THE CYBER SECURITY PROJECT

Understanding Federal Cybersecurity

Kate Charlet

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
APRIL 2018

The Cyber Security Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/Cyber

Layout by Andrew Facini

Cover photo: A view of the National Cybersecurity and Communications Integration Center before remarks by President Barack Obama, on Tuesday, Jan. 13, 2015, in Arlington, Va. (AP Photo/Evan Vucci).

Printed in the United States of America

THE CYBER SECURITY PROJECT

Understanding Federal Cybersecurity

Kate Charlet

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
APRIL 2018

About the Author

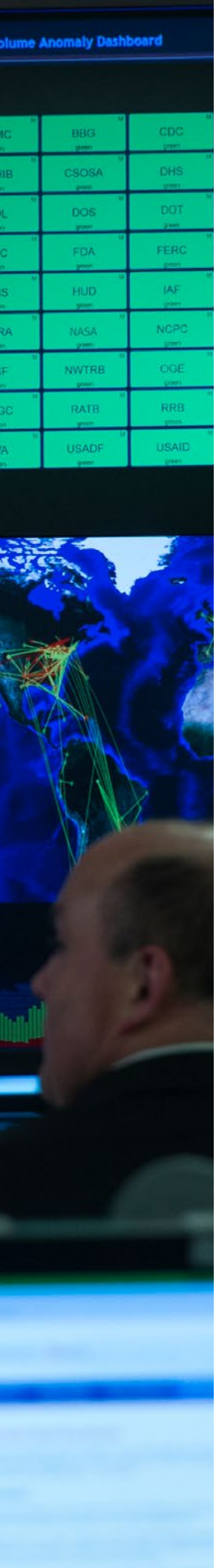
Kate Charlet is the Program Director for Technology and International Affairs at the Carnegie Endowment for International Peace and former Deputy Assistant Secretary of Defense (Acting) for Cyber Policy. In 2016, she served as an advisor to the Presidential Commission on Enhancing National Cybersecurity, where she focused on federal cybersecurity.

Acknowledgements

The author gratefully acknowledges the invaluable contributions and in-depth research of Gabriella Roncone, a research assistant at the Belfer Center's Cyber Security Project. Many other colleagues offered important insights and assistance, including Thomas E. Donilon, Mari Dugas, Eric Goldstein, Andrew Grotto, Heather King, Tim Maurer, Ross Nodurft, George Perkovich, Charley Snyder, Ari Schwartz, Michael Sulmeyer, Kathryn Taylor, Kiersten Todt, two anonymous peer reviewers for the Belfer Center, and multiple current/former officials at NIST, OMB, GSA, DHS, DOD, and NSC. Any errors, of course, are solely those of the author.

Table of Contents

Cover Image
A view of the National Cybersecurity and Communications Integration Center before remarks by President Barack Obama, on Tuesday, Jan. 13, 2015, in Arlington, Va. (AP Photo/Evan Vucci)



Executive Summary

Federal networks are attractive targets for foreign intelligence services and other malicious actors in cyberspace. Networks serving over 100 agencies and millions of employees enable government missions and operations, handle sensitive internal communications, and store personal data on millions of Americans. The level of threat faced by federal government networks has few parallels, and agencies have been unable to keep up.

Federal cybersecurity is a dense, inaccessible topic to those outside the information security community and even to some inside it. Information is scattered across a variety of government documents, with no "one stop shop" to understand the topic. This report fills the gap by:

- Characterizing the **federal cybersecurity landscape**, to include describing roles and responsibilities of various federal agencies and identifying systemic challenges.
- Summarizing **recent federal drives** to improve it, such as through information technology modernization, identification of high value assets, using shared services and commercial technologies, detecting and blocking threats, identifying and fixing risk factors, and improving incident response.
- Reviewing efforts to improve the **foundations of federal cybersecurity** by enhancing the cyber workforce, research and development efforts, acquisition, and leadership.

Securing federal civilian networks and systems is a complex and daunting prospect. Several systemic factors contribute to a challenging environment:

1. **Difficult tradeoffs between centralized and decentralized management**. The overall federal structure is largely decentralized, with each agency managing its own risk, and implementing its own security solutions. Full centralization would bring its own challenges, such as limiting agencies'

ability to develop tailored, agile solutions to their cybersecurity challenges.

2. **Varying levels of engagement of agency top leadership on cyber risk management.** Successful agency heads develop an awareness of cyber risk and actively manage it. Within agencies, the authorities of chief information officers vary widely.

3. **Varying effectiveness of levers to direct, incentivize, and enforce action by nonperforming federal agencies**. The Department of Homeland Security and Office of Management and Budget have some levers to drive action by individual agencies, and DHS' increasing operational authority has been critical.

4. **Resource constraints and a rigid government budgeting cycle.** Properly resourcing cybersecurity priorities can be expensive, and the structure of the government budgeting process poses challenges for agency cybersecurity efforts.

5. **Scattered congressional oversight**. No single congressional body has the full picture of federal cybersecurity measures, and legislative requirements are spread across many bills, making it complicated for federal agencies to adapt to threats.

In developing approaches to better manage cyber risk to federal government systems, policymakers, agency leaders, cybersecurity professionals, and congressional staff should consider the following themes:

- **Sound risk management underpins all federal cybersecurity efforts**. Federal agencies cannot and will not prevent every incident or intrusion. Agencies must identify the most important missions and assets, then craft strategies to reduce, mitigate, or accept the risks.

- **Sustained, high-level leadership from agency heads is critical to success.** Agencies with engaged department heads or deputies are much more likely to use resources strategically, force mission or business owners to attend to cybersecurity, and empower chief information officers to take steps needed to protect systems and enforce standards.

- **Effective management demands clarity on roles and responsibilities.** The federal cybersecurity system is complex. This is not inherently bad but it does demand constant effort to refine, clarify, and institutionalize roles and responsibilities to ensure coherence.
- **Steady, incremental progress makes a difference.** The Cyber Sprint in 2016, modest as it was, demonstrated that agencies can make progress when held accountable for discrete milestones, especially on issues of basic cyber hygiene often exploited by intruders.
- **Some areas, however, require constant innovation, or even a fundamental "rethink."** The most advanced agencies have policies that reward and implement innovative ideas on topics like workforce, procurement, and executive education.
- **Congress plays a critical role**. Congress authorizes and appropriates agency missions, authorities, and budgets. Very little can be done without strong support and engagement from the legislative branch.
- **Resources matter**. Skimping on resources for modernizing networks or attracting cybersecurity talent will reduce the ability of agencies to secure their core missions, with real impacts to both government and citizens.
- **Evolving technology will change the game**. Innovation in the digital ecosystem, like automation, will bring both new threats and new defensive applications. The government will need to plan 5- to 10-years ahead to keep from lagging behind.

There are no silver bullets for federal cybersecurity. The system will retain its inherent complexity, necessitating close coordination and partnership. Federal cybersecurity will be an enduring mission, always evolving and changing to stay ahead of the threat. In other words, there is no "finish line"—only continual improvement, adaptation, and cooperation to secure the federal government and those it serves.

Introduction

Federal networks are attractive targets for foreign intelligence services and other malicious actors in cyberspace. They enable government missions and operations, handle sensitive internal communications, and store personal data on millions of Americans. The level of threat faced by federal government networks has few parallels, and agencies have been unable to keep up. Multiple compromises—including those of the Office of Personnel Management, the Department of Defense, the Department of State, the Executive Office of the President, and the Internal Revenue Service—have exposed agencies' missions to risk and undermined trust and confidence in the government.

Securing federal networks, one might imagine, ought to be simpler than other aspects of U.S. cybersecurity policy. The issue is not a partisan one, nor do the solutions require as much cajoling and influencing of non-governmental actors, like critical infrastructure operators. So why is it so difficult to secure these systems appropriately? Answering this question requires first understanding the complex environment of federal cybersecurity efforts. Only then can analysts examine why roadblocks remain and what solutions may be most effective.

To date, there is no "one stop shop" for researchers, policymakers, and practitioners to understand the many dimensions of federal cybersecurity. Instead, information is scattered across government reports, memoranda, press releases, contracts, and more –in language inaccessible to those outside Information Technology (IT) professions. To fill this gap, this paper:

1. Characterizes the **federal cybersecurity landscape**, including the complex set of roles, responsibilities, and relationships among federal agencies.
2. Summarizes **recent federal drives** to improve it, with deeper dives on the most important initiatives.
3. Reviews efforts to improve the **foundations of federal cybersecurity**, like those to improve workforce and cybersecurity culture.

1. The Federal Cybersecurity Landscape

Securing federal civilian networks and systems is a complex and daunting prospect. With well over 100 agencies, millions of employees, and tens of millions of devices to manage, the federal government eclipses even the largest private employers in the United States. Every agency is responsible for its own cybersecurity, yet several play cross-cutting roles in directing, shaping, encouraging, or assisting good cybersecurity. Given the complexity of this system, developing sound policies and practices requires a solid grounding in the federal cybersecurity landscape, including key actors, agency roles and responsibilities, and systemic challenges.

The Overall Landscape

Every year, the federal government spends tens of billions of dollars on IT and cybersecurity. Understanding the exact spending trends can be difficult, since accounting methods have differed across various sources. However, the Office of Management and Budget, in its "IT Dashboard," summarizes IT spending trends as $82.8 billion in FY2016, $78.4 billion in FY2017, $81.3 billion in FY2018, and $83.4 billion in FY2019.[1] There is also no fully-agreed upon definition of what portion of IT expenditures is considered "cybersecurity spending." By one calculation, the federal government spent around $14 billion in FY2016.[2] President Barack Obama's administration requested $19 billion for cybersecurity initiatives in FY2017, but the full budget request never passed Congress.[3] It is more difficult to characterize the Trump Administration's cybersecurity budget, which does not offer a consolidated summary for cybersecurity.

1 Executive Office of the President. IT Dashboard. https://www.itdashboard.gov/. These numbers do not include classified IT spending or the IT Modernization Fund.

2 Andrea Shalal and Alina Selyukh, "Obama seeks $14 billion to boost U.S. cybersecurity defenses," Reuters, February 2, 2016. https://www.reuters.com/article/us-usa-budget-cybersecurity/obama-seeks-14-billion-to-boost-u-s-cybersecurity-defenses-idUSKBN0L61WQ20150202.

3 "Fact Sheet: Cybersecurity National Action Plan." February 9, 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

Cybersecurity expenditures support a large and diverse federal government. Although employment accounting methods vary, the Office of Personnel Management estimates 4.1 million total full time equivalents (FTEs) in the federal government for 2017.[4] This includes:

- 2.14 million executive branch civilian FTEs.
- 562 thousand postal service civilian FTEs.
- 1.38 million uniformed military FTEs.
- 34 thousand civilian FTEs in the legislative branch.
- 33 thousand civilian FTEs in the judicial branch.

