 beginning with the FY2014 FISMA report.

Spending on cybersecurity varies greatly among agencies, from less than 5% as a proportion of the agency’s total IT investment for nine of the 24 agencies reporting in FY2014 to more than 20% for three of them—DOD (24%), DHS (22%), and DOJ (22%). With DOD’s mission responsibilities and its large IT budget, accounting for 46% of total federal IT investment, it is

¹⁴ Office of Management and Budget, *Fiscal Year 2010 Report to Congress on Implementation of the Federal Information Security Management Act of 2002*, March 2011, http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/FY10_FISMA.pdf.

¹⁵ Office of Management and Budget, *Fiscal Year 2009 Report to Congress on Implementation of the Federal Information Security Management Act of 2002*, March 2010, http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/FY09_FISMA.pdf.

¹⁶ “Since publishing the FY 2012 FISMA report, OMB has worked internally and with agencies to streamline and improve reporting of this spending information” (Office of Management and Budget, *Annual Report to Congress: Federal Information Security Management Act*, May 1, 2014, 30, http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy_2013_fisma_report_05.01.2014.pdf).

¹⁷ Allie Neill, Legislative Affairs, OMB, email message to author, November 6, 2014.

¹⁸ *Ibid.*

not surprising that DOD's spending on cybersecurity accounted for 70% of the federal total in FY2014, compared to 11% for DHS and 5% for DOJ.¹⁹

There appears to be widespread consensus that the U.S. government, as one of the largest procurers of IT products and services, can and should use its share of that market to leverage improvements not only in federal cybersecurity but across the broader market. A large proportion of federal IT spending is for procurement and acquisition of products and services. For example, in FY2008, from a total investment of \$72.8 billion, procurement costs for IT products and services totaled \$37.9 billion, about 7% of federal spending on all procurement (\$537.8 billion). Half of federal IT products and services overall were procured by the Department of Defense (DOD), followed in order by the Department of Homeland Security (DHS) at 8%, and the General Services Administration (GSA) and the Department of Health and Human Services (DHHS) at about 6% each. About three-quarters of total IT procurement funding consisted of services rather than products.²⁰

The 2013 cybersecurity executive order (E.O. 13636)²¹ required the General Services Administration (GSA) and Department of Defense (DOD) to make recommendations on including cybersecurity standards in acquisition requirements. Those recommendations covered a range of topics, including acquisition strategies and practices, contract requirements, and training.²² FISMA also gives agency heads responsibility for ensuring the cybersecurity of "information systems used or operated...by a contractor of an agency or other organization on behalf of an agency" (44 U.S.C. 2554). In addition to its FISMA standards and guidelines for such systems, NIST has also developed a draft publication with recommended requirements for agencies to use in ensuring the protection of controlled but unclassified information residing on nonfederal information systems.²³

¹⁹ The data for NSF is an anomaly, as the agency reported \$163 million in FISMA spending for FY2014 but only \$101 million in total IT investment. Presumably, this apparent discrepancy is a reporting artifact reflecting NSF expenditures in extramural research, given that the amounts reported for FY2012, before the reporting changes, were \$14 million in FISMA spending and \$103 million in IT investment.

²⁰ These figures are from analysis by CRS of data for 2009 from the Federal Procurement Data System (FPDS-NG), <https://www.fpds.gov>. The funding amounts are for procurement only—they do not include costs for agency personnel. More recent data were not available for this testimony.

²¹ Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," *Federal Register* 78, no. 33 (February 19, 2013): 11737 – 11744, <http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf>. See also CRS Report R42984, *The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress*, by Eric A. Fischer et al.

²² Department of Defense and General Services Administration, *Improving Cybersecurity and Resilience Through Acquisition*, November 2013, http://www.gsa.gov/portal/mediaId/185367/fileName/IMPROVING_CYBERSECURITY_AND_RESILIENCE_THROUGH_ACQUISITION.action.

