Congressional Research Service
Informing the legislative debate since 1914

Perspectives on Federal Cybersecurity Spending

name redacted
Analyst in Emergency Management and Homeland Security Policy

name redacted
Analyst in Cybersecurity Policy

February 25, 2016

Congressional Research Service
7-....
www.crs.gov
R44404

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

The federal government invests significant resources in cybersecurity across every agency through a variety of activities. Although a methodologically rigorous total for these investments has not been calculated and may not be possible, an understanding of how the federal government applies resources to protect U.S. public and private sector data and networks from cyberattacks is necessary for Congress to provide constructive oversight of those efforts.

This report considers federal cybersecurity investments in three broad categories:

- Agency spending to protect its own systems, networks, and data;
- Agency spending to protect other governmental systems, networks, and data; and
- Agency spending to protect non-federal IT systems, networks, and data.

Each department and agency has some level of participation in cybersecurity activities. However, the Office of Management and Budget, the Department of Homeland Security, the Department of Commerce, the Department of Justice, and the Department of Defense have unique responsibilities established by statute—either for their role in assisting other departments and agencies, or, as in the case with the Department of Defense, for their unique responsibility for their own information technology.

Each February the administration releases three sets of documents which describe some facets of the government's investments in cybersecurity:

- The President's Budget;
- Congressional Budget Justifications from each department or agency; and
- The Federal Information Security Management Act (FISMA) report to Congress.

These reports provide some valuable insights into how or why the government makes certain investments associated with promoting cybersecurity. However, on their own, none of these documents provides a complete and precise representation of how much the federal government is spending on cybersecurity. This is in part because of how they are developed; they are developed from agency submissions based on administration guidance that does not require methodologically consistent reporting on cybersecurity spending—or even provide a common definition for what cybersecurity is.

Even if such an authoritative top-line figure for federal cybersecurity investments were available, without detail and context it would not effectively inform the Congressional decision-making process. Understanding the risks an individual agency faces, and what strategies they have for confronting those risks given their size, complexity, and mission is vital to determining the appropriate level of future cybersecurity investments for that agency. Armed with an understanding of those factors, Congress may choose to assess cybersecurity investments of a federal agency independently. Congress may alternatively choose to assess internal cybersecurity investments by an agency relative to similar federal agencies, and external investments relative to, and supporting, the non-".gov" sector.

Contents

Tables

Contacts

Introduction

There is a great deal of interest in the cybersecurity activities of the federal government.

Cyberattacks against the U.S. government and the nation have been reported with increasing frequency since 2006. Recent high profile breaches of federal government systems, including those of the White House, State Department, and Office of Personnel Management, have called into question the ability of the federal government to secure its data and networks adequately in today's threat environment.

Funding for cybersecurity activities has also risen over the years. Although a methodologically rigorous total for these investments has not been calculated, an understanding of how the federal government applies resources to enhance its cybersecurity is necessary for Congress to provide constructive oversight and prevent waste.

This report provides an overview of how the federal government has applied resources to promote cybersecurity in the past, and options for how it could choose to do so in the future.

Cybersecurity Defined for this Report

One of the challenges in discussing federal cybersecurity is that a common definition for the term "cybersecurity" does not exist. The United States Computer Emergency Readiness Team (US-CERT) provides the following definition:

> The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.
>
> Extended Definition: Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.

This definition presents cybersecurity as an integrated function. Any federal agency that employs information technology engages in cybersecurity activities in some way.

Rather than attempting to explore the "full range" of activities in the above US-CERT definition, this report will focus on a more limited range of activities: those involved in the protection of U.S. public and private sector data and networks from cyberattacks. Issues of deterrence, international engagement, diplomacy, military, and intelligence missions will largely be left for discussion in other reports.

How the Federal Government Invests in Cybersecurity

For this report, federal government spending on cybersecurity will be analyzed in three ways:

- Agency spending to protect its own systems, networks, and data;
- Agency spending to protect other governmental systems, networks, and data; and

- Agency spending to protect non-federal IT systems, networks, and data.