Pinpointing the exact number of agencies in the federal government is difficult, but for the purposes of federal cybersecurity, it is common to see agencies grouped into two categories: "CFO Act" agencies and "non-CFO Act" agencies. CFO Act agencies are the 24 largest federal agencies (in terms of budget) that receive particular management oversight by the Office of Management and Budget (OMB).[5] These agencies make up the vast majority of federal government personnel and are required to report information security data for monitoring and tracking by the Department of Homeland Security (DHS), OMB, and Congress.[6] References to *civilian* CFO Act agencies include all CFO Act agencies except the Department of Defense, which is sometimes treated differently in terms of its reporting and other requirements because of its role managing "national security systems."

The rest of the agencies consist mostly of small (<6,000 employees) and micro (<100 employees) agencies as well as some larger, often independent,

4 Office of Management and Budget. *Analytical Perspectives: Budget of the U.S. Government Fiscal Year 2017.* Table 8-3 https://www.gpo.gov/fdsys/pkg/BUDGET-2017-PER/pdf/BUDGET-2017-PER.pdf.

5 CFO Act agencies include the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, Interior, Justice, Labor, State, Transportation, Treasury, Veterans Affairs; the U.S. Agency for International Development; the Environmental Protection Agency; the General Services Administration; the National Aeronautics and Space Administration; the National Science Foundation; the Nuclear Regulatory Commission; the Office of Personnel Management; the Small Business Administration; and the Social Security Administration.

6 Chief Financial Officers Act of 1990. http://govinfo.library.unt.edu/npr/library/misc/cfo.html.

regulators.[7] Cybersecurity efforts for this group come with unique challenges because small agencies may have less cybersecurity capability and fewer oversight requirements, yet nonetheless manage important missions and information. OMB estimates that non-CFO Act agencies "employ more than 100,000 Federal workers and manage billions of taxpayer dollars."[8] Nonetheless, these agencies are not required by law to report on information security to OMB, although around 60 of them do so voluntarily.

Cybersecurity at regulatory agencies is coming into the spotlight following reports of compromises at the U.S. Consumer Financial Protection Bureau and the Securities Exchange Commission.[9] Regulators tend to fiercely protect their independence from political executive branch agencies, because their missions are meant to be apolitical and independent. This independence tends to carry over into management, operations, and budget for these agencies, which makes it more difficult for the White House to drive or influence regulatory agencies to adopt certain cybersecurity practices. This means that when the White House identifies priority threats or challenges for cybersecurity, they can galvanize the rest of the interagency to make progress, but can't do the same with the regulatory agencies.

Congress plays a crucial role in federal cybersecurity. It legislates the fundamental principles of how the federal government manages its information technology, and it authorizes and appropriates agency IT missions, authorities, and budgets. There are many relevant pieces of legislation, but the key bills for federal cybersecurity include:

- The 1996 **Clinger-Cohen Act**, also known as the Information Technology Management Reform Act (ITMRA), changed how the federal government had managed IT for several decades. The law allowed agencies to acquire IT resources more independently.

7 Examples of non-CFO act agencies include the Marine Mammal Commission, the Peace Corps, the Federal Reserve Board of Governors, the Securities and Exchange Commission, and the Federal Communications Commission.

8 Office of Management and Budget. Federal Information Security Modernization Act of 2014 Annual Report to Congress Fiscal Year 2015. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/final_fy_2015_fisma_report_to_congress_03_18_2016.pdf. Page74.

9 Lisa Lambert. "U.S. Financial Regulator Must Beef up Cybersecurity: Inspector." Reuters, October 4, 2017. https://www.reuters.com/article/us-usa-consumers-cyber/u-s-financial-regulator-must-beef-up-cyber-security-inspector-idUSKBN1C92X5.

It also required every agency to appoint a chief information officer and gave then greater accountability for IT planning and operations.[10]

- The 2002 **Federal Information Security Management Act (FISMA)** is a foundational piece of legislation that outlined roles and responsibilities for federal cybersecurity and required agencies to develop, document, and implement programs to secure their information and information systems.[11]

- The 2014 **Federal Information Security Modernization Act (FISMA 2014)** modified the original 2002 law to clarify and update the responsibilities and authorities of DHS and OMB in relation to federal agency information security.[12]

- The **National Cybersecurity Protection Act of 2014** formalized the National Cybersecurity and Communications Integration Center within DHS to interface and share cybersecurity information across federal and non-federal entities.[13]

- The **Federal Information Technology Acquisition Reform Act (FITARA)** of 2014 expanded the authorities of chief information officers (CIOs) and addressed matters like risk management for IT investments, data center consolidation, IT training, and acquisition/procurement.

- The **Cybersecurity Act of 2015** incentivized information sharing between the federal government and private industry, via DHS, by providing liability protections for private sector actors that share threat indicators and defensive measures with DHS. It also required all civilian agencies to implement EINSTEIN, a DHS program to detect and block threats to federal networks.[14]

10 Paul McCloskey. "Clinger-Cohen and the end of the Brooks Act." FCW, September 26, 2016. https://fcw.com/articles/2016/09/26/clinger-cohen-and-the-end-of-the-brooks-act.aspx?m=1.

11 *The E-Government Act of 2002.* Public Law 107-342. December 17, 2002. https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf16.

12 National Institute of Standards and Technology (NIST). FISMA Background. https://csrc.nist.gov/projects/risk-management/detailed-overview.

13 *The National Cybersecurity Protection Act of 2014.* Public Law No 113-282. December 18, 2014. https://www.congress.gov/bill/113th-congress/senate-bill/2519/text/pl.

14 Paul Rosenzweig. "The Cybersecurity Act of 2015." Lawfare, December 16, 2015. https://www.lawfareblog.com/cybersecurity-act-2015.

Partly because of FISMA requirements, the federal government produces a wealth of data on federal cybersecurity. OMB's annual FISMA report is the most comprehensive resource, covering federal performance on topics like cybersecurity incidents, implementation of government-wide cybersecurity initiatives, and progress on information security goals.[15] While it is important to collect such data and understand trend lines, it is equally important to understand the inherent limitations. Confidence in data accuracy is mixed, since agencies can struggle to gather complete and accurate data about their networks. Nor can such data express the full context of where agencies are accepting risk or where they might be most vulnerable.

15 Office of Management and Budget. Federal Information Security Modernization Act of 2014 Annual Report to Congress Fiscal Year 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/briefing-room/presidential-actions/related-omb-material/fy_2016_fisma_report%20to_congress_official_release_march_10_2017.pdf.

Roles and Responsibilities

By law, every federal agency is responsible for its own cybersecurity.[16] But other agencies, especially OMB, the National Institute of Standards and Technology (NIST), DHS, and the General Services Administration (GSA) play cross-cutting roles to support, monitor, or oversee other agencies' implementation of cybersecurity practices. DHS, in particular, plays the primary day-to-day operational role in directing, assisting, and engaging with agencies to implement federal cybersecurity measures.

All these entities interact in a complex and federated fashion with distributed roles and responsibilities. In a simplified model, the sequential interaction between key agencies is:

OMB promulgates government-wide policies.

↓

NIST develops mandatory standards and guidelines for agencies.

↓

Agencies implement policies, standards, and guidelines;

DHS provides operational direction, assistance, and technical capabilities to help them;

GSA aids agencies in obtaining the necessary cybersecurity products and services.

↓

OMB monitors and reports on implementation.

16 *Federal Information Security Modernization Act of 2014*. Public Law 113-283. https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf16.

More specifically:

OMB develops and oversees the implementation of policies, principles, standards, and guidelines on information security. This includes: coordinating the development of standards and guidelines under the National Institute of Standards Technology Act and enforcing their adoption in federal agencies; requiring agencies to identify and provide adequate cybersecurity protections for federal information and information systems; providing data and risk-based oversight federal cybersecurity programs; issuing and implementing federal policies to address emerging IT security risks; working with DHS to reduce adverse impact of major incidents and vulnerabilities on the federal government; and developing memoranda and circulars to promulgate information security policies across the federal government.[17]

In 2016, the Obama Administration announced the creation under the federal CIO of a federal CISO, to focus solely on developing, managing, and coordinating cybersecurity strategy, policy, and operations across the federal government. While the Obama Administration appointed a federal CISO in September 2016, the duration of this appointment was too short to log any major changes or to institutionalize the position. In January 2018, the Trump Administration named its first federal CIO, but as of this writing has not yet named a federal CISO, which means that other individuals, like the new federal CIO and Senior Director for Cybersecurity at the NSC (currently dual-hatted as the Acting CISO), must conduct these responsibilities alongside their other duties.[18]

NIST "develops standards and guidelines for non-national security federal information systems."[19] Although NIST standards for federal systems are mandatory for federal agencies to implement, NIST itself does not have a compliance/oversight role, and does not assess, audit, or test agency security implementations. Among other roles, NIST creates Federal Information Processing Standards, providing federal agencies with guidelines

17 *Federal Information Security Modernization Act of 2014*. Public Law 113-283, Sec. 3553(a)(1). https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf16.

18 Ravindranth, Mohana. "The White House's Cyber Tool List." Defense One. October 5, 2017. http://www.defenseone.com/technology/2017/10/white-houses-cyber-tool-wish-list/141570.

19 *The E-Government Act of 2002.* Public Law 107-342. December 17, 2002. https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf16.

that cover a range of topics like BIOS management and measurement, electronic authentication, wireless protocols, supply chain risk management, and more.[20] Developing these guides through open, multi-stakeholder processes with industry stakeholders aims to help government tap into commercial-off-the-shelf technologies; familiarize industry with government standards; and identify industry best practices to the government.

DHS plays a leadership and operational role, supporting federal civilian agencies in their cybersecurity risk management. [21] DHS plays a vital role in helping secure federal networks. First, DHS seeks to provide a "common baseline" of security (for example, by providing a common set of security services to all agencies, discussed later). Second, DHS acts as a hub for information sharing—for example, sharing indicators of malicious activity as well as best practices—across the federal government and between the government and the private sector.[22] Third, DHS promotes the widespread adoption of NIST guidance and conducts risk assessments with other agencies. Finally, DHS assists other agencies in responding to incidents.

GSA supports federal government agencies by identifying and delivering cybersecurity products and services. This includes, for example, helping agencies by creating standardized methods ("acquisition vehicles") to quickly identify and purchase quality cybersecurity products and services. GSA also helps promote the cybersecurity of connected devices used by federal agencies, like those in buildings or vehicles. One office within GSA, called 18F, "partners with federal agencies to improve the user experience of government" by improving government websites, digitizing internal systems, and fixing technical problems."[23]

---

20 National Institute of Standards and Technology (NIST). Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach. SP 800-37 Rev. 1. February 2010. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf.

21 DHS authorities in federal cybersecurity are derived from the Federal Information Security Modernization Act, the National Cybersecurity Protection Act, and the Cybersecurity Act of 2015. *See* 44 USC §3553, 6 USC §148 *et seq*., and 6 USC §1501 *et seq*., respectively. See https://www.dhs.gov/topic/cybersecurity for an overview of DHS roles & responsibilities.

