Congressional Research Service

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

Before

Subcommittee on Research and Technology
Committee on Science, Space, and Technology
U.S. House of Representatives

January 27, 2015

on

"The Expanding Cyber Threat"

Chairwoman Comstock, Ranking Member Johnson, and distinguished Members of the Subcommittee:

Thank you for the opportunity to discuss issues related to cybersecurity with you today. In my testimony, I will provide an overview of federal cybersecurity activities related to science and technology (S&T). As you requested, I will also address long-term challenges the federal government faces related to cybersecurity, differing views about the federal role in cybersecurity, and how the *Cybersecurity Enhancement Act of 2014* (P.L. 113-274) affects existing cybersecurity efforts.

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 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.

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, 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 address various aspects of cybersecurity. More than 50 federal statutes 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. Those functions[4] relating to S&T include

- 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;

[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).

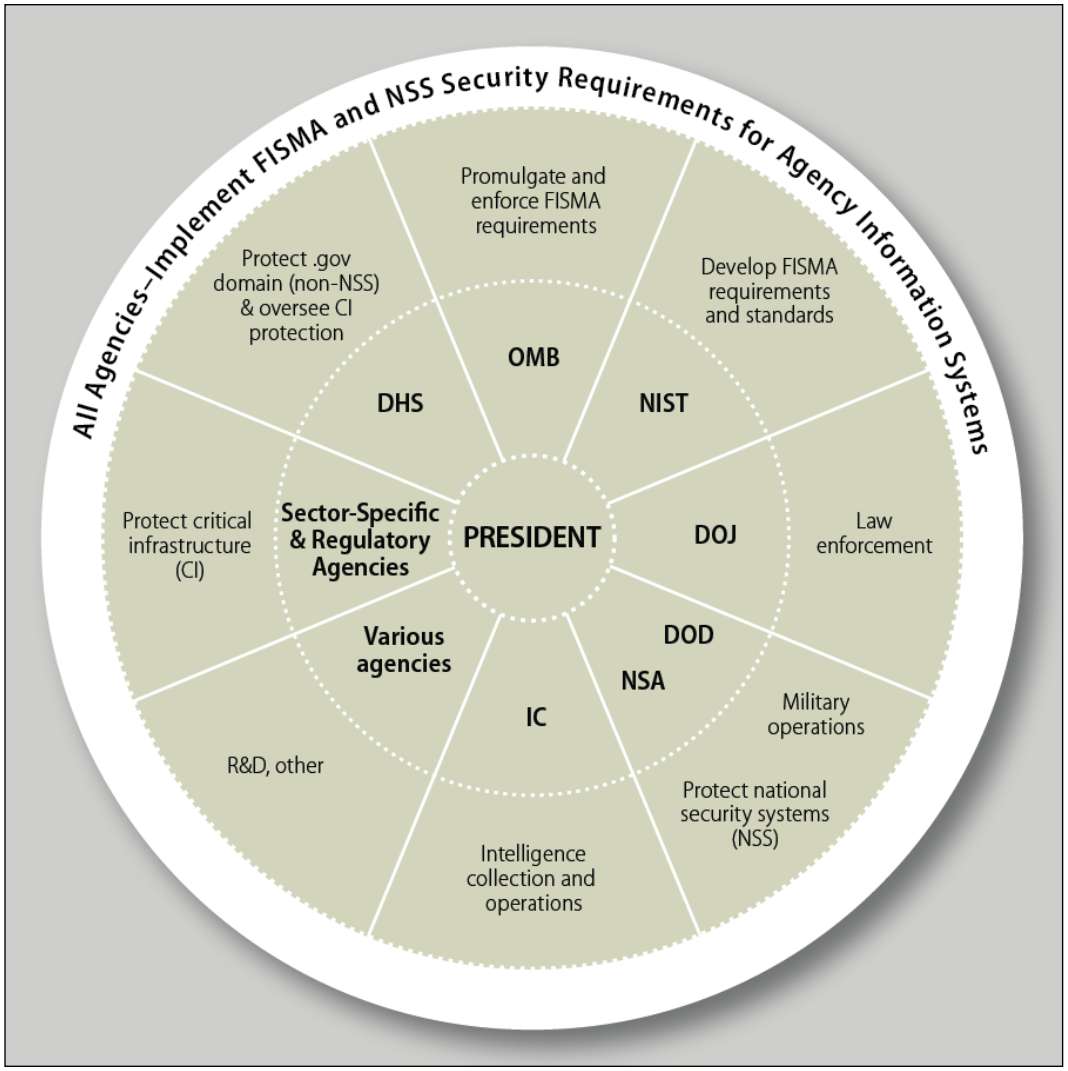
[2] See, for example, Department of Homeland Security, "Continuous Diagnostics and Mitigation (CDM)," June 24, 2014, http://www.dhs.gov/cdm.

