Congressional Research Service

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

Before

Committee on Homeland Security
U.S. House of Representatives

February 25, 2015

on

"Examining the President's Cybersecurity Information Sharing Proposal"

Chairman McCaul, Ranking Member Thompson, and distinguished Members of the Committee:

Thank you for this opportunity to discuss legislative proposals on information sharing in cybersecurity.[1] In January of this year, the White House announced a revision of its 2011 information-sharing proposal as part of a set of updated proposals and other actions relating to cybersecurity:[2]

- A draft bill to enhance information sharing on cybersecurity within the private sector and between the private sector and the federal government. Most of my testimony today will focus on this proposal and related bills in the 113th and 114th Congresses.[3]
- A draft bill to amend federal statutes relating to cybercrime by creating or increasing criminal penalties for certain types of offenses and providing some other authorities to law-enforcement agencies and the courts.[4]

[1] This statement is limited to a policy analysis of the proposals and initiatives discussed and is not intended to reach any legal conclusions regarding them.

[2] The White House, "Securing Cyberspace: President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts," Press Release (January 13, 2015), http://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat.

[3] The White House, *Updated Information Sharing Legislative Proposal*, 2015, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-information-sharing-legislative-proposal.pdf.

- A draft bill to harmonize state laws requiring companies holding personal information on customers to notify them of data breaches involving such information.[5]
- A five-year, $25 million grant to create a new cybersecurity consortium consisting of 13 Historically Black Colleges and Universities (HBCUs), the Lawrence Livermore and Sandia National Laboratories of the Department of Energy, and a South Carolina school district. The object of the program is to help fill demand for cybersecurity professionals while diversifying the pipeline of talent for this and related fields of expertise.[6] This program can be seen as a complement to legislation enacted by the 113th Congress that addresses cybersecurity workforce needs in the Department of Homeland Security[7] (DHS) and more broadly.[8]

The announcement also included a description of the White House cybersecurity summit held on February 13 at Stanford University.

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 critical infrastructure.[9] 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.

---

[4] The White House, *Updated Administration Proposal: Law Enforcement Provisions*, 2015, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-law-enforcement-tools.pdf.

[5] The White House, *The Personal Data Notification & Protection Act*, 2015, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-data-breach-notification.pdf.

[6] The White House, "Vice President Biden Announces $25 Million in Funding for Cybersecurity Education at HBCUs," Press Release (January 15, 2015), http://www.whitehouse.gov/the-press-office/2015/01/15/vice-president-biden-announces-25-million-funding-cybersecurity-educatio.

[7] H.R. 2952, the Cybersecurity Workforce Assessment Act (P.L. 113-246), and S. 1691, the Border Patrol Agent Pay Reform Act of 2014 (P.L. 113-277), requiring assessments of workforce needs within the Department of Homeland Security and providing enhanced authorities to the Secretary for recruitment and retention of cybersecurity personnel.

[8] S. 1353, the Cybersecurity Enhancement Act of 2014 (P.L. 113-274), establishing in statute a National Science Foundation program for educating cybersecurity professionals for government agencies, and an interagency program of challenges and competitions in cybersecurity to stimulate identification and recruitment of cybersecurity professionals more broadly as well as cybersecurity research and innovation.

[9] 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.

A few sectors are subject to federal notification requirements,[10] but most such information sharing is voluntary, often through sector-specific Information Sharing and Analysis Centers (ISACs)[11] or programs under the auspices of the Department of Homeland Security (DHS) or sector-specific agencies.[12]

While there is some disagreement among experts about whether federal legislation is needed to address the problem, there appears to be fairly broad consensus that such legislation could be useful if crafted appropriately but potentially harmful if not. However, there is disagreement about what the key characteristics of useful legislation would be. Proposals to reduce or remove such barriers, including provisions in legislative proposals in the last two Congresses, have raised concerns, 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, or anticompetitive collusion among businesses that would currently violate federal law.