22 DHS' National Cybersecurity Communications Integration Center (NCCIC) serves as a "federal civilian interface for the multi-directional and cross-sector sharing of information related to cybersecurity risks, incidents, analysis, and warnings for federal and non-federal entities," among other functions.

23 General Services Administration. "About 18F" https://18f.gsa.gov/about/.

Other agencies play critical support roles in federal cybersecurity, including the Department of Defense (DOD), Federal Bureau of Investigation (FBI), and the intelligence community (IC), especially the National Security Agency (NSA).

Information from the intelligence community is vital in helping civilian elements of the federal government to identify, block, and respond to known cyber threats. DOD and NSA can support other agencies, upon request, with defensive assistance and technical expertise. Following an intrusion or attack on federal systems, the FBI would lead any federal investigation. DOD and intelligence agencies are also responsible for securing and defending national security systems, such as classified networks and networks supporting weapons systems, but this responsibility is outside the scope of this paper.

The U.S. Digital Service (USDS) was formed in 2014 to improve the way U.S. citizens interact with government-provided digital services. USDS, which administratively falls under OMB, has active teams at seven federal agencies who seek to identify cost savings and make governments more effective. Though many successful projects focus on improving the user experience with government services, several of the projects also have direct or indirect benefits for federal cybersecurity. These include a GSA-partnered effort to improve and secure the way the public logs in to government services, and a Defense Digital Service program to provide "bug bounties" for security researchers to submit vulnerabilities discovered in Department of Defense (DOD) public-facing websites. (Source: www.usds.gov)

Systemic Challenges

Although roles and responsibilities are generally well understood by the agencies performing them, the complex and federated nature of cybersecurity in the federal government contributes to uneven progress across agencies. Several systemic factors contribute to this dynamic:

1. Difficult tradeoffs between centralized and decentralized management.
2. Varying levels of engagement of agency top leadership on cyber risk management.
3. Varying effectiveness of levers to direct, incentivize, and enforce action by nonperforming federal agencies.
4. Resource constraints and a rigid government budgeting cycle.
5. Scattered congressional oversight.

Challenge #1—Difficult tradeoffs between centralized and decentralized management. The overall federal structure is largely decentralized, though with growing areas of centralized management, such as the use of trusted internet connections (see below). Each agency controls and manages its own connections to the Internet, makes its own decisions about risk, implements its own security solutions, and decides how to handle noncompliance within the agency. This system has contributed to uneven progress across the federal government. On the other hand, full centralization (e.g., putting one agency in charge of a single .gov federal network) would bring its own challenges, such as limiting agencies' ability to develop tailored, agile solutions to their cybersecurity challenges. An important step forward, driven by FISMA 2014, was increasing operational authority allowing DHS to direct other agencies to take steps to mitigate vulnerabilities and reduce risk.

Challenge #2—Varying levels of engagement of agency top leadership on cyber risk management. One of the biggest informal indicators of how well an agency does on managing cyber risk is the level of engagement from the agency head. Successful agency heads develop an awareness of

cyber risk, see cybersecurity as core to executing their missions, and hold their agency accountable. Yet this doesn't come naturally to many, given that cyber risk is difficult to internalize and because agency heads face so many competing demands.

Within agencies, the authorities of CIOs vary widely, with some having centralized authority and others almost entirely lacking in oversight, budget, appointment authority, or control over IT operations across the agency. Legislation enacted in 2014, known as Federal Information Technology Acquisition Reform Act (FITARA), seeks to strengthen the role of CIOs in federal agencies and give them more authority and responsibility for producing IT programs on time and on budget. However, CIOs may still struggle to proactively identify and remediate systemic risks. They may struggle with "shadow IT"—with organizational components connecting devices to federal agency networks without their knowledge.[24] They may lack the ability to institute comprehensive initiatives that address agency-wide problems. And they may struggle to ensure compliance with administration or departmental mandates.

Challenge #3—Varying effectiveness of levers to direct, incentivize, and enforce action by nonperforming federal agencies. The reasons for noncompliance with federal government information security policies—whether they are systemic, bureaucratic, resource, or technical—can often be strong driving forces, and even understandable ones. This is why strong, constant, informal, and formal relationships between agencies, CIOs, DHS, and OMB are a critical part of any effort to improve federal cybersecurity.

DHS and OMB do have levers to drive action by individual agencies. FISMA 2014, for example, was a "game-changer" for giving DHS the authority to issue Binding Operational Directives (BODs). This step is particularly notable insofar as it marked the first time an agency has had the authority to direct other agency heads to take actions to protect their networks. The Secretary of Homeland Security can also issue emergency directives to the head of an agency "to take any lawful action" to protect

24 Shaun Waterman. "DHS Cyber Tool Finds Huge Amount of 'Shadow It' in U.S. Agencies." CyberScoop, April 13, 2017. https://www.cyberscoop.com/dhs-cdm-cyber-tool-finds-huge-shadow-information-technology-federal-agencies/.

information systems, although there are no public indications that this emergency authority has been used to date.

DHS has issued several BODs mandating that agencies take actions, such as patching identified vulnerabilities or, more recently, identifying and removing Kaspersky Lab products.[25] The ability to issue directives like this is important because it provides a formal mechanism to prioritize significant actions, prompt action, and track implementation. BODs have generally been successfully implemented by recipient agencies.[26] However, agency heads are not subject to any defined penalty for failing to adhere to a BOD or emergency directives issued by DHS.

OMB also has levers to direct or incentivize agency behavior. OMB can direct agency action by issuing memoranda on various topics.[27] These memoranda carry the persuasive force of the White House, but, as with BODs, there is no immediate consequence for agency non-compliance. In its annual reports to Congress, OMB can also highlight instances of strong or lagging cybersecurity performance, which can result in Congressional inquiries or hearings and therefore encourage agency action. OMB is also responsible for the federal budget, so to the extent that the federal CIO and agency budget examiners cooperate, OMB can utilize its budget authority to drive greater attention and resources to agency cybersecurity efforts.

While all these levers can be effective, they remain mostly "soft" levers, given that each agency head, by statute, is ultimately responsible and accountable for providing information security protections and making risk management decisions for their agency.

25 Jeanette Manfra. U.S. Congress, House. House Committee on Homeland Security, Subcommittee on Cybersecurity and Infrastructure Protection. *Examining DHS's Cybersecurity Mission*. 115th Congress, October 3, 2017. http://docs.house.gov/meetings/HM/HM08/20171003/106448/HHRG-115-HM08-Wstate-ManfraJ-20171003.pdf.

26 Department of Homeland Security. "Remarks by Secretary of Homeland Security Jeh Charles Johnson on 'Securing The .Gov' at the Center for Strategic and International Studies." July 8, 2015. https://www.dhs.gov/news/2015/07/08/remarks-secretary-homeland-security-jeh-charles-johnson-securing-gov.

27 Office of Management and Budget. Memorandum M-17-09, Management of Federal High Value Assets. December 9, 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-09.pdf.

Challenge #4 –Resource constraints and a rigid government budgeting cycle. Properly resourcing cybersecurity priorities—especially attracting talent and modernizing legacy systems—gets expensive. But in addition to the significant resource constraints affecting these areas, the structure of the government budgeting process also poses challenges for agency cybersecurity efforts.[28] While the Intelligence Community and DOD plan budgets five years out, other agencies are on a one-year budget cycle, which makes it difficult to reliably plan or spread out costs of multi-year investments and modernization efforts. The cycle is also fairly rigid, with limited ability to adapt to emergent needs, which means it can be difficult for agencies to adapt to new cyber threats or problems with legacy IT systems. This is especially so, if those needs emerge outside relatively narrow timeframes each year within which budgeting takes place. There are some techniques, such as the use of working capital funds, to enable more flexible use of funds, but these tend to be difficult to gain Congressional approval for because they are harder to oversee.[29] Legacy IT problems were on one of multiple factors contributing to the disastrous breaches of millions of sensitive records from the Office of Personnel Management, which, according to OPM Director Beth Cobert in January 2017, needed "fundamentally…new systems."[30]

Challenge #5—Scattered congressional oversight. Further complicating the federal cybersecurity landscape is the patchwork of Congressional oversight. The Senate Homeland Security and Governmental Affairs Committee and the House Homeland Security Committee play active roles in federal cybersecurity. Each chamber's armed services, intelligence, or agency-specific committees are also active regarding cybersecurity protections and incidents related to their areas or agencies of interest. And of course, appropriators from each chamber determine the funding available for federal cybersecurity initiatives. In January 2017, Senator Cory Gardner (R-CO) introduced a resolution to create a Select Committee on Cybersecurity to streamline the Senate's oversight, but, the proposal did not make

28 Overall, estimated civilian IT spending for CFO Act agencies in FY2018 vary between $13.8 billion (Department of Health and Human Services) and $100 million (Small Business Administration). The Department of Defense budget was $42.5 billion, or 44.4% of the total IT budget. See https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/budget/fy2018/ap_16_it.pdf.

29 Working funds could enable organizations to spread out equipment costs over multiple years or replace equipment when needed vice the year they've been budgeted.

30 Billy Mitchell. "How Beth Cobert resurrected OPM IT after historic cyber breaches." FedScoop, January 18, 2017. https://www.fedscoop.com/beth-cobert-opm-cyber-improvement/.

it through committee.[31] The result of scattered oversight is not simply a reporting burden on agencies. It also means that no congressional body has the full picture of federal cybersecurity measures, and that legislative requirements are spread across many bills, making it more complicated for federal agencies to adapt to threats or adopt new approaches.

31 U.S. Congress. Senate. *A resolution establishing the Select Committee on Cybersecurity*. S.Res.2. 115th Congress, 2017. https://www.congress.gov/bill/115th-congress/senate-resolution/23.

2. Major Federal Cybersecurity Initiatives

The federal government, motivated by a string of intrusions and failures over the last five years (see Appendix A), has driven a series of initiatives to improve cybersecurity at federal agencies. Three initiatives in 2015 and 2016, the Cybersecurity Sprint, the Cybersecurity Strategy Implementation Plan (CSIP), and the Cybersecurity National Action Plan (CNAP)—formed the core of the Obama Administration's response.[32] The Trump Administration built upon these initiatives, tasking additional work in the May 2017 Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure and making several notable moves on shared services and cloud adoption. This section reviews these broad efforts and delves into the most prominent initiatives in federal cybersecurity.

Although this paper focuses on progress in recent years, it must be noted that the foundation of many current programs lie with the January 2008 Comprehensive National Cybersecurity Initiative (CNCI) by the George W. Bush administration.[33] The CNCI was reaffirmed by the Obama Administration's Cyberspace Policy Review, and continued several years thereafter.[34] Some see failures in the CNCI. It did not fully engage the range of actors necessary, like many of the civilian agency leaders, necessary for effective implementation. Nonetheless, several initiatives, such as managing federal networks as a single enterprise, deploying intrusion detection and prevention systems across the federal enterprise, and better coordinating cybersecurity research and development—claim roots in the CNCI.