The first two types of spending can be termed "internal" spending, as they relate to the government dealing with its own cybersecurity responsibilities within the federal .gov domain. Each of these includes spending on information technology infrastructure (i.e., hardware and software) and services (including the costs of personnel).

The third type can be termed "external" spending, as it relates to the government promoting cybersecurity to elements beyond its direct control. This type can also be divided into two categories: direct funding—usually in the form of grants or other direct financing—and services—which could include training, technical assistance, regulatory efforts, information sharing efforts, or other programs where the government helps facilitate cybersecurity functions of outside organizations.

After reviewing these various cybersecurity responsibilities and potential ways to assess federal spending to meet them, this report will analyze three sources often cited as totals of cybersecurity spending, and discuss what would be necessary to provide an authoritative total that could support oversight efforts.

Federal Government Internal Cybersecurity Responsibilities

As noted above, all federal agencies that use information technology make investments in cybersecurity in their own systems and personnel. A handful of other agencies have specific cybersecurity responsibilities in protecting the whole federal government enterprise from cyberattacks.

Common Federal Agency Responsibilities for Internal Cybersecurity

Federal agency investments in their own cybersecurity include acquisitions of security hardware and software, the hiring of specialized personnel, and the training of staff. Generally, an agency is responsible for the security of its own systems, networks, and data. This includes agency generated data (like financial information) and collected data (like that submitted by the citizen population). This is governed by the requirements in the Federal Information Security Management Act as amended (hereinafter referred to as FISMA).[1]

Specific Federal Agency Responsibilities for Internal Cybersecurity

Several cabinet-level departments and federal agencies have unique responsibilities in promoting internal cybersecurity within the federal government.

- The Office of Management and Budget (OMB), in exercising its management role, requires agencies to implement cybersecurity protocols.
- The Department of Homeland Security (DHS) implements government-wide programs to protect the federal .gov domain from adversaries and oversees agency adoption of cybersecurity.
- The Department of Commerce (DOC), acting through the National Institutes for Standards and Technology (NIST), develops the standards for federal information technology systems.

[1] 44 U.S.C. §3551

- The Department of Justice (DOJ) investigates and prosecutes crimes involving federal information technology.
- The Department of Defense (DOD) participates in the requirements for unclassified systems under FISMA, and chairs the Committee on National Security System (CNSS) which performs a similar function as DHS for national security systems.[2] The DOD has unique authorities for ensuring the cybersecurity of the .mil domain.

A list of CRS experts capable of addressing Congressional inquiries regarding the cybersecurity functions of these departments is provided at the end of this report.

External Spending to Promote Cybersecurity

The federal government plays a role in enhancing cybersecurity in the non-federal sector as well. The non-federal sector includes state, local, and tribal governments; the private sector; academia; and non-governmental organizations.

Federal investment in the nation's cybersecurity is based on the increased reliance American companies and individuals have on the Internet. About 85% of the U.S. population uses the Internet—for communication, commerce, entertainment, financial transactions, and even the monitoring, control, and enabling of industrial activities.[3]

When agencies invest federal resources in cybersecurity outside the .gov domain, they are generally fulfilling one of three responsibilities:

1. The first responsibility is to broadly improve national cybersecurity (e.g., information sharing programs or law enforcement activities). An example of this is the National Cybersecurity and Communications Integration Center (NCCIC) at DHS, or the National Cyber Investigative Joint Task Force (NCIJTF) hosted by the Federal Bureau of Investigation (FBI). Both of these organizations share information on cyber threats and how those threats can be mitigated.
2. Another is to encourage improved cybersecurity activities within a specific sector (e.g., sector-specific agency activities for critical infrastructure). An example of this is the grant programs the Department of Energy (DOE) provides to industry to research ways to bolster the cybersecurity of the electric grid.
3. Finally, agencies wield regulatory authority over certain sectors of the economy that encompasses their cybersecurity practices. Examples of this include the Department of the Treasury's establishment of regulations for record-keeping and the retention of records, and the Federal Trade Commission enforcing regulations by fining individual companies for violating consumer protections.

[2] National security systems are defined in 44 U.S.C. §3552.