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

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

- engaging in electronic surveillance and other *intelligence-gathering* activities to detect cyberthreats;
- engaging in investigations of cybercrime and other *law enforcement* activities;
- developing and enforcing federal *cybersecurity* regulations; and
- preparing for and engaging in *cybercombat*.

Figure 1. Simplified Schematic Diagram of Federal Agency Cybersecurity Roles



Source: CRS

Figure 1 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 subcommittee, 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 roles 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, 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. Cybersecurity is inherently technological, and many of the activities of agencies described below are therefore related to S&T.

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.

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

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.

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.

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

[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."

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.

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.

NASA—National Aeronautics and Space Administration. Most cybersecurity activities of this agency appear to be associated with protection of agency systems.

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 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 16 federal agencies and other entities responsible for various forms of intelligence collection and operations, including those relating to cybersecurity. The Director of National Intelligence sets standards for mission-crucial IC systems other than NSS. The Intelligence Advanced Research Projects Activity (IARPA) also engages in cybersecurity R&D.

NSA — National Security Agency.[9] 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

[8] CRS Report R43838, *Cyber Operations in DOD Policy and Plans: Issues for Congress*, by Catherine A. Theohary and Anne I. Harrington.

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

(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.

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.

SSAs — Sector-Specific Agencies. SSAs are those federal agencies responsible for leading public/private collaborative efforts to protect the 16 designated CI sectors.[10] A plan has been developed for each sector, and many of those plans include discussion of cybersecurity concerns and activities for the different sectors.[11]

Regulatory Agencies. The regulatory environment for cybersecurity is complex, involving both technical and nontechnical activities by various agencies.[12]

Research and Development

Many federal agencies, including those discussed above, engage in R&D related to cybersecurity. Cross-agency coordination of cybersecurity R&D is the responsibility of the National Coordinating Office (NCO), under the interagency National Science and Technology Council (NSTC) of the White House. The NCO coordinates the multiagency Networking and Information Technology Research and Development (NITRD) program.[13] Agencies identifying cybersecurity R&D activities over the last three budget cycles, with funding amounts, are presented in **Table 1**.

---

[10] 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.

[11] See Department of Homeland Security, "Sector-Specific Plans", 2012, http://www.dhs.gov/files/programs/gc_1179866197607.shtm.

[12] 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.

[13] CRS Report RL33586, *The Federal Networking and Information Technology Research and Development Program: Background, Funding, and Activities*, by Patricia Moloney Figliola.

Table 1. Agency Budgets for Cybersecurity and Information Assurance in the NITRD Program

Agency	Funding ($millions)		
	FY2013 Actual	FY2014 Estimate	FY2015 Request
NSF	97.9	106.6	102.5
NIST	49.7	59.7	59.7
NASA	—	—	—
DHS	75.3	77.8	67.5
DOE	32.6	36.7	30.0
DARPA	223.0	293.5	286.6
Other DOD	174.6	192.1	168.4
Other Agencies	—	—	—
Total Cybersecurity	*653.0*	*766.6*	*714.7*
Total NITRD	*3,567.6*	*3,909.4*	*3,807.2*

Source: Subcommittee on Networking and Information Technology Research and Development, Committee on Technology, *Supplement to the President's Budget for Fiscal Year 2015: The Networking and Information Technology Research and Development Program*, March 2014, https://www.nitrd.gov/pubs/2015supplement/FY2015NITRDSupplement.pdf.

Note: In addition to NASA, the other agencies reporting NITRD but not CSIA activities were the National Institutes of Health, the National Oceanic and Atmospheric Administration, the Environmental Protection Agency, the Department of Transportation, the Agency for Healthcare Research and Quality, and the National Archives and Records Administration.