32 These initiatives are by no means the only major initiatives, just the most recent. Information on major past initiatives—including the Bush Administration's Comprehensive National Cybersecurity Initiative (CNCI) of 2008; the CSIS Task Force on Cybersecurity for the 44th Presidency; and the Obama Administration 60-Day Cyberspace Policy Review of 2009—had significant impact on cybersecurity over the last several years.

33 The White House. National Security Presidential Directive/NSPD-54, Homeland Security Presidential Directive/HSPD-23. *Cybersecurity Policy.* January 8, 2008. https://fas.org/irp/offdocs/nspd/nspd-54.pdf.

34 Obama White House Archives. *The Comprehensive National Cybersecurity Initiative*. https://obamawhitehouse.archives.gov/sites/default/files/cybersecurity.pdf.

Driving Overall Progress, 2015-2018

In June 2015 following the OPM intrusion, the federal CIO launched a 30-day **Cybersecurity Sprint** to address the need for quick and dramatic progress in key areas. During the Sprint, the federal CIO directed agencies to (1) immediately scan systems and check logs against DHS indicators of priority threat-actor techniques, tactics, and procedures; (2) patch certain critical vulnerabilities; (3) tighten policies and practices for privileged users; and (4) accelerate the use of multi-factor authentication, especially for privileged users.[35]

The Sprint, while modest overall, demonstrated that the federal government can close key gaps in cybersecurity when it is collectively focused on discrete, high-priority actions. By its end, nine agencies had achieved the goal of strong authentication for 100% of privileged users, with fifteen reaching the goal by the spring of 2016. Agencies also accelerated implementation of a May 2015 DHS directive to mitigate critical vulnerabilities in Internet-facing systems, resolving nearly all active critical vulnerabilities identified at the time of the directive by the end of 2015.[36] During the Sprint, agencies also conducted scans for indicators of compromise; identified a certain set of high value assets; and completed reviews of privileged users.[37]

A major output of the Cyber Sprint was the development of OMB's **Cybersecurity Strategy and Implementation Plan (CSIP)**, released in October 2015, which set forward a further series of short term actions to improve federal cybersecurity.[38] The CSIP established objectives and tasked key actions related to the protection of high value assets and information; the detection, response, recovery, and lessons-learned from cyber incidents;

35 Tony Scott "Strengthening & Enhancing Federal Cybersecurity for the 21st Century." White House Blog post. July 15, 2015. https://obamawhitehouse.archives.gov/blog/2015/07/31/strengthening-enhancing-federal-cybersecurity-21st-century.

36 Binding Operational Directive 15-01, "Critical Vulnerability Mitigation." May 21, 2015. https://cyber.dhs.gov/bod/15-01/.

37 Office of Management and Budget. Federal Information Security Modernization Act of 2014 Annual Report to Congress Fiscal Year 2016. (8-10), https://www.whitehouse.gov/sites/whitehouse.gov/files/briefing-room/presidential-actions/related-omb-material/fy_2016_fisma_report%20to_congress_official_release_march_10_2017.pdf.

38 Office of Management and Budget "Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government" Memorandum M-16-04. October 30, 2015. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf.

the recruitment and retention of cyber talent; and the acquisition and deployment of technology.

Finally, in February 2016, the Obama Administration announced a broad-based initiative, the **Cybersecurity National Action Plan (CNAP)**, which included many of the efforts begun during the Sprint and CSIP as well as additional federal and private sector projects. The CNAP announcement accompanied a $19 billion investment set forth in the FY2017 President's Budget.[39] The CNAP included a proposed $3.1 billion Information Technology Modernization Fund (ITMF); establishment of a federal Chief Information Security Officer (CISO); continued identification and review of highest value and most at-risk IT assets; an increase in government-wide shared services for IT and cybersecurity; expansion of DHS EINSTEIN and Continuous Diagnostics and Mitigation (CDM) programs; an increase in DHS federal civilian cyber defense teams to a total of 48; and an investment in cybersecurity workforce programs to support federal government needs.[40] Many agencies met the 2016 milestones set out by the CNAP, but most initiatives continue today.

As part of the CNAP, president Obama signed an executive order establishing a bipartisan **Commission on Enhancing National Cybersecurity** to make detailed recommendations to strengthen cybersecurity, including cybersecurity in federal government.[41] In December 2016, the commission published a series of recommendations and action items to, among other imperatives, "better equip government to function effectively and securely in the digital age." Federally-focused recommendations included: consolidating basic network operations; promoting technology adoption and tech refresh in the federal sector; maturing federal agencies' approach to enterprise risk management; realigning White House leadership positions for

39 "Fact Sheet: Cybersecurity National Action Plan." February 9, 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

40 "Fact Sheet: Cybersecurity National Action Plan." February 9, 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

41 Executive Order 13718. *Commission on Enhancing National Cybersecurity*. February 9, 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity.

cybersecurity; and further clarifying federal roles and responsibilities for cyber incidents.[42]

Most recently, the Trump Administration's May 2017 **Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure** set out expectations and principles for risk management and tasks detailed reviews by each agency. Notably, the president "will hold [agency heads] accountable for managing cybersecurity risk to their enterprises. In addition, because risk management decisions made by agency heads can affect the risk to the executive branch as a whole, and to national security, it is also the policy of the United States to manage cybersecurity risk as an executive branch enterprise." [43] The order required agency heads to adhere to the NIST Framework for Improving Critical Infrastructure Cyber Security, resolving a longstanding irritant for industry members, who were contractually held to the NIST standards even when the government was not. It tasked all agencies to provide a risk management report to OMB, which would then be reviewed comprehensively by DHS and OMB, with a final report due to the President in October 2017 on how to address insufficiencies or misalignments.[44]

Although this executive order demonstrated significant continuity from the last administration, the efforts it directs may drive change in areas like enterprise risk management and preference for shared services. These areas were reinforced in the Administration's National Security Strategy, released in December 2017, which identifies building defensible government networks as a priority. In doing so, it states: "[the government] will use the latest commercial capabilities, shared services, and best practices to modernize our Federal information technology. We will improve our ability to

42 Report on Securing and Growing the Digital Economy. Commission on Enhancing National Cybersecurity. December 1, 2016. https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf.

43 Executive Order 13800. *Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.* May 11, 2017. Section 1. https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal.

44 Executive Order 13800. *Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.* May 1,, 2017. Section 1.c. https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal.

provide uninterrupted and secure communications and services under all conditions." [45]

Modernizing Information Technology (IT)

The federal government relies on legacy IT systems that are both difficult to secure and expensive to maintain. In May 2016, the GAO reported that such legacy investments were becoming increasingly obsolete, with the use of outdated programming languages (such as COBOL); old parts (including 8-inch floppy disks); and unsupported hardware and software (such as Microsoft operating systems from the 1980s and 1990s).[46] The ten oldest IT investments or systems reported to GAO ranged from 39-56 years old. The GAO assessed that of the more than $80 billion spent per year across the federal government, 77 percent went to operations and maintenance of systems and 23 percent to development, modernization, and enhancement. This reflected a 9 percent increase in operations and maintenance since 2010, and an overall reduction of $7.3 billion in development, modernization, and enhancement in that same period.[47] In other words, a relatively large and increasing proportion of the federal IT budget is spent just keeping the old systems running.

Both the Obama and Trump Administrations acknowledged challenges of legacy IT and set out strategies for IT modernization. The federal CIO recently issued a draft Report to the President on IT Modernization, which was circulated for industry comment in fall 2017.[48] The vision outlines actions to consolidate and modernize networks, adopt shared services to enable future network architectures, and realign resources for

45 The White House. *National Security Strategy of the United States of America*. December 2017. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf.

46 United States Government Accountability Office. *Information Technology: Federal Agencies Need to Address Legacy Systems*, GAO 16-468. May 2016. http://www.gao.gov/assets/680/677436.pdf.

47 United States Government Accountability Office. *Information Technology: Federal Agencies Need to Address Legacy Systems*, GAO 16-468. May 2016. http://www.gao.gov/assets/680/677436.pdf.

48 U.S. Federal CIO. Report to the President on Federal IT Modernization. 2017. https://itmodernization.cio.gov/assets/report/Report%20to%20the%20President%20on%20IT%20Modernization.pdf.

modernization priorities.[49] The plan offers useful priorities, such as emphasizing high-risk high-value assets and modernizing the system by which agencies connect to the Internet. However, it also relies on the "realignment" of resources, rather than the addition of new resources; this may be insufficient given the magnitude of the task.

A prominent feature of the government's modernization approach has been the establishment of a "revolving fund," also known as a "working capital fund," to support IT modernization goals. Revolving funds offer greater flexibility for agencies, allowing them to spend money on modernization projects with the assumption that they will be able to repay the investment over time as they replace costly, antiquated systems with more modern, efficient ones.[50] By this logic, the Obama Administration estimated that its proposed $3.1 billion fund would support an estimated $12 billion worth of modernization projects over ten years.[51]

Most recently, the Modernizing Government Technology (MGT) Act, sponsored by Representative Will Hurd of Texas, in 2018 passed into law as part of the National Defense Authorization Act bill.[52] This act establishes a valuable revolving fund that will help agencies make upgrades and longer-term investments. The amount authorized, $500 million, is much less than what is ultimately required to overcome the federal governments legacy IT debt. This means that Congress' work isn't finished. But the fund offers a critical foundation for future investments.[53]

49 U.S. Federal CIO. Report to the President on Federal IT Modernization. 2017. https://itmodernization.cio.gov/assets/report/Report%20to%20the%20President%20on%20IT%20Modernization.pdf.

50 "Fact Sheet: Cybersecurity National Action Plan." February 9, 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

51 Michael Daniel, Tony Scott, Ed Felten. "The President's National Cybersecurity Plan: What You Need to Know." White House Blog post. February 9, 2016. https://obamawhitehouse.archives.gov/blog/2016/02/09/presidents-national-cybersecurity-plan-what-you-need-know.

52 The office of William Hurd. "Hurd's Landmark IT Overhaul Approved by Senate." Press Release. 18 September 2017. https://hurd.house.gov/media-center/press-releases/breaking-hurd-s-landmark-it-overhaul-approved-senate.

53 U.S. Congress. House. *National Defense Authorization Act for Fiscal Year 2018*. HR 2810. 115th Congress, 2017. https://www.congress.gov/bill/115th-congress/house-bill/2810/text.