[3] The U.S. population is estimated at around 322 million people as of January 2015 according to the U.S. Census Bureau. The United States has around 276 million Internet users according to a 2014 estimate from the C.I.A. World Factbook, accessed February 12, 2016, at https://www.cia.gov/library/publications/the-world-factbook/rankorder/2153rank.html. The OECD "Digital Economic Outlook 2015" highlights some of the uses of the Internet in the digital economy, the report is available online at http://www.oecd.org/internet/oecd-digital-economy-outlook-2015-9789264232440-en.htm.

Totaling Federal Cybersecurity Spending

There are several different reasons for interest in various calculations of federal spending on cybersecurity. One might ask how much the government spends on cybersecurity in an attempt to gauge a level of commitment to confronting the issue. At the agency level, there may be an interest in looking at spending on cybersecurity as part of an effort to compare the level of activity across the government. An authoritative top-line number for federal government spending on cybersecurity cannot be calculated, however, without an explicit definition of what such a total encompasses and consistent reporting of data from all federal agencies. As such, neither the President's nor the agency budget justifications, nor the FISMA report (both discussed below) can be considered complete and accurate representations of how much the federal government is spending on cybersecurity.

Existing Assessments of Federal Cybersecurity Spending

Each February, the administration is expected to submit to Congress the following:

- The President's Budget for the fiscal year;
- Agency budget justifications; and
- The Annual Report to Congress: Federal Information Security Management Act.

Each of these submissions includes a manner of accounting for cybersecurity spending.

The Budget Request

Federal law requires the President to submit the budget of the U.S. government for the coming fiscal year "On or after the first Monday in January but not later than the first Monday in February."[4] Although sometimes the release of the budget and its supporting documents is delayed beyond the statutory window, usually they are released by the Office of Management and Budget (OMB) on the first Monday in February. Each year, the budget includes documents outlining government's activities and the administration's policy priorities in the coming fiscal year.

The Obama Administration's FY2017 budget request included a three-page fact sheet on cybersecurity spending.[5] This fact sheet stated that the Administration requested $19 billion "to support a broad-based cybersecurity strategy." It went on to highlight roughly $5.8 billion in funding requested for seven agencies in a brief discussion of priority cybersecurity programs. The FY2016 budget request included a similar four-page fact sheet on cybersecurity spending, which stated that the Administration requested $14 billion "to support the Administration's cybersecurity strategy." It went on to highlight roughly $12.4 billion in priority programs.[6]

While the methodology used in OMB's analysis in developing these totals is unknown, closer examination of the funding for each of the agencies highlighted showed inconsistencies in

[4] 31 U.S.C. §1105.

[5] The Fiscal Year 2017 Key Issue Fact Sheet for Cybersecurity is available online at https://www.whitehouse.gov/sites/default/files/omb/budget/fy2017/assets/fact_sheets/strengthening_federal_cybersecurity.pdf

[6] The Fiscal Year 2016 Key Issue Fact Sheet for Cybersecurity is online at https://www.whitehouse.gov/sites/default/files/omb/budget/fy2016/assets/fact_sheets/cybersecurity-updated.pdf.

methodologies among the agencies' accounting (discussed further below) and significant lack of detail.

Agency Budget Justifications

At roughly the same time as the release of the budget request by OMB, agencies release justifications outlining their own proposed budgets in much greater detail than is included in the President's budget request documents.

CRS appropriations experts reviewed agency budget justifications as part of an effort to assess the inclusiveness of the Administration's total number cited in the budget request, to determine if it was a total calculation of federal cybersecurity investments. Those reviews revealed a lack of consistency in agency reporting on cybersecurity spending across the government in their budget justifications. This inconsistency makes agency-to-agency comparisons in cybersecurity investments difficult.

Some agencies, such as DOE, included cybersecurity as a crosscut analysis of their budget. This crosscut accounted for DOE's protection of their own, internal IT systems. They also included spending for their external mission, pointing out proposed spending on their agency mission to enhance electric grid cybersecurity.

