Congressional Research Service
Informing the legislative debate since 1914

TESTIMONY

Statement of

Chris Jaikaran
Analyst in Cybersecurity Policy

Before

Committee on Veterans' Affairs
Subcommittee on Technology Modernization
U.S. House of Representatives

Hearing on

"Cybersecurity and Risk Management at VA: Addressing Ongoing Challenges and Moving Forward"

May 20, 2021

Congressional Research Service
7-5700
www.crs.gov
<Product Code>

Chair Mrvan, Ranking Member Rosendale, and Members of the subcommittee, thank you for the opportunity to testify before you today. My name is Chris Jaikaran. I am an analyst in cybersecurity policy at the Congressional Research Service (CRS) with a focus on national cybersecurity policy and federal agency cybersecurity. I have been in this role at CRS since 2015. CRS provides Congress with analysis that is authoritative, confidential, objective, and nonpartisan. Any arguments presented in my written or oral testimony are provided for the purposes of informing Congress, not to advocate for a particular policy outcome.

My testimony today addresses the principles of risk management agencies consider when developing cybersecurity programs, federal agencies and policies involved with the Department of Veteran's Affairs (VA) cybersecurity, and options for Congress.

Introduction

VA provides a variety of services and benefits to veterans across the nation. These services and benefits include: healthcare for 9.3 million enrollees; disability compensation for 5.7 million veterans and their survivors; life insurance for 5.8 million veterans, servicemembers and their families; pension benefits for 392,000 veterans and survivors; educational assistance for 950,000 people; and interment services for 137,000 eligible people.[1] In delivering these services, VA stores, transmits, and processes, sensitive information—such as protected health information (PHI) and personally identifiable information (PII)—for millions of Americans. The VA provides these services at more than 5,000 owned facilities, over 1,000 leased facilities, and through many other private-sector partner organizations.[2]

This array of disparate services delivered to millions of customers requires the support of many information technology (IT) systems. VA maintains over 6,000 approved IT tools (e.g., software) in its inventory to assist the department in fulfilling its missions.[3] The volume of customers, number of facilities, and large inventory of IT systems creates unique complexities in developing, implementing, and monitoring a cybersecurity program at VA. Adding to this complexity is the variety of endpoints that VA must secure. Consumer IT (e.g., laptops and smartphones), enterprise IT (e.g., network routers and servers), Internet of Things devices (e.g., internet-enabled security cameras) and medical devices (e.g., blood pressure monitors) constitute VA's inventory of devices, all of which present a potential attack vector and as such require security.

Cybersecurity Principles

Cybersecurity is a risk management process rather than a static goal. It involves continual work to: (1) identify; (2) protect; (3) detect; (4) respond; and (5) recover from potential and actual cybersecurity incidents. Agencies may choose to evaluate their IT risks by understanding the threats they are susceptible to, the vulnerabilities they have; and the consequences of a successful attack on their mission and to their customers.

The Office of Management and Budget (OMB) describes cybersecurity for federal agencies as follows.[4]

[1] Department of Veterans Affairs, "VA 2021 Budget Request: Fast Facts," document, at https://www.va.gov/budget/docs/summary/fy2021VAsBudgetFastFacts.pdf.

[2] Department of Veterans Affairs, "FY2021 Budget Submission: Budget in Brief," document, February 2020, at https://www.va.gov/budget/docs/summary/fy2021VAbudgetInBrief.pdf.

[3] Department of Veterans Affairs, "About IT at VA," webpage, January 20, 2021, at https://www.oit.va.gov/about/.

[4] Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular No. A-130, Washington, DC, 2016, p. 28, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf.

> ‘Cybersecurity’ means prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation.

Prior to purchasing a cybersecurity tool or implementing a new process agencies must first understand what data and systems they possess, how that data and those systems may be attacked, how likely those attacks are, and what challenges the agency may face if its data and systems are impaired. This assessment helps to ensure that the agency is taking a proactive approach to cybersecurity in a resource limited environment. Agencies may consider threats, vulnerabilities, and consequences against the cybersecurity tenets of confidentiality, integrity, and availability (i.e., the C-I-A triad).

The concepts of “confidentiality,” “integrity,” and “availability” are defined in U.S. Code as part of “information security”.[5]

- *Confidentiality* refers to the attribute that data are known only to authorize parties and not made available or disclosed to unauthorized parties.
- *Integrity* refers to the attribute that data have not been altered or destroyed in an unauthorized manner.
- *Availability* refers to the attribute that data are available for access by an authorized party when they choose.