Identifying and Protecting High Value Assets

Both the Obama and Trump administrations have required federal agencies to identify and prioritize their highest value and most at-risk IT assets, and then to take additional steps to improve their security.[54] [55] The U.S. Government developed a definition of a high value asset (HVA) and a list of attributes to consider when determining whether an asset, dataset, or repository is of high value. All civilian CFO Act agencies reported their HVAs to DHS, which conducted vulnerability assessments for more than 20 of the most consequential sets of assets in FY2016 and has continued conducting assessments through FY2017. Through these assessments, DHS, in partnership with an agency's CIO, conducts penetration testing and other types of risk assessments, provides specific findings and recommendations, and helps agencies develop a remediation plan for identified vulnerabilities. Due to the decentralized nature of federal government in cybersecurity, the primary responsibility for remediation remains with each agency, as does continued monitoring and assessments of the HVAs. To assist with this, GSA developed a contract vehicle for agencies to procure pre-vetted cybersecurity risk assessments based upon a common methodology established by DHS and NSA.[56] This vehicle is intended to help agencies conduct regular, recurring assessments of high value assets.

These steps to identify and harden high value assets are important. But some agencies are beginning to shift from a mindset of "protecting assets" to a more holistic approach of "protecting missions." The Department of Defense, for example, is adapting its traditional mission assurance methodology to better identify and manage cyber risks to military missions. This kind of mindset helps to identify cyber risk from assets that aren't individually considered high value--whether those assets are networks, weapons system components, information databases, embedded cyber-physical systems, or electrical and communications infrastructure--but that

54 "Fact Sheet: Cybersecurity National Action Plan." February 9, 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

55 Executive Order 13800. *Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.* May 11,2017. Section 1.c. https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal.

56 General Services Administration. "Highly Adaptive Cybersecurity Services (HACS)" https://www.gsa.gov/portal/content/151154.

nonetheless could disrupt an agency from performing a key function. It is unclear whether agencies are focused in this way, for example looking at immigration for DHS, investigations for FBI, food safety inspections for the Department of Agriculture.

Leveraging Shared Services and Commercial Technologies

In the context of federal cybersecurity, shared services are IT or cybersecurity services that are used by multiple agencies or entities. Examples of shared services could include mobile security, cloud computing, digital rights management, encryption services, and provisioning of core IT services like Domain Name Service resolution. Shared services reduce the need for individual agencies or components to negotiate, procure, and manage those services on their own. Benefits include reduced complexity across the federal government, better cost-sharing, a stronger negotiating position (due to increased collective buying power), and more efficient operations. Shared services also help the federal government standardize and simplify cybersecurity measures.

The federal government has pushed for greater use of shared services since the early 1980s.[57] More recently, in 2011, OMB directed each federal agency to shift to shared services in at least two areas of the agency's choice.[58] In 2012, the White House Federal IT Shared Services Strategy set out a "full range and lifecycle" strategy for shared services adoption.[59] Later, in 2016, the CNAP set a goal for shared services to help take "each individual agency out of the business of building, owning, and operating their own IT when more efficient, effective, and secure options are available."[60] The 2017

57 U.S. Federal CIO. Report to the President on Federal IT Modernization. 2017. (17) https://itmodernization.cio.gov/assets/report/Report%20to%20the%20President%20on%20IT%20Modernization.pdf.

58 Executive Office of the President. "Federal Information Technology Shared Services Strategy." 2 May 2012. https://www.dhs.gov/sites/default/files/publications/digital-strategy/shared-services-strategy.pdf.

59 Executive Office of the President. "Federal Information Technology Shared Services Strategy." 2 May 2012. https://www.dhs.gov/sites/default/files/publications/digital-strategy/shared-services-strategy.pdf.

60 "Fact Sheet: Cybersecurity National Action Plan." February 9, 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

Trump Administration's cyber EO goes the furthest yet, explicitly directing agencies to prioritize shared services. The subsequent draft Report to the President on Federal IT Modernization in August 2017 set out a goal that agencies build new capabilities "only when shared services and commercial technologies cannot meet mission need."[61]

In particular, smaller agencies greatly benefit from shared services because they lack the resources and workforce to manage and secure individual services on their own. The U.S. government has been experimenting with increases in managed IT services to dozens of the small federal (non-CFO Act) agencies. Such services can help raise the overall cybersecurity of these often under-resourced agencies, many of which handle sensitive data sets. If these pilot programs are successful in standardizing a level of managed security services, more of the small agencies could join.

Converging with the trend toward shared services is a trend toward the increasing adoption of commercial capabilities, including email and cloud services. On one hand, private sector services can offer sophisticated protections that government does not have available in house. On the other hand, these services may not account for unique federal cybersecurity needs or challenges such as ensuring access to information about security events, enabling reporting on potentially malicious use activity, or enabling the use of USG programs like EINSTEIN. The report to the president on Federal IT Modernization strongly encourages the use of commercial technology and lays out several actions to reduce barriers to its adoption.

Since 2007, a significant area of work has been the federal government's push to use trusted internet connections (TICs).[62] [63] Under the TIC initiative, the federal government has reduced its number of internet connection points from several thousand to less than a hundred, with the goal of

61 U.S. Federal CIO. Report to the President on Federal IT Modernization. 2017. https://itmodernization.cio.gov/assets/report/Report%20to%20the%20President%20on%20IT%20Modernization.pdf.

62 Office of Management and Budget. "Implementation of Trusted Internet Connections." Memorandum M-08-05. 20 November 2007. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-05.pdf.

63 Office of Management and Budget. "Update on the Trusted Internet Connections Initiative." Memorandum M-09-32. 17 September 2009. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/memoranda_fy2009/m09-32.pdf.

reducing to a target of 50 connections.[64] The high-level idea is that, by using a smaller number of internet connections, it becomes easier to set common security standards for those connections, as well as to monitor and block threats traveling through those connections. Every TIC deployed today must adhere to security standards developed by OMB and deploy sensor technologies and analytic tools provided by DHS.[65] According to 2009 data, there were twenty agencies that OMB had designated as TIC Access Providers, each of which could manage up to two of their own internet access points.[66] Although some TIC Access Provider agencies, such as the State Department, support other small agencies,[67] most smaller agencies that can't manage their own trusted internet connections procure those services from outside vendors. The federal government is currently working to make it easier and more cost effective for small agencies to obtain such services, as well as to adapt the TIC strategy to increased use of the cloud.[68]

Shared services and commercial technologies, however, do not come without risk. In 2015, in the process of shifting IT operations to a third party, the Swedish Transport Agency accidentally exposed large amounts of information, including classified information, to foreign nationals.[69] And in March 2017, Gizmodo reported that a DOD contractor had uploaded sensitive but unclassified files onto a publically accessible cloud environment, including unencrypted user credentials.[70] Good policies and oversight

64 Eric Chabrow. "What's Happening with the Trusted Internet Connection?" Gov Info Security, March 1, 2010. https://www.govinfosecurity.com/interviews.php?interviewID=45.

65 U.S. Federal CIO. Report to the President on Federal IT Modernization. 2017. (11) https://itmodernization.cio.gov/assets/report/Report%20to%20the%20President%20on%20IT%20Modernization.pdf.

66 Department of Homeland Security. "TIC Update for the Information Security and Privacy Board." July 29, 2009. https://csrc.nist.gov/CSRC/media/Events/ISPAB-JULY-2009-MEETING/documents/ispab_july09-donelan_tic-external-connections.pdf.

67 Department of Homeland Security. "TIC Update for the Information Security and Privacy Board." July 29, 2009. https://csrc.nist.gov/CSRC/media/Events/ISPAB-JULY-2009-MEETING/documents/ispab_july09-donelan_tic-external-connections.pdf.

68 U.S. Federal CIO. Report to the President on Federal IT Modernization. 2017. (10-16) https://itmodernization.cio.gov/assets/report/Report%20to%20the%20President%20on%20IT%20Modernization.pdf.

69 "Sweden data leak 'a disaster', says PM" BBC News, July 24, 2017. http://www.bbc.com/news/technology-40705473.

70 Dell Cameron, "Top Defense Contractor Left Sensitive Pentagon Files on Amazon Web Server With No Password," Gizmodo, May 31, 2017, https://gizmodo.com/top-defense-contractor-left-sensitive-pentagon-files-on-1795669632.

are thus important to guide the transition and implementation of greater shared services and commercial technologies.

Detecting and Blocking Threats at the Perimeter

Although federal government agencies are responsible for their own cybersecurity, DHS has the statutory mission to provide a common set of baseline security measures across the government and to help agencies manage their cyber risk.[71] One of DHS's signature initiatives is the EINSTEIN program, which aims to detect and block adversaries at the perimeter before they can compromise federal agencies. To do this, EINSTEIN leverages known cyber threat indicators, such as e-mail addresses used to send spear phishing emails, or internet protocol (IP) addresses known to be used by malicious actors.

The first two versions of EINSTEIN, which are fully deployed for all federal civilian traffic routed through a TIC, use unclassified indicators to detect malicious traffic. EINSTEIN 3 Accelerated (E3A), which includes classified indicators, is completing deployment through the primary Internet Service Providers serving the federal government. Although DHS must have each agency's voluntary consent to provide cybersecurity services such as EINSTEIN, the Cybersecurity Act of 2015 required all federal civilian agencies to implement EINSTEIN 3A by December 18, 2016. Secretary Jeh Johnson stated in early 2017 that EINSTEIN 3A covered 93 percent of the civilian workforce of the executive branch.[72]

Past DHS officials have cited the OPM breach as an example of EINSTEIN's success: after the initial malicious indicators from the first OPM breach were identified, those indicators helped EINSTEIN detect the

71 DHS authorities in federal cybersecurity are derived from the Federal Information Security Modernization Act, the National Cybersecurity Protection Act, and the Cybersecurity Act of 2015. *See* 44 USC §3553, 6 USC §148 *et seq*., and 6 USC §1501 *et seq.*, respectively. See https://www.dhs.gov/topic/cybersecurity for an overview of DHS roles & responsibilities.

72 "Statement by Secretary Johnson Concerning the Deployment of Einstein 3A" January 11, 2017. https://www.dhs.gov/news/2017/01/11/statement-secretary-johnson-concerning-deployment-einstein-3a.

second breach.[73] However, agencies have expressed frustration over: (1) insufficient speed of incorporating known cyber threat information into the system; and (2) the difficulty of detecting previously *unknown* cyber threats. To address the first challenge, DHS has pursued a program to more quickly ingest cyber threat indicators from non-federal entities in real-time, known as Automated Indicator Sharing (the program, in return, also shares indicators with the private sector). To do this, DHS has established a system to share and receive "machine-readable" cyber threat indicators automatically and in real time, using a common format known as STIX/TAXII. To address previously unknown threats, DHS is "developing advanced malware and behavioral analysis capabilities that will automatically identify and separate suspicious traffic for further inspection, even if the precise indicator has not been seen before."[74]

Identifying and Fixing Vulnerabilities and Risk Factors Inside Agency Networks

Whereas EINSTEIN detects and blocks threats at the perimeter, another DHS signature initiative, the Continuous Diagnostics and Mitigation (CDM) program, identifies vulnerabilities and risk factors inside agency networks.[75] Through the CDM program, DHS purchases commercial cybersecurity tools for federal agencies. These tools identify and catalog devices on agency networks and check for vulnerabilities (Phase 1), manage identities, accounts, and privileges (Phase 2), identify and manage suspicious activity inside agency networks (Phase 3) and help secure sensitive / high value data (Phase 4).[76]

---

73 Testimony of Andy Ozment, Department of Homeland Security. Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies. "DHS' Efforts to Secure .Gov" 114th Congress, June 24, 2015. http://docs.house.gov/meetings/HM/HM08/20150624/103698/HHRG-114-HM08-Wstate-OzmentA-20150624.pdf.