Others, such as DHS, highlighted some activities within various agency components, but did not present an overall total of those components' investment in cybersecurity, either individually or as a group. DHS did highlight cybersecurity spending as a mission area for the department, but did not provide an associated funding total for the department.

How an agency builds its IT systems also affected how cybersecurity spending is accounted for in the agency budget justifications. The Department of Veterans Affairs (VA) employs an enterprise architecture which does not distinguish (at least in publicly available documents) the security between managerial systems (such as financial systems and data) and mission-execution systems (such as those used to deliver benefits and services to veterans). Both types of systems are within their enterprise and are thus protected by the same investments in cybersecurity.

Other agencies make distinct investments for managerial systems and mission-execution systems. The Department of the Treasury distinguished, in their budget justification, between department-wide cybersecurity and the cybersecurity of the Internal Revenue Service (IRS). The IRS further distinguished between their taxpayer-facing systems and other systems, for the purposes of their budget justification.

FISMA Reporting

Pursuant to the E-Government Act of 2002 (P.L. 107-347), OMB is required to submit an annual report to Congress on federal agencies' implementation of FISMA. The report is released in February and covers the fiscal year that ended the previous September. The report addresses agency reporting on their progress as well as Inspector General assessments of the agency's progress in implementing FISMA. Based on agency reporting and following a construct provided by OMB, the report also includes a totaling of agency investments for their own internal cybersecurity.

Appendix 4 of the annual FISMA report to Congress includes an accounting of "IT Security Spending Reported by CFO Act Agencies."[7] The Final Report for FY2014 was released at the end

[7] The Chief Financial Officer (CFO) Act (P.L. 101-576) mandated that cabinet-level and certain independent agencies (continued...)

of February 2015, and reports $12.7 billion in federal spending. According to the appendix, this amount encompasses three broad-ranging activities: the agencies' efforts to "Prevent Malicious Cyber Activity; Detect, Analyze, and Mitigate Intrusions; and Shape the Cybersecurity Environment." These three activities encompass a broad range of more specific activities, outlined in **Table 1**.

Table 1. Categories of Spending Included in FISMA Reporting

Prevent Malicious Cyber Activity	Detect, Analyze, and Mitigate Intrusions	Shape the Cybersecurity Environment
Trusted Internet Connections (TICs)	Computer Emergency Response Teams (CERTs)	National Strategy for Trusted Identities in Cyberspace
Intrusion prevention systems	Federal incident response centers	Workforce development
User identity management and authentication	Cyber threat analysis	Employee security training
Supply chain monitoring	Law enforcement	Standards development and propagation
Network and data protection	Cyber continuity of operations (COOP)	International cooperation activities
Counterintelligence	Incident response and remediation	Information security and assurance research and development
Insider threat mitigation activities	Forensics and damage assessment	
	ISCM and IT security tools	
	Annual FISMA testing	

Source: Office of Management and Budget, *Annual Report to Congress: Federal Information Security Management Act*, Washington, DC, February 27, 2015, pp. 81-82, https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy14_fisma_report_02_27_2015.pdf.

Analysis of Cybersecurity Spending Totals

Some have asked if the federal government is spending "enough" on cybersecurity.[8] The question of "enough" is difficult to answer. Under the FISMA guidance, and other industry-respected cybersecurity frameworks (e.g., the Cybersecurity Framework and the CIS Critical Security Controls), cybersecurity decisions must be made from an understanding of risk. However, quantifying the cybersecurity risk to the nation is difficult, partly due to the size of the nation, the complexity of systems, and the speed at which the threat, vulnerability, and consequence landscape evolves.

Furthermore, the total amount of federal cybersecurity spending does not properly inform the decisionmaking process. There is no single decision that drives the top-line number. Instead, there are hundreds of cybersecurity-related programs large and small across the government. The

(...continued)

have a chief financial officer. More information on the CFO Act may be found online at https://cfo.gov/.