These terms apply to the data stored, processed, and transmitted by IT systems, but also to the IT systems themselves. A fourth term for information security is sometimes discussed as a pillar of cybersecurity: *authentication,* or the ability to confirm that parties using a system and accessing data are who they claim to be and have legitimate access to that data and system. A fifth term, *non-repudiation* refers to the ability of a sender of data to confirm delivery and a recipient to confirm the sender’s identity, so that neither can deny having processed the data.

Elements to ensure cybersecurity involve policies spanning a range of fields, including education, workforce management, investment, entrepreneurship, and research and development. Software development, law enforcement, intelligence, incident response, and national defense may be involved in the response, when something goes awry in cyberspace.

Federal Agencies Relevant to VA Cybersecurity

The Federal Information Security Modernization Act of 2014 (FISMA, P.L. 113-283)[6] delineates the federal roles and responsibilities for the cybersecurity of civilian agencies (commonly referred to as the “.gov” space). Primary roles reside with the Office of Management and Budget (OMB), U.S. Department of Homeland Security (DHS), the National Institute of Standards and Technology (NIST), each agency, and the agency’s inspector general (IG). In this model, OMB provides agencies strategic support, DHS, provides agencies operational support, and each agency executes its own tactical-level cybersecurity actions.

The Office of Management and Budget, exercising its oversight of agency budgets, is responsible for overseeing agency adoption of cybersecurity practices and guiding agencies to a cybersecurity posture commensurate to their risk. Through its budgetary authority, OMB enforces the adoption of cybersecurity practices by directing the expenditure of funds for this purpose. OMB may also install new senior

[5] These definitions are at 44 U.S.C. §3552.

[6] 44 U.S.C. Chapter 35, Subchapter II.

officials to oversee mismanaged cybersecurity programs, but CRS was unable to find an instance of OMB exercising that authority.[7] OMB also annually reports to Congress on overall agency cybersecurity performance and provides summaries of agency evaluations.[8]

The Department of Homeland Security oversees agency adoption of cybersecurity programs, provides tools to protect agency networks, and coordinates government-wide efforts on federal cybersecurity. DHS also mandates agencies take certain cybersecurity actions on their networks to mitigate immediate risks or implement processes to improve their overall cybersecurity.

Agency heads are ultimately responsible for ensuring that risks are effectively managed in their own organization, with cybersecurity being one such risk (financial and operational risk are among the others). In accordance with FISMA, agency heads shall delegate the responsibility for cybersecurity to a senior official, frequently a chief information security officer.[9]

The National Institute of Standards and Technology develops standards (i.e., the Federal Information Processing Standards) and guidance (i.e., Special Publications) to inform agencies of security practices to adopt.[10] Agencies are compelled to adopt these standards.[11] But, NIST is not responsible for ensuring agency adoption, OMB is.[12] NIST's standards and guidance are also applicable to agency contractors and any other organization that is operating a system or processing data on behalf of the federal government.

Inspectors General annually evaluate their agency's cybersecurity programs and provide recommendations on improving their agency's cybersecurity posture. The Comptroller General may also periodically evaluate and report to Congress on agency information security policies and practices.

Policies Relevant to VA Cybersecurity

VA is subject to a variety of federal government-wide and agency-specific laws and guidance that address cybersecurity. Brief discussions of laws and guidance that are maximally applicable are below. Additionally laws and guidance may apply under certain conditions, but are not discussed here.

Federal Laws

Three federal statutes establish the main principles under which federal agencies and the VA secure their IT equipment and networks, and data. Primarily, these laws establish roles and responsibilities across the federal government.

The Federal Information Security Modernization Act of 2014 (FISMA)[13] establishes roles and responsibilities for federal agency information technology security. Broadly, agency heads are ultimately responsible for the security of their agency's IT, but may delegate those responsibilities to a senior agency official. In implementing their IT security programs, agencies must follow guidance issued by OMB and

[7] 40 U.S.C. §11303.

[8] For an example, see Office of Management and Budget, "Federal Information Security Modernization Act 2014: Annual Report to Congress," *FISMA FY 2019 Annual Report to Congress*, May 2020, at https://www.whitehouse.gov/wp-content/uploads/2020/05/2019-FISMARMAs.pdf.

[9] 44 U.S.C. §3554, (a) (3) (A).

[10] NIST, "FIPS Publications," website, October 16, 2015, at http://csrc.nist.gov/publications/PubsFIPS.html. And NIST, "Special Publications," website, April 8, 2016, at http://csrc.nist.gov/publications/PubsSPs.html.

[11] 15 U.S.C. §278g—3.

[12] 44 U.S.C. §3553.