²³ Ron Ross et al., *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, NIST Special Publication 800-171, Final Public Draft, (April 2015), http://csrc.nist.gov/publications/drafts/800-171/sp800_171_second_draft.pdf.

Cybersecurity Issues and Challenges

The risks associated with any cyberattack depend on three factors: *threats* (who is attacking), *vulnerabilities* (how they are attacking), and *impacts* (what the attack does). The management of risk to information systems is considered fundamental to effective cybersecurity.²⁴

Threats. People who perform cyberattacks generally fall 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.

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.

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. *Destructive* attacks can damage computers and other ICT devices, and if directed at *industrial control systems*, can result in the destruction of the equipment they control, such as generators, pumps, and centrifuges.

Most cyberattacks have limited impacts, but a successful attack on some components of CI 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.

Reducing the risks from cyberattacks usually involves (1) removing the threat source (e.g., by closing down botnets²⁵ or reducing incentives for cybercriminals); (2) addressing vulnerabilities by hardening ICT assets (e.g., by patching software and training employees); and (3) lessening

²⁴ 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>.

²⁵ Botnets are basically a form of distributed computing, in which groups of computers or other Internet-enabled devices, called bots or zombies, perform automated tasks in a distributed manner over the Internet. Some bots are benign, but malicious botnets are a major cybersecurity problem. In such botnets, devices are infected with software that allows a controller, called a botmaster or bot herder, to use the devices in an Internet network for malicious purposes, usually without the knowledge or approval of the owner of the device.

impacts by mitigating damage and restoring functions (e.g., by having back-up resources available for continuity of operations in response to an attack).

Cybersecurity often involves highly technical measures, and the structure of ICT systems and of cyberspace is very complex. Therefore, identifying cybersecurity needs and the means to address them can be difficult. However, several near-term cybersecurity needs appear to be fairly well-established and straightforward. They include, for example,

- preventing cyber-based disasters and espionage by removing threats and hardening systems;
- reducing the impacts of successful attacks;
- improving inter- and intrasector collaboration to protect systems, particularly with respect to information sharing;
- clarifying federal agency roles and responsibilities;
- building and maintaining a capable cybersecurity workforce for both the public- and private sectors; and
- fighting cybercrime.

Many current cybersecurity activities are aimed at addressing these and related needs. More than 200 bills that would address such needs were introduced in the last three Congresses. The 113th Congress enacted five bills that arguably address aspects of several of those needs,²⁶ including

- amending FISMA to improve the cybersecurity of federal systems;
- updating of agency authorizations for cybersecurity R&D;
- providing for assessment of cybersecurity workforce needs at DHS and enhancing recruitment and retention capabilities; and
- providing statutory bases for a DHS information-sharing program, a NIST public/private partnership effort to develop best practices for CI cybersecurity, and an NSF program for educating cybersecurity professionals.

Bills not enacted included some that would have provided mechanisms to reduce legal and other barriers to information sharing, revised current federal cybercrime law, or provided a federal standard for notification of data breaches of data held by private-sector entities that contain the personal information of individuals.

The immediate and short-term needs discussed above exist in the context of more difficult long-term challenges. The existence of such challenges has been recognized by various observers over many years. For example, the 2008 Comprehensive National Cybersecurity Strategy recognized a need for the development of long-term strategic options and the need to identify “grand

²⁶ In addition to P.L. 113-256, P.L. 113-274, and P.L. 113-282 discussed above, Congress also enacted P.L. 113-246, the *Cybersecurity Workforce Assessment Act*, and P.L. 113-248, the *Border Patrol Agent Pay Reform Act of 2014*. The bills both provide for assessments of the DHS cybersecurity workforce, and the latter provides DHS with new authorities to establish cybersecurity positions and set compensation for them.

challenges” to address difficult cybersecurity problems.²⁷ The 2011 NSTC strategic plan for cybersecurity R&D recognized the need to develop cybersecurity principles that would endure changes in both technologies and threats.²⁸ Such challenges can be characterized in many different ways. One approach that may be useful is to characterize a particular set of difficult challenges that could be used to inform longer-term government and private-sector activities. One such set consists of four challenges: design, incentives, consensus, and environment (DICE).