74 Testimony of Andy Ozment, Department of Homeland Security. U.S. Congress, House. Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies. "DHS' Efforts to Secure .Gov" 114th Congress, June 24, 2015. http://docs.house.gov/meetings/HM/HM08/20150624/103698/HHRG-114-HM08-Wstate-OzmentA-20150624.pdf.

75 DHS Continuous Diagnostics and Mitigation (CDM) Program Briefing, http://csrc.nist.gov/groups/SMA/forum/documents/dec2013/gmoore_dec2013_managers-forum.pdf.

76 Testimony of Jeanette Manfra, Department of Homeland Security. U.S. Congress, House. Committee on Homeland Security, Subcommittee on Cybersecurity and Infrastructure Protection. *Examining DHS's Cybersecurity Mission*. 115th Congress, October 3, 2017. http://docs.house.gov/meetings/HM/HM08/20171003/106448/HHRG-115-HM08-Wstate-ManfraJ-20171003.pdf.

The CDM program aims to achieve three benefits. First, CDM helps federal government agencies acquire commercial cyber security tools in a cost-effective way. Second, it enables the use of common sensors across the federal civilian government. This allows agencies to track and report on the same types of data with the same degree of validity. Third, CDM will more quickly feed vulnerability information to DHS, so it can track agency progress in mitigating critical issues and understand risk trends across the executive branch.

DHS has provided Phase 1 tools—which identify agencies' hardware and software assets and associated vulnerabilities—to participating federal civilian agencies. In FY2016, DHS provided new CDM Phase 2 tools to a total of 65 agencies and aimed to provide the balance of Phase 2 tools to agencies in FY17.[77] Through FY18, DHS will provide agencies with tools covering CDM Phase 3. CDM Phase 4 remains in the planning phase. Information from CDM tools is fed both to a dashboard at each agency and in real-time to DHS's NCCIC, along with information to help agencies prioritize their mitigation efforts.

While most federal agencies and CIOs appear to support the objectives and intent of the CDM program, some have expressed frustrations that the program is not sufficiently fast-moving and agile to meet their needs.[78] Others find elements of the program, like pre-pricing tools and services, hard to manage because of the difficulty in predicting what will really be needed.[79] Critics will be looking toward August 2018, when the original contract for CDM expires, for DHS to evolve the program to address these challenges.[80] An ongoing conversation about governance and oversight issues will be necessary for CDM to fully realize the aims of the program.

77 Department of Homeland Security. "FY2018 Budget in Brief." 2017. https://www.dhs.gov/sites/default/files/publications/DHS%20FY18%20BIB%20Final.pdf.

78 Jason Miller. "The CDM quandary many agencies are facing." Federal News Radio. August 24, 2015. https://federalnewsradio.com/contractsawards/2015/08/cdm-quandary-many-agencies-facing/.

79 Jason Miller. "CDM suffering growing pains so GSA, DHS begin future planning." Federal News Radio. May 16, 2016. https://federalnewsradio.com/reporters-notebook-jason-miller/2016/05/cdm-suffering-growing-pains-gsa-dhs-begin-future-planning/.

80 Jason Miller. "CDM program to get facelift to fix problems with initial $6B contract." Federal News Radio. March 27, 2017. https://federalnewsradio.com/reporters-notebook-jason-miller/2017/03/cdm-program-get-facelift-fix-problems-initial-6b-contract/.

Improving Incident Management

The July 2016 Presidential Policy Directive 41 (PPD-41) on U.S. Cyber Incident Coordination was a significant step forward in codifying and communicating U.S. government principles, roles, and responsibilities governing the federal government's response to any cyber incident.[81] PPD-41 leverages an Incident Severity Schema to assess cybersecurity incidents based on upon actual or potential impact on public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.[82] It further outlines roles and responsibilities for incident response, including:

- The Department of Justice (DOJ) is the lead federal agency for "threat response," including "the law enforcement and national security investigation of a cyber incident."
- DHS has the lead for "asset response," including "providing technical assets and assistance to mitigate vulnerabilities and reducing the impact of the incident, identifying and assessing the risk posed to other entities and mitigating those risks, and providing guidance on how to leverage Federal resources and capabilities."
- The Office of the Director of National Intelligence (ODNI) has the lead for "intelligence support," including "intelligence collection in support of investigative activities, and integrated analysis of threat trends and events."
- Any "affected federal agency" will have primary responsibility to "engage in a variety of efforts to manage the impact of the cyber incident" such as maintaining business and operational continuity.

Although much of PPD-41 contemplates federal government response to incidents involving critical infrastructure owners and operators (and therefore out of scope of this report), the fourth bullet on the "affected

81 *Presidential Policy Directive -- United States Cyber Incident Coordination.* PPD-41. July 26, 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

82 Obama White House Archives, "Cybersecurity Incident Severity Schema." https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/Cyber%2BIncident%2BSeverity%2BSchema.pdf.

federal agency" reinforces the general rule that each agency is responsible for managing its own cybersecurity and incident response. Should there be multiple federal agencies involved in a given incident, one could expect that DHS and DOJ would play coordination roles, including through the Unified Cyber Coordination Group, to enhance communication and coordination among the multiple affected federal agencies. (See additional details in the National Cyber Incident Response Plan.[83])

In terms of resources for responding to incidents within a federal agency, the affected agency would first draw upon its own internal personnel and contractors for incident response. DHS, through NCCIC, may provide assistance, typically in cases where agency capacity is exhausted, the incident has a national security nexus, the affected asset is particularly critical, or the incident involves a threat actor of particular significance. (In order to reduce deployment time in an emergency, federal agencies are required to maintain a standing Federal Network Authorization with DHS.[84]) In the 2016 CNAP, the Obama administration announced an intent to increase DHS' cyber defense teams from 10 to 48. The Trump Administration's proposed FY2018 budget would add $42.3 million and 20 personnel to the NCCIC, with some of those resources going to building the cyber defense teams. However, it seems unlikely that the requested figure would resource the full 48 teams.[85]

DHS and the GSA have also developed a contract vehicle to enable agencies to have "quicker access to key, pre-vetted support services," which would be particularly beneficial in urgent situations like network compromises.[86] This includes, for example, easier access to private contract services for incident response (to determine the extent of a compromise

83 U.S.-CERT. "National Cyber Incident Response Plan." December 2016. https://www.us-cert.gov/ncirp.

84 Office of Management and Budget. "Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements." Memorandum M-16-03. October 30, 2015. (10) https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-03.pdf.

85 Department of Homeland Security. "FY2018 Budget in Brief." 2017. https://www.dhs.gov/sites/default/files/publications/DHS%20FY18%20BIB%20Final.pdf.

86 General Services Administration. "Highly Adaptive Cybersecurity Services (HACS)" https://www.gsa.gov/portal/content/151154.

and remove an adversary from systems) and hunt services (to determine what other systems an adversary may have compromised).[87]

Finally, the U.S. government has also begun establishing and exercising policies for civilian agencies to request defensive assistance from DOD. If called upon (and available), DOD would likely turn to the Cyber Protection Teams on U.S. Cyber Command's National Mission Force, or perhaps its Reserve Component forces, to provide the necessary assistance to other agencies. However, more work is needed to develop greater clarity on specific circumstances or thresholds when DOD forces would be likely to get involved in other agencies' incident response.

87 General Services Administration. "Highly Adaptive Cybersecurity Services (HACS)" https://www.gsa.gov/portal/content/151154.

3. Foundations of Federal Cybersecurity

No major cybersecurity initiative, like those described above, can be successful without the right people, technology, and leadership to set out a vision, implement that vision effectively, and adapt to new threats. Setting the right foundations for strong cybersecurity, therefore, is arguably even more important than individual initiatives. This section outlines major efforts in the areas of enhancing the federal cyber workforce; building a foundation through research and development; modernizing acquisition and procurement; and promoting leadership, accountability, and a culture of cybersecurity.

Enhancing the Federal Cyber Workforce

Although current federal cyber workforce gaps are not publically available, there may be up to a 10,000 person gap in the federal government.[88] Challenges that federal agencies cite include long lag times created by clearance processes, constraints imposed by inflexible human resources processes, and the need to "re-adjudicate" clearances that were granted by other agencies. Inadequate incentives make hiring difficult, especially when competing for professionals who can earn more in the private sector. Bureaucratic challenges may have an even greater impact, because of the uncertainty and delay on potential employee's livelihoods.

As part of the CNAP, the FY2017 president's budget proposed $62 million in programs to either directly or indirectly help the federal government recruit and retain cybersecurity talent with technical, policy, and leadership skillsets. Initiatives included an expansion of the CyberCorps program, which offers scholarships for Americans who wish to obtain cybersecurity education and serve their country in the civilian federal government; development of a cybersecurity core curriculum for academic institutions; a strengthened National Centers for Academic Excellence in Cybersecurity Program; enhanced student loan forgiveness

88 Author interview with former OMB officials in 2016.

for cybersecurity experts joining the federal workforce; and investment in cybersecurity education through the President's Computer Science for All initiative.[89] It is unclear the extent to which funding for these programs were also included in the Trump administration's FY2018 budget.

The National Initiative for Cybersecurity Education (NICE) is a NIST-led partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. NICE published the National Cybersecurity Workforce Framework in 2017, which offers a "common lexicon" by which to classify cybersecurity workers and serves as a resource for guidance on cybersecurity workforce programs.[90] NICE manages a number of other projects, such as Cyber Seek, a tool to visualize cybersecurity job and worker availability;[91] regional alliances and multi-stakeholder partnerships; education conferences and expos; and designation of cybersecurity centers of excellence.[92]

On July 12, 2016, the Obama White House released the Federal Cybersecurity Workforce Strategy, which detailed government-wide actions to identify, expand, recruit, develop, retain, and sustain a capable and competent workforce in key functional areas to address complex and ever-evolving cyber threats. The strategy also identified new approaches to address persistent federal workforce challenges. The Action Plan for the Strategy tasked out 22 specific actions, over 12 months, supporting four broad goals of (1) identifying workforce needs; (2) expanding the workforce through education and training; (3) recruiting and hiring highly skilled talent; and (4) retaining and developing highly skilled talent.[93]

89 Shaun Donovan, Beth Cobert, Michael Daniel, Tony Scott. "Strengthening the Federal Cybersecurity Workforce" White House Blog post. July 12, 2016. https://obamawhitehouse.archives.gov/blog/2016/07/12/strengthening-federal-cybersecurity-workforce.