More broadly, debate has tended to focus on questions such as the following:

1. What are the kinds of information for which barriers to sharing exist that make effective cybersecurity more difficult, and what are those barriers?
2. How should information sharing be structured in the public and private sectors to ensure that it is efficient and effective?
3. What are the risks to privacy rights and civil liberties of individual citizens associated with sharing different kinds of cybersecurity information, and how can those rights and liberties best be protected?
4. What, if any, statutory protections against liability are needed to reduce disincentives for private-sector entities to share cybersecurity information with each other and with government agencies, and how can the need to reduce such barriers best be balanced against any risks to well-established protections?
5. What improvements to current standards and practices are needed to ensure that information sharing is useful and efficient for protecting information systems, networks, and their contents?

---

[10] Notable examples include the chemical industry, electricity, financial, and transportation sectors.

[11] See, for example, ISAC Council, "National Council of ISACS," 2015, http://www.isaccouncil.org/. ISACs were originally formed pursuant to a 1998 presidential directive (The White House, "Presidential Decision Directive 63: Critical Infrastructure Protection," May 22, 1998, http://www.fas.org/irp/offdocs/pdd/pdd-63.htm).

[12] See also CRS Report R42114, *Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions*, by Eric A. Fischer; CRS Report R42409, *Cybersecurity: Selected Legal Issues*, by Edward C. Liu et al.; CRS Report R42984, *The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress*, by Eric A. Fischer et al.; CRS Report R4381, *Legislation to Facilitate Cybersecurity Information Sharing: Economic Analysis*, by N. Eric Weiss.

The White House information sharing proposal would attempt to address such questions in several ways. The discussion below includes a summary of how the proposal would address them in comparison to the following bills addressing information sharing:

- H.R. 234, the Cyber Intelligence Sharing and Protection Act (CISPA), in the 114th Congress, identical to H.R. 624 as passed by the House in the 113th Congress;
- S. 2588, Cybersecurity Information Sharing Act of 2014 (CISA) as reported to the Senate in the 113th Congress;
- S. 456, the Cyber Threat Sharing Act of 2015, as introduced in the 114th Congress.

Kinds of Information Shared

Information sharing can involve a wide variety of material communicated on a wide range of timescales, ranging from broad cybersecurity policies and principles to best practices to descriptions of specific threats and vulnerabilities to computer-generated data transmitted directly from one information system to another electronically. The level of sensitivity of information can also vary—for example, it may be classified, proprietary, or personal. Information of any class will also vary in its value for cybersecurity and the degree to which it needs human processing to be useful.[13]

To the extent that the goal of information sharing is to defend information systems against cyberattacks, there appears to be a consensus that shared information needs to be actionable—that is, it should identify or evoke a specific response aimed at mitigating cybersecurity risks. To be meaningfully actionable, information may often need to be shared very quickly or even in an automated fashion. There may therefore be little or no time for human operators to examine a specific parcel of data to determine whether sharing it could raise privacy, liability, or other concerns.

The White House proposal would limit the scope of shared information covered under the proposal to "cyber threat indicators," which includes information needed to "indicate, describe, or identify" malicious reconnaissance or command and control activities, methods of social engineering and of defeating technical or operational controls, and technical vulnerabilities, and from which "reasonable efforts" have been made to remove personally identifying information if the person is thought to be unrelated to the threat. The definition in S. 456 is largely identical.

The definition in the White House proposal and S. 456 are arguably the narrowest in scope. S. 2588 also focuses on "cyber threat indicators," with a definition that is similar to that in the White House proposal, but is somewhat broader, including other attributes, such as the actual or potential harm caused by an incident. It also expressly permits sharing of information on countermeasures—measures to prevent or mitigate threats and vulnerabilities.

H.R. 234 uses the term "cyber threat information," characterized as information "directly pertaining to" efforts to gain unauthorized access to information systems or to effect negative impacts on systems or networks, threats to the information security of a system or its contents,

[13] See, for example, Kathleen M. Moriarty, "Transforming Expectations for Threat-Intelligence Sharing," *RSA Perspective* (August 3, 2013), https://www.emc.com/collateral/emc-perspective/h12175-transf-expect-for-threat-intell-sharing.pdf.

and vulnerabilities of systems and networks. The bill also defines a related term, "cyber threat intelligence," with characteristics similar to those of cyber threat information but is in the possession of the Intelligence Community.