Design. Experts often say that effective security needs to be an integral part of ICT design, not something that is added on toward the end of the development cycle. Yet, developers have traditionally focused more on features than security, largely for economic reasons. Also, many future security needs cannot be predicted with any certainty, 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. Economic incentives can be influenced by many factors, but one fundamental consideration is the degree to which users demand good cybersecurity as an essential feature of ICT systems and components.

Consensus. Cybersecurity means different things to different stakeholders, 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. Efforts such as the development of the NIST-led Cybersecurity Framework appear to be achieving some improvements in such consensus. However, one fundamental difficulty is that the increasing economic and societal prominence of cyberspace arises to a significant degree from the ability of ICT to connect things in unprecedented and useful ways. In contrast, security traditionally involves separation. Increasingly, cybersecurity experts and other observers are arguing that traditional approaches such as perimeter defense are insufficient, but consensus on a new conceptual framework has yet to emerge.

Environment. Cyberspace has been called the fastest evolving technology space in human history, both in scale and properties. This rapid evolution poses significant challenges for cybersecurity, exacerbating the speed of the “arms race” between attackers and defenders, and arguably providing a significant advantage to the former. 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. In a sense, such developments may provide

²⁷ The White House, “The Comprehensive National Cybersecurity Initiative,” March 5, 2010, <http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative>.

²⁸ National Science and Technology Council, *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*, December 2011, http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf.

defenders with opportunities to shape the evolution of cyberspace toward a state of greater security.

Legislation and executive actions in the 114th Congress 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 Cybersecurity Framework may improve consensus about cybersecurity, and federal initiatives in cloud computing and other new components of cyberspace may help shape the evolution of cybersecurity.

Debate about Federal Agency Roles in Improving Cybersecurity

Ongoing debate about the proper role of government in improving cybersecurity may have significant impacts on legislative developments. In general, that debate has mirrored the broader debate about the role of government. Two examples are described below.

Cybersecurity Regulations

For example, some observers have argued that more government regulation of at least some CI sectors is important for improving their cybersecurity, both to provide incentives for implementation of effective cybersecurity measures and guidance for what kinds of protection should be implemented. Proponents have also argued, among other things, that voluntary approaches have not worked well. They also state that CI sectors and subsectors that are already regulated, in particular financial services and electric power, have been largely successful at improving their cybersecurity as a result at least in part of regulatory requirements, and that opposition to such regulations within the sectors is minimal.

Opponents of increased regulation argue, in contrast, that expanding federal requirements would be costly and ineffective, that better mechanisms exist to enhance cybersecurity, and that given the rate of change in the cyber-technology space, increased regulation would in many cases be too inflexible to be useful and may impede innovation and economic growth and the international competitiveness of American companies. In addition, some have argued that the Cybersecurity Framework may provide sufficient incentives and guidance for CI entities to improve their cybersecurity.

Under Executive Order 13636, the Obama Administration required that certain regulatory agencies engage in consultative review of the framework, determine whether existing cybersecurity requirements are adequate, and report to the President whether the agencies have authority to establish requirements that sufficiently address the risks (it does not state that the agencies must establish such requirements, however), propose additional authority where required, and identify and recommend remedies for ineffective, conflicting, or excessively burdensome cybersecurity requirements.

The assessments of regulatory requirements and proposed actions under the order focused on three agencies: DHS, the Environmental Protection Agency (EPA), and the Department of Health and Human Services (HHS). The Administration concluded that “existing regulatory

requirements, when complemented with strong voluntary partnerships, are capable of mitigating cyber risks to our critical systems and information.”²⁹

Information Sharing

Barriers to the sharing of information on threats, attacks, vulnerabilities, and other aspects of cybersecurity—both within and across sectors—have long been considered by many to be a significant hindrance to effective protection of information systems, especially those associated with CI.³⁰ Examples have included legal barriers, concerns about liability and misuse, protection of trade secrets and other proprietary business information, and institutional and cultural factors—for example, the traditional approach to security tends to emphasize secrecy and confidentiality, which would necessarily impede sharing of information.