Cybersecurity and Information Assurance (CSIA) is one of eight R&D topics, called Program Component Areas (PCAs), currently distinguished in the NITRD program. From FY2013-FY2015, CSIA activities accounted for about 19% of total NITRD funding. That is almost certainly an underestimate, because a significant proportion of R&D that agencies might reasonably consider related to cybersecurity may well be categorized in one of the other PCAs, such as High Confidence Software and Systems, Human Computer Interaction and Information Management, or Software Design and Productivity. Even for those agencies with no funding listed under CSIA, activities under other PCAs may well be related to cybersecurity. For example, NASA reported funding of $43.8 million in FY2013 for the other three PCAs listed above.

The CSIA activities described for each agency in **Table 1** cut across a broad range of topical areas, such as

- developing trusted computing and networking environments,
- improving the capacity of systems to evade attackers,
- improving the incentive structure for cybersecurity,
- developing better capabilities to build security into information systems,
- improving the ability to resist and recover from attacks,
- creating a more robust scientific foundation for cybersecurity,
- addressing cybersecurity priorities for CI sectors, and

- accelerating capabilities for transforming the results of R&D into usable technology and other applications.

Agencies also support and perform research on a broad array of topics aligned with their specific missions.

Cybersecurity Issues and Challenges

The risks associated with any attack 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.[14]

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 botnets[15] or reducing incentives for cybercriminals); (2) addressing vulnerabilities

---

[14] 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.

[15] 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,

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).

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,[16] 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.

---

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.

[16] 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.

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 challenges" to address difficult cybersecurity problems.[17] 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.[18] 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

---

[17] The White House, "The Comprehensive National Cybersecurity Initiative," March 5, 2010, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

[18] 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.

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 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."[19]

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.[20] 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,[21] 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 decade[22] and was a factor in the passage of the

---

[19] 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.

[20] See, for example, The Markle Foundation Task Force on National Security in the Information Age, *Nation At Risk: Policy Makers Need Better Information to Protect the Country*, March 2009, http://www.markle.org/downloadable_assets/20090304_mtf_report.pdf; CSIS Commission on Cybersecurity for the 44th Presidency, *Cybersecurity Two Years Later*, January 2011, http://csis.org/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf.

[21] 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.

Cybersecurity Research and Development Act in 2002 (P.L. 107-305, H.Rept. 107-355). That 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.[23]

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.

Cybersecurity Enhancement Act of 2014 (P.L. 113-274)

The enactment of P.L. 113-274 was in many ways a culmination of legislative efforts that had begun with the 111th Congress in 2009 with the introduction and passage by the House in 2010 of H.R. 4061, a bipartisan bill with a similar name from the House Science and Technology Committee. Neither that bill nor a related bill passed by the House in the 112th Congress, H.R. 2096, received floor consideration in the Senate. In the 113th Congress, the House again passed a related bill, H.R. 756. At the end of the 113th Congress, the Senate and House both passed and the President signed S. 1353, the Cybersecurity Enhancement Act of 2014, which became P.L. 113-274. Those bills all included revisions to the Cyber Security Research and Development Act, enacted in 2002, which provided authorization for research and postsecondary education activities in cybersecurity at NSF and NIST, as well as NIST cybersecurity standards activities.

Both H.R. 756 and S. 1353 had several similar provisions:

- A requirement for a strategic plan for cybersecurity R&D to be developed under the NITRD program;
- Revisions to NIST activities associated with development of standards for federal systems;
- Revision of NIST authorities for cybersecurity R&D;
- Authorization of NSF's cybersecurity Scholarship-for-Service Program; and
- Authorization of NIST activities in the development of international cybersecurity technical standards, the development of a federal cloud-computing strategy, and R&D related to identity management.

---

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

[23] 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. See also **Table 1**.

Provisions of H.R. 756 that were not included in P.L. 113-274 included authorization of NSF social and behavioral cybersecurity research, a government-wide assessment of federal cybersecurity workforce needs, and establishment of a university-industry task force in cybersecurity.

Provisions in P.L. 113-274 that were not in H.R. 756 included

- Authorization of a public-private partnership through NIST related to the one used in developing the Cybersecurity Framework;
- Authorization for interagency programs of competitions and challenges in cybersecurity aimed at recruiting talented individuals to the cybersecurity workforce and stimulating innovative R&D and applications in cybersecurity; and
- Authorization of activities by NIST in cybersecurity awareness and education related to the agency's existing NICE program.[24]

Given the recent enactment of P.L. 113-274, a substantive analysis of the impacts of the provisions would likely be premature.

[24] National Institute of Standards and Technology, "National Initiative for Cybersecurity Education (NICE)," January 20, 2015, http://csrc.nist.gov/nice/.

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.