Structure of Information Sharing

Information sharing can conceivably lead to information overload, where an entity receives much more information than it can reasonably process. That could include not only information of uncertain quality and use, but also similar or redundant information from a variety of sources. In addition, a proliferation of sharing mechanisms could lead to stovepiping, which could reduce sharing across sectors, for example, and lack of clarity with respect to responsibilities, which could lead to gaps in sharing useful information. In contrast, a narrow, tightly defined structure for information sharing could lead to logjams or impede innovation in response to continuing evolution of cyberspace.

The White House proposal and S. 456 would create a structure for information sharing that includes the National Cybersecurity and Communications Integration Center (NCCIC) as the federal hub for receipt and distribution of cybersecurity information, and fostering the use of private information sharing and analysis organizations (ISAOs) as recipients of information from private entities.[14] ISAOs could presumably also share such information under the provisions of the Homeland Security Act, but the proposal does not specifically address that function for them. The proposal would require the DHS Secretary to ensure that indicators are shared in a timely fashion with other federal agencies. S. 456 would require that procedures for such sharing be established and would specifically require the Secretary to ensure that both useful classified and unclassified information is shared with nonfederal entities.

H.R. 234 would create an entity at DHS (presumably the NCCIC[15]) to share threat information and an entity at the Department of Justice to share cybercrime information. It would require individual agencies that receive threat information to develop procedures for sharing it. In contrast to S. 456, it would require the Director of National Intelligence to establish procedures for sharing classified threat information. It would also designate specific classes of private-sector entities as those permitted to monitor systems and share threat information under the bill. Those include entities that provide cybersecurity goods and services to others or to themselves.

S. 2588 would require DHS to create a "capability and process" for sharing both threat indicators and countermeasures. It would establish an interagency process to develop procedures for

---

[14] ISAOs were defined in the Homeland Security Act (6 U.S.C. §131(5)) as entities that gather and analyze information relating to the security of critical infrastructure, communicate such information to help with defense against and recovery from incidents, and disseminate such information to any entities that might assist in carrying out those goals. The proposal covers receipt of indicators by ISAOs but does not mention communication or dissemination of information by them, except, by inference, to the NCCIC. Information Sharing and Analysis Centers (ISACs) are more familiar to most observers. They may also be ISAOs but are not the same, having been originally formed pursuant to a 1998 presidential directive (The White House, "Presidential Decision Directive 63: Critical Infrastructure Protection," May 22, 1998, http://www.fas.org/irp/offdocs/pdd/pdd-63.htm).

[15] The text in the bill was originally drafted before the enactment of the National Cybersecurity and Communications Integration Center Act of 2014 (P.L. 113-282), which established the NCCIC by statute.

sharing federal information with the private sector. It would require development of an interagency process for sharing classified threat indicators.

Timeliness of Sharing

The timescale on which shared information will be most useful varies. That is especially an issue in an environment where the relevance of timing for shared information may be measured in seconds or even milliseconds in many cases.[16] The White House proposal and S. 456 would address this concern by requiring the NCCIC to share indicators "in as close to real time as practicable" and by requiring establishment of a program to advance automated mechanisms for such sharing.

H.R. 234 and S. 2588 would also require "real-time sharing." The meaning of this term is not explicitly defined or described in the bills, but it presumably refers to sharing that occurs rapidly, for example, by machine-to-machine transmission. That is consistent with the stated purposes of the legislative proposals, in that threat information would likely need to be disseminated quickly in order to detect or prevent incoming cyberattacks, which can occur very quickly. This raises the question of whether this term should require any particular mode of sharing, for example, by machine-to-machine transmission without or with minimal intervening processing by human operators, and how different interpretations of the term may impact operational effectiveness, privacy interests, and competition for technical and financial resources. The White House proposal appears to address that through its proposed development of automated mechanisms, and S. 2588 would require development of a process to receive indicators and countermeasures electronically, including via an "automated process between information systems."