Proposals to reduce or remove such barriers, including provisions in legislative proposals in the last two Congresses, have raised concerns,³¹ some of which are related to the purpose of barriers that currently impede sharing. Examples include

- risks to individual privacy and even free speech and other rights;
- use of information for purposes other than cybersecurity, such as unrelated government regulatory actions;
- commercial exploitation of personal information; and
- anticompetitive collusion among businesses that would currently violate federal law.

Research and Development

The need for improvements in fundamental knowledge of cybersecurity and new solutions and approaches has been recognized for well over a decade³² and was a factor in the passage of the Cybersecurity Research and Development Act in 2002 (P.L. 107-305, H.Rept. 107-355). That

²⁹ Michael Daniel, “Assessing Cybersecurity Regulations,” *The White House Blog*, May 22, 2014, <http://www.whitehouse.gov/blog/2014/05/22/assessing-cybersecurity-regulations>. The document notes that the executive order does not apply to independent regulatory agencies.

³⁰ See, for example, CSIS Commission on Cybersecurity for the 44th Presidency, *Cybersecurity Two Years Later*, January 2011, http://csis.org/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf.

³¹ See, for example, Greg Nojeim, “WH Cybersecurity Proposal: Questioning the DHS Collection Center,” *Center for Democracy & Technology*, May 24, 2011, <http://cdt.org/blogs/greg-nojeim/wh-cybersecurity-proposal-questioning-dhs-collection-center>; and Adriane Lapointe, *Oversight for Cybersecurity Activities* (Center for Strategic and International Studies, December 7, 2010), http://csis.org/files/publication/101202_Oversight_for_Cybersecurity_Activities.pdf. See also comments received by a Department of Commerce task force (available at <http://www.nist.gov/itl/cybersecnoi.cfm>) in conjunction with development of this report: Internet Policy Task Force, *Cybersecurity, Innovation, and the Internet Economy* (Department of Commerce, June 2011), http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf.

³² See, for example, National Research Council, *Trust in Cyberspace* (Washington, DC: National Academies Press, 1999), <http://www.nap.edu/catalog/6161.html>.

law focuses on cybersecurity R&D by NSF and NIST. The Homeland Security Act of 2002, in contrast, does not specifically mention cybersecurity R&D. However, DHS and several other agencies make significant investments in it, and several of the cybersecurity bills considered by the last three Congresses would have addressed the role of DHS. About 60% of reported funding by agencies in cybersecurity and information assurance is defense-related (invested by DARPA, NSA, and other defense agencies), with NSF accounting for about 15%, and NIST, DHS, and DOE about 5%-10% each.³³

R&D is generally regarded as one of the less contentious cybersecurity issues. Debate has generally focused on the roles of the agencies involved, priorities relating to specific R&D areas of inquiry, and what are the optimum levels of funding for federal programs.

Other Issues

Other cybersecurity issues that have been considered in recent Congresses include the following:

- **Cybercrime Laws**—updating criminal statutes and law-enforcement authorities relating to cybersecurity. *Controversies:* Adequacy of current penalties and authorities, impacts on privacy and civil liberties.
- **Data-Breach Notification**—requiring notification to victims and other responses after data breaches involving personal or financial information of individuals. *Controversies:* Federal vs. state roles and what responses should be required.
- **Workforce**—improving the size, skills, and preparation of the federal and private-sector cybersecurity workforce. *Controversies:* Hiring and retention authorities, occupational classification, recruitment priorities, and roles of DHS, NSA, NSF, and NIST.