"Fact Sheet: Cybersecurity National Action Plan." February 9, 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

90 National Institute of Standards and Technology. "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework." SP. 800-181. August 2017. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.

91 CyberSeek tool. http://cyberseek.org/index.html#partners.

92 National Initiative for Cybersecurity Education (NICE) website. https://www.nist.gov/itl/applied-cybersecurity/nice (accessed October 2017).

93 Shaun Donovan, Beth Cobert, Michael Daniel, Tony Scott. "Strengthening the Federal Cybersecurity Workforce" White House Blog post. July 12, 2016. https://obamawhitehouse.archives.gov/blog/2016/07/12/strengthening-federal-cybersecurity-workforce.

The July 2016 strategy may well be incorporated into and superseded by studies coming out of the Trump Administration's Executive Order on Strengthening Cybersecurity, which directs a report on the sufficiency of efforts to build the cybersecurity workforce.[94] The executive order also directs a report on the workforce development efforts of "potential foreign cyber peers" by the ODNI. Taken together, these reports are expected to enable a better understanding of long-term U.S. cyber workforce competitiveness and establish the new administration's cyber workforce strategy.

Some agencies, most notably DHS and DOD, have been able to obtain critical expanded authorities for more flexible and streamlined hiring of skilled cybersecurity personnel. The Border Patrol Pay Agent Reform Act of 2014 authorizes the Secretary of Homeland Security to establish cybersecurity positions in the excepted service and set the compensation scale for such positions.[95] OPM has also authorized DHS to hire cybersecurity personnel under Direct Hire Authorities and waive competitive hiring requirements such as listing a position on USAJobs.com and veteran's preference criteria.[96] The FY2016 NDAA also authorized the Secretary of Defense to establish certain civilian positions supporting U.S. Cyber Command as excepted service positions.[97] DoD has now set and started implementing its policy for such hiring.[98]

The U.S. government has also increasingly leveraged "crowdsourcing" methods to access talent outside government. In April 2016, DOD, under Secretary Ash Carter, conducted its "Hack the Pentagon" bug bounty pilot, in which security researchers were paid to discover and submit vulnerabilities on DOD systems. Over the course of 24 days, security researchers "hacked" five public-facing DOD websites, including the main DOD website. The program exceeded expectations, with 1,410 participants, 138

94 Executive Order 13800. *Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.* May 11, 2017. Section 1.c. https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal.

95 *See* 6 U.S.C. §147.

96 *See generally* Kathryn A. Francis et al. The federal Cybersecurity Workforce: Background and Congressional Oversight Issues for the Departments of Defense and Homeland Security. Congressional Research Service. 8 January 2016.

97 *National Defense Authorization Act for Fiscal Year 2016,* Section 1107. Public Law 114–92. https://www.congress.gov/114/plaws/publ92/PLAW-114publ92.pdf (Codified at 10 USC 1599f).

98 DoD Instruction 1400.25, Volume 3001. *DoD Civilian Personnel Management System: Cyber Excepted Service (CES) Introduction*. August 15, 2017. http://fedne.ws/uploads/JiD1mdkwCP.

valid/unique reports submitted, and 58 hackers paid 117 bounties totaling $75,000 and a total program cost of $150,000.[99] By late 2016, DOD had developed a contract avenue that has since enabled multiple components, including the Army and Air Force, to run similar bounties. DOD also encouraged source code contracted by DOD to go through a bug bounty.[100] Bug bounties are not the solution for every agency, however, because the influx of vulnerability reports over a short period of time requires a fairly mature capability for vulnerability management.

Another promising crowdsourcing approach has been the development of vulnerability disclosure programs for federal systems. These programs allow members of the public—many of whom would never or could never work in the federal government—to report vulnerabilities discovered in federal systems without fear of prosecution. DOD established the first such program in 2016 by establishing a disclosure policy, process, and portal for vulnerability submission.[101] It has produced tangible results, with thousands of vulnerabilities reported through this channel, including dozens of high or critical severity.[102] Unlike bug bounties, no payments are made to security researchers, but disclosure programs are not cost-free either. Agencies must ensure good communication with participants for ingesting and managing vulnerabilities and reporting back on their remediation; otherwise participants can quickly lose interest. Every federal agency—on the principle that it is better to know about your vulnerabilities than to remain ignorant of them—could build toward a vulnerability disclosure policy, drawing upon a Department of Justice framework published in July 2017.[103]

99 U.S. Department of Defense. "Defense Secretary Ash Carter Releases Hack the Pentagon Results." NR-225-16. June 17, 2016. https://www.defense.gov/News/News-Releases/News-Release-View/Article/802929/defense-secretary-ash-carter-releases-hack-the-pentagon-results/.

100 Shannon Collins. U.S. Department of Defense. "DoD Announces 'Hack the Pentagon' Follow-Up Initiative" October 20, 2016. https://www.defense.gov/News/Article/Article/981160/dod-announces-hack-the-pentagon-follow-up-initiative/.

101 "DOD Vulnerability Disclosure Policy" HackerOne. https://hackerone.com/deptofdefense.

102 Presentation of the author at the George C. Marshall Center Cyber Security Studies Program, February 2017.

103 Department of Justice. "A Framework for a Vulnerability Disclosure Program for Online Systems" July 2017. https://www.justice.gov/criminal-ccips/page/file/983996/download.

Building a Foundation through Research and Development (R&D)

The federal government is an important driver of basic research and development on technology priorities for the nation. This is true in the cyber domain as well. The results of federal R&D investments can change how network defenders do their jobs, including those within the U.S. government itself, for example, through adopting greater automation, detecting anomalous behavior, analyzing data, and reducing software vulnerabilities.

The 2016 Federal Cybersecurity R&D Strategic Plan built on efforts to coordinate cyber R&D efforts sponsored or conducted by the USG in order to eliminate redundancies in federally funded cybersecurity research, identify research gaps, set priorities for R&D efforts, and ensure return on taxpayer investments.[104] The plan set near-term (1-3 years), mid-term (3-7 years), and long-term (7-15 years) objectives for deterring, protecting, detecting, and adapting to malicious cyber activities."[105] These R&D objectives are not specifically oriented in support of the federal government, but several would benefit federal agencies, such as:

- Develop secure update mechanisms that support the full range of product formats, applications, and lifecycles. (Near-term)
- Discover and apply automated tools to map networks, including entities, attributes, roles, and logical relationships between processes and behaviors. (Near-term)
- Use data analytics to identify malicious cyber activities and differentiate them from authorized user behavior with low false positive and false negative rates. (Mid-term)
- Create tool chains that support development of software with one defect per hundred thousand lines of code with a relative efficiency

104 The plan was developed by the Office of Science & Technology Policy (OSTP) and National Science and Technology Council (NSTC). It builds upon an effort first generated through the 2008 Comprehensive National Cybersecurity Initiative (CNCI).

105 Greg Shannon, Tim Polk. "National Challenges and Goals for Cybersecurity Science and Technology" White House Blog post, February 9, 2016. https://obamawhitehouse.archives.gov/blog/2016/02/08/national-challenges-and-goals-cybersecurity-science-and-technology.

metric of 90 percent for productivity and system performance. (Long-term)

It remains unclear how much support these objectives are receiving under the Trump Administration. An August 2017 memorandum outlining the Administration's R&D priorities for FY2019 mentions cyber only briefly.[106]

A range of other federal initiatives are aimed at driving high-reward innovations. As part of the Defense Advanced Research Projects Agency (DARPA) Cyber Grand Challenge in August 2016, teams from around the world competed to "automate the cyber defense process, fielding the first generation of machines that can discover, prove and fix software flaws in real-time, without any assistance."[107] Seven high-performance computers competed against one another in the first all-computer Capture the Flag exercise, offering insights into how sophisticated automation might affect cybersecurity in the future. In August 2016, seven teams competed to test their machines' automated self-defense capabilities.[108] These kinds of innovations—especially those related to automation and machine learning—could have major impacts in the next 5-10 years on how both businesses and governments secure their networks, and hold the potential to shift the advantage from the attacker to the defender.

Modernizing Acquisition and Procurement

The federal government spends hundreds of billions of dollars a year for goods and services. This means that the federal government is a significant customer able to use its purchasing power to effect change in support of greater cybersecurity. On the other hand, this power only goes so far in influencing the overall global market (<1 percent) and can be weakened

106 Office of Management and Budget. "FY 2019 Administration Research and Development Budget Priorities." Memorandum M-17-30. August 17, 2017. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-30.pdf.

107 For more information, see the Cyber Grand Challenge website at https://www.cybergrandchallenge.com/.

108 DARPA, "The World's First All-Machine Hacking Tournament." http://archive.darpa.mil/cybergrandchallenge/.

by varied or uncoordinated acquisition requirements across federal agencies.[109]

The Federal Acquisition Regulations (FAR) are the set of regulations governing all acquisitions and contracting procedures in the federal government. The FAR requires agency heads to prescribe procedures to ensure that IT acquisitions comply with FISMA, OMB, and NIST standards and guidance on cybersecurity. The Defense Federal Acquisition Regulations Supplement (DFARS) expands requirements for contractors to safeguard controlled unclassified information, requires contractors be compliant with NIST 800-171, requires contractors to report certain cyber incidents, and requires protection of contractor information provided to DOD in response to a cyber incident.[110]

Nonetheless, challenges abound in federal agencies' acquisition and procurements systems. Acquisition processes architect systems without adequate focus on cybersecurity, which means agencies have to cobble together cybersecurity "fixes" later on. Many acquisition processes are culturally prone to favor "features" in systems, which increase opportunities for compromise. (Take, for example, the F-35's suite of integrated sensors, electronic warfare capabilities, surveillance and reconnaissance capabilities, radar, targeting systems, helmet mounted displays, and more.[111]) At minimum, the federal government could benefit from processes to better ensure that IT components and systems have the requisite trustworthiness necessary for the nation's most critical and sensitive missions.

The acquisition community, like others, faces a shortage in skilled cybersecurity-minded talent. There aren't enough acquisition professionals or program management professionals with experience in software product development, which means that acquisition decisions can provide inadequate weight to cybersecurity.[112] Another challenge is that in-house employees and contract vendors are guided by different incentives, where

109 Author's interview with GSA officials, October 2016.

110 Office of the Deputy Assistant Secretary of Defense for Systems Engineering. "Guidance for Stakeholders for Implementing Defense Federal Acquisition Supplement Clause 252.204-712 (Safeguarding Controlled Unclassified Technical Information)" August 2015. http://www.acq.osd.mil/se/docs/DFARS-guide.pdf.