[8] Aliya Sternstein, "Is Obama's $14 Billion Cybersecurity Request Enough?," *Defense One*, February 3, 2015, online at http://www.defenseone.com/technology/2015/02/obamas-14-billion-cybersecurity-request-enough/104421/, and Bob Bryan, "The US government Is Not Spending Enough on Cybersecurity," *Business Insider*, September 3, 2015, online at http://www.businessinsider.com/us-government-cybersecurity-spending-2015-9.

Administration requested $6.7 billion in cybersecurity funding for DOD for FY2017—roughly one-third of the $19 billion they attributed to their government cybersecurity strategy.[9] The influence of the DOD investment on the total cybersecurity budget masks the significance of increases or decreases in the civilian cybersecurity budget if they are rolled into the same total, despite the fact that the DOD investment has limited impact on the cybersecurity of the rest of the federal information technology enterprise. Cybersecurity in the federal government enterprise—even when defined in the narrowest of terms—requires such a breadth of individual activities, as noted in the FISMA report, that the top-line number may be more of a curiosity rather than a useful data point in setting policy.

Considerations for Congress

Assessing Federal Government Cybersecurity Investments

For Congress to perform oversight of the federal government's investments in cybersecurity efforts as a whole, one could posit that four elements are necessary: an overarching federal cybersecurity strategy, a plan to execute that strategy, metrics that allow Congress to assess progress against the strategy's goals, and consistent reporting across agencies on how that strategy is being carried out.

The Administration released, in conjunction with the FY2017 budget, the Cybersecurity National Action Plan (CNAP). The CNAP incorporates previous federal-only strategies, such as the Cybersecurity Strategy and Implementation Plan (CSIP), and national strategies, such as the National Strategy for Trusted Identities in Cyberspace. However, given the breadth and complexity of the federal cybersecurity enterprise, an overarching strategy by necessity lacks a certain level of detail. Nevertheless, an articulate statement of the goals of the enterprise would improve opportunities for coordinated efforts among its parts.

Plans to meet the goals of the strategy are discussed below, as they should conform to the responsibilities and capabilities of each agency. However, metrics and reporting can best support comparative analysis of cybersecurity efforts if they are developed with such analysis in mind.

Assessing Federal Agency Cybersecurity Investments[10]

The cybersecurity functions of the federal government are carried out on an agency-by-agency basis, with decisions made and executed by the varied agencies and departments rather than by a central authority. As such, it is generally practical for oversight to be carried out in a similar agency-by-agency basis.

[9] The Administration's FY2017 cybersecurity fact sheet states the budget request is $19 billion for cybersecurity and is available online at https://www.whitehouse.gov/sites/default/files/omb/budget/fy2017/assets/fact_sheets/strengthening_federal_cybersecurity.pdf. The Department of Defense FY2017 budget fact sheet states the cybersecurity investment will be $6.7 billion and is available online at http://www.defense.gov/News/News-Releases/News-Release-View/Article/652687/department-of-defense-dod-releases-fiscal-year-2017-presidents-budget-proposal.

[10] Some elements of internal cybersecurity programs may be considered law-enforcement sensitive or classified for national security reasons, and not discussed as a part of public budget justification documents.

Assessing Internal Cybersecurity Investments

As noted above, there are several strategy documents governing some aspects of federal government cybersecurity functions. The closest document to an overarching strategy for the federal civilian cybersecurity enterprise is found in OMB Memorandum M-16-04, "Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government."[11] More prescriptive than a typical strategy document, this memorandum was issued October 30, 2015, as a follow on to the June-July 2015 "Cybersecurity Sprint." The Sprint was a 30-day implementation of high-priority actions aimed at improving the internal cybersecurity of the federal government in the wake of a series of breaches of government systems, including those at the Office of Personnel Management.