Cybersecurity Bills Enacted in the 113th Congress

Until the 113th Congress, no major cybersecurity legislation had been enacted since 2002. Five bills were signed into law in December 2014 (**Table 2**) addressing aspects of several but not all of the issues discussed above.

They addressed the following issues:

- **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;
- **FISMA Reform:**
P.L. 113-283 retains, with some amendments, most provisions of FISMA; also provides statutory authority to DHS for overseeing operational cybersecurity of federal civilian information systems; requires agencies to implement DHS

³³ The percentages were calculated from data in R&D budget crosscuts available at the Networking And Information Technology Research And Development (NITRD) Program, “Supplements to the President’s Budget,” *NITRD Publications*, 2014, <https://www.nitrd.gov/publications/supplementsall.aspx>.

directives; requires OMB to establish procedures for notification and other responses to data breaches of personal information;

Table 2. Cybersecurity Bills Enacted in the 113th Congress

Public Law	Bill No.	Title
113-246	H.R. 2952	Cybersecurity Workforce Assessment Act
113-274	S. 1353	Cybersecurity Enhancement Act of 2014
113-277	S. 1691	Border Patrol Agent Pay Reform Act of 2014
113-282	S. 2519	National Cybersecurity and Communications Integration Center Act of 2014
113-283	S. 2521	Federal Information Security Modernization Act of 2014

Source: CRS.

- Privately Held CI:**
 P.L. 113-274 establishes a process led by NIST similar to that created in Executive Order 13636 to develop a common set of practices for protection of CI; P.L. 113-282 provides statutory authority and stipulates responsibilities for the NCCIC, which was established by DHS in 2009 under existing statutory authority to provide and facilitate information sharing and incident response among public and private-sector CI entities; also requires DHS to develop and exercise incident-response plans for cybersecurity risks to CI;
- Information Sharing:**
 P.L. 113-282 establishes the NCCIC to provide and facilitate information sharing;
- 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.

Legislation in the 114th Congress

In the 114th Congress, more than 30 bills have been introduced in the House and the Senate that would address several issues, including data-breach notification, incidents involving other nation-states, information sharing, law enforcement and cybercrime, protection of CI, workforce development, and education. The Obama Administration has released proposals for three bills—on information sharing, data-breach notification, and revision of cybercrime laws. Several bills have received or are expected to receive committee or floor action.

Short Narrative Biography

ERIC FISCHER is the Senior Specialist in Science and Technology at the Congressional Research. As a senior policy analyst at CRS, he provides expert written and consultative support to Congress on a broad range of issues in science and technology policy, including cybersecurity, election reform, environment, research and development, and other topics. He has authored more than 30 CRS reports and more than 100 analytical memoranda for congressional offices on those subjects and has provided analytical support to Congress on cybersecurity for more than 10 years. As a Library of Congress official, he also served as head of the former science policy division of CRS and has been active in strategic planning and other management activities at the Library.

Dr. Fischer received a Bachelor of Science degree in biology from Yale University in 1970 and a PhD in zoology from the University of California Berkeley in 1979. After a National Science Foundation Postdoctoral Fellowship at the University of Sussex in England, he joined the faculty in psychology at the University of Washington in Seattle, where he continued his research on the ecology of marine fishes. In 1987, he was selected as a Congressional Science and Technology Policy Fellow by the American Association for the Advancement of Science and worked with the Senate Budget Committee. In 1988, he became Deputy Director of the Smithsonian Tropical Research Institute in Panama. In 1990, he joined the National Audubon Society as Senior Vice President for Science and Sanctuaries. From 1992 to 1996, Dr. Fischer was Director of the Board on Biology and the Institute of Laboratory Animal Resources at the National Research Council. He has been at CRS since 2007. He also served from 1993 to 2008 as a consultant to the United States Conference of Catholic Bishops, fostering dialogue among scientific and religious leaders on topics of common interest such as evolution, environment, genetic research, and end-of-life medical care.