Privacy and Civil Liberties

Concerns relating to privacy and civil liberties, especially the protection of personal and proprietary information and uses of shared information, have been a significant source of controversy in debate about information sharing legislation. Such concerns have arisen in part because the White House proposal and the bills would permit sharing of specified cybersecurity information by covered private entities "notwithstanding any other provision of law." That would arguably remove barriers to sharing stemming from concerns that information would inadvertently violate laws such as those on privacy and antitrust.

However, it also raises concerns about privacy and civil liberties. In particular, personally identifying information might be included in the shared information but might not be related to the threat. In addition, data analytics might conceivably be used to draw inferences about identity from data sets even if any given piece of the shared information would not be identifying. Second, if access to shared information is not strictly controlled and restricted, or is used for purposes other than cybersecurity, risks to civil liberties may arise. Concerns have also been raised about regulatory use of shared information and disclosure of proprietary business information.

The White House proposal would address such concerns by

---

[16] See, for example, M.J. Herring and K.D. Willett, "Active Cyber Defense: A Vision for Real-Time Cyber Defense," *Journal of Information Warfare* 13, no. 2 (April 2014): 46–55.

- limiting application of the "notwithstanding" provision to indicators disclosed to the NCCIC and ISAOs;
- limiting private-sector use of shared indicators to purposes relating to protection of information systems and their contents;
- requiring minimization of personally identifiable information and safeguarding of any such information that cannot be removed;
- requiring development of guidelines by the Attorney General on limiting the acquisition and sharing of personally identifiable information and establishing processes for anonymization, safeguarding, and destruction of information;
- exempting information received by the federal government from disclosure under the Freedom of Information Act;
- prohibiting use of shared information for regulatory enforcement;
- requiring penalties for federal violations of its restrictions relating to information sharing; and
- an annual report to Congress on privacy and civil liberties.

S. 456 includes those provisions but would also permit a private entity to receive indicators under the "notwithstanding" provision.

H.R. 234 and S. 2588 have related provisions except as follows: Both bills explicitly limit federal use of shared information to cybersecurity purposes and uses relating to protection of individuals and investigation and prosecution of cybercrimes and certain other offenses. They both require various activities to reduce the degree to which personal information is shared and other means of safeguarding it from unauthorized sharing and use. H.R. 234 requires that guidelines be developed through an interagency process.

Liability Protections

Concern about liability has often been cited as a significant barrier to private-sector sharing of cybersecurity information, both with other private entities and with the federal government. In addition to the protections granted by the use of "notwithstanding any other provision of law" with respect to provision of information by private-sector entities, the White House proposal would address this issue by prohibiting civil or criminal actions in federal or state courts for covered activities with respect to lawfully obtained cyberthreat indicators disclosed to or received from the NCCIC or a certified ISAO. However, it also specifies monopolistic actions such as price-fixing that are not permitted.

The prohibition on civil or criminal actions in H.R. 234 covers acquisition and sharing of cyberthreat information, or decisions for cybersecurity purposes based on such information. The bill stipulates that actions must be taken in good faith. The S. 2588 prohibition covers only private defendants, and includes monitoring systems or sharing information. S. 2588 states that a good-faith reliance that an activity was permitted under the bill's provisions will serve as a complete defense against any court action. It also stipulates that private-sector exchange of cyberthreat information or assistance for cybersecurity purposes does not violate antitrust laws, but further specifies monopolistic actions such as price-fixing that are not permitted.

Improvements to Standards and Practices

The concerns discussed above about what information would be most useful to share and how raise the question of whether better standards and best practices are needed for improving the effectiveness and efficiency of information sharing.[17] The White House proposal and S. 456 would require the DHS Secretary to establish a process for selecting a private entity that would determine best practices for creating and operating private ISAOs. The recent executive order on information sharing has a similar provision.[18] There are no similar provisions in the other bills.

[17] See, for example, Moriarty, *Transforming Expectations for Threat-Intelligence Sharing*.

[18] Executive Order 13691, "Promoting Private Sector Cybersecurity Information Sharing," *Federal Register* 80, no. 34 (February 20, 2015): 9349–53.