The Sprint listed the following key principles:

- Protecting Data: Better protect data at rest and in transit.
- Improving Situational Awareness: Improve indication and warning.
- Increasing Cybersecurity Proficiency: Ensure a robust capacity to recruit and retain cybersecurity personnel.
- Increas[ing] Awareness: Improve overall risk awareness by all users.
- Standardizing and Automating Processes: Decrease time needed to manage configurations and patch vulnerabilities.
- Controlling, Containing, and Recovering from Incidents: Contain malware proliferation, privilege escalation, and lateral movement. Quickly identify and resolve events and incidents.
- Strengthening Systems Lifecycle Security: Increase inherent security of platforms by buying more secure systems and retiring legacy systems in a timely manner.
- Reducing Attack Surfaces: Decrease complexity and number of things defenders need to protect. [12]

Among the activities of the Sprint was the formation of a team that included OMB's E-Gov Cyber and National Security Unit, the National Security Council Cybersecurity Directorate, the Department of Homeland Security, and the Department of Defense. The "Cybersecurity Sprint Team" conducted a 30-day review of "Federal Government cybersecurity policies, procedures, and practices," and based on that review, the federal CIO was to do two things: "create and operationalize a set of action plans and strategies to further address critical cybersecurity policies, and recommend a *Federal Civilian Cybersecurity Strategy*." While the CSIP did not explicitly organize around the same eight "key principles" outlined for it in the announcement of the Sprint, it addresses most, if not all, of those principles in its discussion. The CSIP listed the following objectives:

- Prioritized Identification and Protection of High Value Information and Assets;
- Timely Detection of and Rapid Response to Cyber Incidents;

[11] Shaun Donovan and Tony Scott, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, Office of Management and Budget, M-16-04, Washington, DC, October 30, 2015, https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf.

[12] United States Chief Information Officer Tony Scott, *Fact Sheet: Enhancing and Strengthening the Federal Government's Cybersecurity,* Washington, DC, June 12, 2015.

- Rapid Recovery from Incidents When They Occur and Accelerated Adoption of Lessons Learned from the Sprint Assessment;
- Recruitment and Retention of the Most Highly-Qualified Cybersecurity Workforce Talent the Federal Government Can Bring to Bear; and
- Efficient and Effective Acquisition and Deployment of Existing and Emerging Technologies.[13]

Currently, the most uniform reporting on cybersecurity activity is provided through the annual FISMA report. Two factors complicate using the FISMA report as a source of overall cybersecurity funding. First, FISMA only requires reporting on the specific categories outlined in the table above. These specific categories are not exhaustive of all cybersecurity spending, especially for external cybersecurity activities, although they do give a view to the breadth of activities involved in information technology security. Second, the FISMA report is based on self-reported data from the agencies, compiled after the end of the fiscal year—it is a window on where agencies have been, rather than where they are going.

Under FISMA, an agency's Inspector General (IG) is required to perform independent audits of its agency's IT systems and submit their findings to Congress. This review takes a system-by-system approach which includes recommendations for remediating IG-identified deficiencies.

Federal agencies present Congress with a range of budget justification formats and structures. Some agencies highlight their cybersecurity investments by presenting a crosscutting budget item that aggregates information from across the agency appropriations. Others may highlight one or two programs that represent priority initiatives for those agencies, note cybersecurity-related increases on top of ongoing programs (which may or may not be wholly dedicated to cybersecurity) or simply not highlight them at all. In these latter cases budget justification documents may not allow Congressional staff to identify specific levels of cybersecurity investment, and additional questioning of the department or agency may be necessary.

Getting Consistent Budget Data

If the budget request, FISMA reporting, and agency budget justifications do not provide adequate data on cybersecurity spending, the question becomes one of how effective oversight of cybersecurity funding can be performed. The initial question seems to be straightforward: how much does a given agency spend on cybersecurity? However, the answer is only helpful in the context of an understanding of what the agency considers cybersecurity spending, how the total is divided among those activities, and what type of risks they face. Further useful context would include an understanding of what functions are performed "in-house" by agency staff, as opposed to what functions are contracted out.

Aside from a given agency's total investment in their own cybersecurity, questions Congress may explore in regards to an agency's internal cybersecurity may include:

- Whose data does the agency possess and how does it handle it?
- Is the agency investing to enhance their cybersecurity posture based on improved understanding of the threat landscape?
- How did the agency come to understand their level of risk?

[13] Donovan and Scott, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, Office of Management and Budget, M-16-04.

- Has the agency experienced breaches over the past year? Was a mitigation plan established? Who determined the plan is adequate and is the plan fully funded?
- What are the results and progress from independent audits to agency systems?