111 Lockheed Martin. "About the F-35." https://www.f35.com/about/capabilities.

112 Author's interview with the Defense Digital Service, October 2016.

in-house employees may have greater incentives to focus on cybersecurity. Finally, there remains a distinction in the acquisition community between "development" vs "sustainment" contracts for IT, which creates an illusion that software and other IT products can be considered "complete" instead of requiring constant maintaining.[113]

Promoting Leadership, Accountability, and a Culture of Cybersecurity

Just as CEOs are getting more involved in cyber risk management, leaders of federal agencies are getting increasingly involved. Having an engaged agency head is likely to indicate an overall healthier cybersecurity posture in any given agency. But top leaders have many competing priorities, as well as a significant learning curve to develop comfort with making risk management decisions about cybersecurity. There remains a need for better tools for decision-making, as well as executive education.

The Obama Administration kept senior leaders engaged on cybersecurity discussions by discussing cybersecurity at OMB-led CIO Council and Deputy-level meetings of the President's Management Council (PMC).[114] The Trump Administration reinforced its attention to hold agency heads accountable for cybersecurity, and has directed all agencies to submit a "senior accountable official" for cybersecurity risk management.[115] This kind of high-level, sustained engagement can at least keep a spotlight on federal agency cybersecurity and serve as a forcing function for agencies to keep senior leaders engaged on the issues.

OMB manages an overall scorecard to track the cybersecurity posture of federal agencies, through the PMC and via FISMA reporting.[116] Multiple other agencies, like DOD and DOJ, have developed internal dashboards or

113 Author's interview with the Defense Digital Service, October 2016.

114 General Services Administration. "President's Management Council (PMC)" https://www.gsa.gov/node/85931.

115 Office of Management and Budget. "Reporting Guidance for Executive Order on Strengthening Cybersecurity of Federal Networks and Critical Infrastructure." Memorandum M-17-25. 19 May 2017. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/M-17-25.pdf.

116 Author interview with DHS officials, September 2017.

scorecards to track their own progress. However, maintaining agency focus on cybersecurity requires leadership and sustained engagement from the very top of the organization. But few senior leaders have the training, tools, or subject matter comfort level to truly take ownership of cybersecurity risk management for their agencies.

DOD's Cybersecurity Scorecard is one example of a tool for senior-most leaders to drive understanding and accountability for cybersecurity.[117] The Scorecard is managed by the CIO, provided monthly to the Deputy Secretary and quarterly to the Secretary, and discussed in senior leader forums several times per year. It was developed following analysis that a high percentage of known intrusions or intrusion attempts into DOD networks took advantage of failures in basic cyber hygiene. The Scorecard currently scores DOD components on key areas of cyber hygiene, but over time will expand to depict the status of the cybersecurity of core DOD mission areas, such as nuclear command and control; space; position, navigation and timing; and ballistic missile defense, as well as other critical areas like workforce and acquisition.[118]

While top-down attention has been central to the increased attention within agencies on cybersecurity issues, there are arguments for also pursuing broader culture change down to the user level. DOD has an example initiative underway that aims to reinforce, for all employees across DOD, principles of integrity, level of knowledge, procedural compliance, formality and backup, and a questioning attitude.[119]

4. Moving Forward

117 Department of Defense. "Improving Cyber Basics: DoD Cyber Discipline Implementation Plan and DoD Cyber Scorecard" December 2016. http://dodcio.defense.gov/Portals/0/Documents/Cyber/CNDSP%20Plain%20Language%20Overview%20-%20DISTRO.pdf?ver=2017-01-31-125734-897.

118 Department of Defense. "DoD Cybersecurity Discipline Implementation Plan" February 2016. http://dodcio.defense.gov/Portals/0/Documents/Cyber/CyberDis-ImpPlan.pdf.

119 Department of Defense. "Department of Defense Cyber Culture and Compliance Initiative (DC3I)" September 28, 2015. https://www.defense.gov/Portals/1/Documents/pubs/OSD011517-15-RES-Final.pdf. These principles were drawn from other endeavors that have inculcated high levels of personnel reliability into daily operations.

Federal cybersecurity is a dense, inaccessible topic to those outside the information security community and even to some inside it. A more holistic understanding of the topic will help policymakers, agency leaders, cybersecurity professionals, and congressional staff make smart public policies and better manage cyber risk to federal government systems. In pursuing these efforts, practitioners should consider the following themes:

- **Sound risk management underpins all federal cybersecurity efforts**. Federal agencies cannot and will not prevent every incident or intrusion. Nor should every database or network be protected to the same degree. Agencies must prioritize their efforts. This requires identifying the most important assets and missions that support the nation and its citizens, then crafting tailored strategies to reduce, mitigate, or accept the risks.
- **Sustained, high-level leadership from agency heads is critical to success.** Cybersecurity risks affect agencies' fundamental ability to perform their key missions and functions. Risk decisions, therefore, are too important to be made solely at low levels in an agency or even by agency chief information officers. Agencies with engaged department heads or deputies are much more likely to use resources strategically, force mission or business owners to attend to cybersecurity, and empower chief information officers to take steps needed to protect systems and enforce standards.
- **Effective management demands clarity on roles and responsibilities.** The federal cybersecurity system is complex, with many agency roles and responsibilities. This is not inherently bad but it does demand constant effort to refine, clarify, and institutionalize roles and responsibilities to ensure coherence and effectiveness.
- **Steady, incremental progress makes a difference.** The Cyber Sprint in 2016, modest as it was, demonstrated that agencies can make progress when held accountable for discrete milestones, especially on issues of basic cyber hygiene often exploited by intruders.
- **Some areas, however, require constant innovation, or even a fundamental "rethink."** Innovative ideas are filtering up on areas like tapping outside expertise, improving cybersecurity in procurement,

and educating executives on cyber risk management. The most advanced agencies have policies that reward and implement such ideas.

- **Congress plays a critical role**. Legislation sets the fundamental principles of how the federal government manages its cybersecurity, and Congress authorizes and appropriates agency missions, authorities, and budgets. Very little can be done without strong support and engagement from the legislative branch.
- **Resources matter**. All agencies and Congress must steward cybersecurity resources wisely and find new efficiencies. Skimping on resources for modernizing networks or attracting cybersecurity talent will reduce the ability of agencies to secure their core missions, with real impacts to both government and citizens.
- **Evolving technology will change the game**. Innovation in the digital ecosystem, like automation, will bring both new threats and new defensive applications. The government will need to plan for these trends in the 5- to 10-year timeframe to keep from lagging behind.

There are no silver bullets for federal cybersecurity. The system will retain its inherent complexity, necessitating close coordination and partnership. Federal cybersecurity will be an enduring mission, always evolving and changing to stay ahead of the threat. In other words, there is no "finish line"—only continual improvement, adaptation, and cooperation to secure the federal government and those it serves.

Appendix:
Timeline of Federal Civilian Cybersecurity Incidents, 2012—2017

January 2012—Federal Bureau of Investigation, DHS, and U.S. Copyright Office
DDoS claimed by hacker group Anonymous takes multiple websites offline.

February 2012—Federal Bureau of Investigation
Hacker group Anonymous eavesdropped and posted online a call between FBI and Scotland Yard.

April 2012—Department of Commerce
Unknown intruders infected the Department of Commerce networks with a virus.

July 2013—Department of Energy
Hackers exploited vulnerabilities in Adobe software and stole personal data of around 150,000 individuals.

August 2014—Department of Health and Human Services
HHS server that supported the Obamacare website was attacked.

October 2014—White House
Non-classified, sensitive information accessed.

November 2014—National Oceanic and Atmospheric Agency
Four websites of the agency compromised

November 2014—U.S. Postal Service
800,000 employees' personal data compromised.

November 2014—State Department
Data pilfered from unclassified system.

May 2015—Internal Revenue Service
Around 800,000 accounts compromised.

June 2015—Office of Personnel and Management
Two intrusions—one compromised information of 4.2 million current/former government employees, the other compromising information of 21.5 million employees/contractors.

January 2016—Internal Revenue Service
Malicious actor tried to generate Electronic Filing Personal Identification Numbers (PINS) based on stolen information.

December 2016—U.S. Election Assistance Commission (EAC)
Malicious actor attempted to sell over 100 stolen access credentials.

April 2017—Internal Revenue Service
Up to 100,000 taxpayers had sensitive information stolen due to faulty data retrieval tool on the Free Application for Student Aid (FAFSA).

September 2017—Securities and Exchange Commission (SEC)
Malicious actors breached the SEC's EDGAR database, "used by companies to file earnings reports and other material information," possibly enabling insider trading.

This list was compiled using the following sources:

Rosenzweig, Paul "Significant Cyber Attacks on Federal Systems -- 2004-present" Lawfare. May 7, 2012. https://www.lawfareblog.com/significant-cyber-attacks-federal-systems-2004-present.

Rosenzweig, Paul; Inserra, David. "Continuing Federal Cyber Breaches Warn Against Cybersecurity Regulation" October 27, 2015. The Heritage Foundation. http://www.heritage.org/defense/report/continuing-federal-cyber-breaches-warn-against-cybersecurity-regulation.

Office of Management and Budget. Federal Information Security Modernization Act of 2014 Annual Report to Congress Fiscal Year 2016. (8—10) https://www.whitehouse.gov/sites/whitehouse.gov/files/briefing-room/presidential-actions/related-omb-material/fy_2016_fisma_report%20to_congress_official_release_march_10_2017.pdf.

Daitch, Heidi "2017 Data Breaches—The Worst So Far" IdentityForce. November 27, 2017. https://www.identityforce.com/blog/2017-data-breaches.

"Here's the Latest About What the SEC Hackers Stole" Fortune. September 25, 2017. http://fortune.com/2017/09/25/sec-hacker-stole/.

Nakashima, Ellen. "New details emerge about 2014 Russian hack of the State Department: It was 'hand to hand combat'" Washington Post. April 3, 2017. https://www.washingtonpost.com/world/national-security/new-details-emerge-about-2014-russian-hack-of-the-state-department-it-was-hand-to-hand-combat/2017/04/03/d89168e0-124c-11e7-833c-503e1f6394c9_story.html?utm_term=.20989f0287a9.

Barysevich, Andrei "Russian-Speaking Hacker Selling Access to the US Election Assistance Commission" Recorded Future. December 15, 2016. https://www.recordedfuture.com/rasputin-eac-breach/.

Nakashima, Ellen. "Hackers breach some White House computers" Washington Post. October 28, 2014. https://www.washingtonpost.com/world/national-security/hackers-breach-some-white-house-computers/2014/10/28/2ddf2fa0-5ef7-11e4-91f7-5d89b5e8c251_story.html?utm_term=.2dcb919d98f1.

Nakashima, Ellen. "China suspected of breaching U.S. Postal Service networks" Washington Post. November 10, 2014. https://www.washingtonpost.com/news/federal-eye/wp/2014/11/10/china-suspected-of-breaching-u-s-postal-service-computer-networks/?utm_term=.9f019ee34ff6.

The Cyber Security Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 John F. Kennedy Street
Cambridge, MA 02138

www.belfercenter.org/Cyber

Printed in the United States of America