An understanding of what risks an agency faces and what strategies the agency currently uses to combat those risks is a foundational element in examining an agency's internal cybersecurity. This information will also assist understanding agency investments in cybersecurity and what next steps are necessary for that agency.

Assessing External Cybersecurity Investments[14]

The appropriate role of the federal government in ensuring a certain level of national cybersecurity is a matter of debate. Among the questions Congress may explore in assessing the appropriate level of investment in external cybersecurity are:

- What is the appropriate role of government in sharing information among victims of cyberattacks, and what might that cost to execute?
- Is it appropriate for the federal government to invest taxpayer dollars in protecting private sector networks that generate profits for private entities?
- What is the proper role for the federal government in cyberattack remediation for non-federal victims?
- Are federal grants supplanting non-federal investment in cybersecurity or complementing it?
- Are federal investments serving the needs of nonfederal organizations?

Understanding the risks organizations in the non-.gov domain face and their relationship with the federal government will inform the Congress and allow them to assess further levels of investment.

As noted above, some agencies bear the added responsibility of helping secure the .gov domain beyond their internal cybersecurity duties. Recent Congresses have altered and clarified agency responsibilities for promoting federal .gov cybersecurity. The Cybersecurity Protection Act of 2014 (P.L. 113-282), the Cybersecurity Enhancement Act of 2014 (P.L. 113-274) and the Cybersecurity Act of 2015 (Division N of P.L. 114-113) include provisions that require agencies to report to Congress on their progress in implementing their responsibilities, to include the resources allocated to these efforts. As of this writing, some of these newly required reports have yet to be provided to Congress or made public; ultimately, they may provide a more detailed context for congressional oversight efforts.

Cross-Agency Cybersecurity Comparisons

The usefulness of comparing one federal agency's investment in cybersecurity to another's has its limits. Agencies vary in size and complexity—in terms of number of employees, number of geographic locations and number of separate systems. Depending on the missions of an agency, their risk profiles will also vary—for instance, an agency which collects and uses citizen data as a core function of its business will have a different risk profile than one that deals mostly with intellectual property as part of research and development. These variances make drawing valid

[14] As noted above, some elements of internal cybersecurity programs may be considered law-enforcement sensitive or classified for national security reasons, and not discussed as a part of public budget justification documents.

conclusions from broad agency to agency comparisons difficult. This also extends to components within a department, which may serve totally different functions.

Keeping such factors in mind, cross-agency comparisons may yet provide useful benchmarks when examining agencies with similar risk profiles, such as those agencies in the national security arena, or those that deliver citizen benefits. These agencies may maintain and process different sets of data, but comparison of how agencies strive to protect data of similar use and value from similar threats may provide useful case studies, insight into best practices, and models for prudent investments as agencies seek to procure and deploy further cybersecurity technologies.

Such comparisons may also help identify opportunities for agencies to achieve enhanced cybersecurity for their data at scale. Two or more agencies with similar risk profiles may seek common, shared platforms for their computing and security needs. Such joint efforts may achieve cost efficiencies while meeting those security needs. This model is proposed in the CNAP, with the Administration requesting $3.1 billion in FY2017 for an information technology modernization fund. While this fund may not expressly be for "cybersecurity technology," the proposal does not seem to bar using its resources for such investments.

Author Contact Information

(name redacted)
Analyst in Emergency Management and Homeland Security Policy
[redacted]@crs.loc.gov, 7-....

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

Key Policy Staff

Area of Agency Expertise	Name	Phone	Email
Department of Homeland Security	(name redacted)	7-....	/redacted/@crs.loc.gov
Office of Management and Budget	Glenn McLoughlin	7-....	/redacted/@crs.loc.gov
Department of Commerce (National Institutes of Standards and Technology)	John F. Sargent, Jr.	7-....	/redacted/@crs.loc.gov
Department of Justice	(name redacted)	7-....	/redacted/@crs.loc.gov
Department of Defense	(name redacted)	7-....	/redacted/@crs.loc.gov