[13] 44 U.S.C. §§3551-3559.

standards promulgated by NIST. DHS is authorized to assist agencies in their IT security programs, and each agency's inspector general must produce an annual evaluation of the agency's cybersecurity. For fiscal year 2020 the VA IG examined the VA's compliance with FISMA.[14] That report made 26 recommendations to improve the agency's cybersecurity, three of which were new and 23 of which were carryovers from prior years. FISMA does not require agencies to implement specific cybersecurity strategies or use certain tools.

The Federal Information Technology Acquisition Reform Act of 2014 (FITARA)[15] expands the role of chief information officers (CIOs) in managing agency IT investments. Specifically, it requires CIOs to review and approve IT acquisitions for their agency and exercise governance and oversight over IT planning, programming, budgeting, and execution (PPBE) activities. While not primarily a cybersecurity law, it also requires CIOs to work with OMB to identify and improve the risk management of IT investments. The VA IG recently evaluated the VA's implementation of FITARA and made 10 recommendations.[16]

The Department of Veterans Affairs Information Security Enhancement Act of 2006[17] amplifies the VA's responsibilities under FISMA. It establishes additional responsibilities for the VA's leadership, including: the Secretary; Under Secretaries; Assistant Secretaries; the Assistant Secretary for Information and Technology; the Associate Deputy Assistant Secretary for Cyber and Information Security; and the Inspector General. It also establishes requirements for independent analysis, notifications, and remediation in the event of a data breach.

The Privacy Act of 1974[18] governs how agencies may collect and retain an individual's records and how they may or may not disclose that information to another party.

Agency Guidance

OMB, DHS and the VA develop and promulgate guidance for the VA's IT managers, each providing a different perspective. OMB provides broad, strategic guidance, while DHS provides operational guidance to help agencies implement laws and guidance. Agencies produce policies and procedures to tactically execute a cybersecurity program against a backdrop of existing laws and guidance.

OMB Guidance

OMB issues memoranda and circulars, which agencies follow for IT security.

[14] Department of Veterans Affairs Office of Inspector General, *Federal Information Security Modernization Act Audit for Fiscal Year 2020*, Report #20-019727-104, Washington, DC, March 31, 2020, at https://www.va.gov/oig/pubs/VAOIG-20-01927-104.pdf.

[15] 40 U.S.C. §§11302, 11315, and 11319; and 44 U.S.C. §3601.

[16] Department of Veterans Affairs Office of the Inspector General, *VA's Implementation of the FITARA Chief Information Officer Authority Enhancements*, Report #18-04800-122, Washington, DC, June 9, 2020, at https://www.va.gov/oig/pubs/VAOIG-18-04800-122.pdf.

[17] 38 U.S.C. §§5721-5728. The Department of Veterans Affairs Information Security Enhancement Act of 2006 is Title IX of the Veterans Benefits, Health Care, and Information Technology Act (P.L. 109-461).

[18] 5 U.S.C. §552a.

OMB Circular A-108: ***Federal Agency Responsibilities for Review, Reporting, and Publication Under the Privacy Act.***[19] The Privacy Act of 1974[20] requires OMB to release additional guidance for agencies to comply with the Privacy Act. Circular A-108 establishes guidance for systems of records notices (SORNs),[21] reporting SORNs to OMB and Congress, implementation rules, exceptions, and how to account for the Privacy Act in other reporting.

OMB Circular A-123: ***Management's Responsibility for Enterprise Risk Management and Internal Control***[22] and ***Appendix A: Management of Reporting and Data Integrity Risk***[23] require agencies to identify and manage any risk to agency operations that may arise. Agencies may manage risk through the development and use of risk profiles and periodic reporting.

OMB Circular A-130: ***Management of Information as a Strategic Resource***[24] establishes general policy for the programming, planning, budgeting, and execution (PPBE) of IT resources (e.g., hardware, software, and personnel) that will use federal information. It includes appendices for the protection of federal information resources and managing personally identifiable information.

OMB M-21-02: ***Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements***[25] provides guidance to agencies on implementing FISMA. It directs agencies to track certain metrics and use the Continuous Diagnostics and Mitigation (CDM)[26] dashboard provided by DHS, and includes reporting requirements.

DHS Guidance

DHS issues Binding Operational Directives (BODs) for federal agencies to implement for the protection and security of federal information and IT systems. DHS is authorized to issue these compulsory directions under FISMA.[27] A selection of BODs that apply broadly over time is included below.

BOD 18-02: ***Securing High Value Assets***[28] is a DHS order that requires agencies to: identify and report their high value IT assets to DHS; allow DHS to assess the security of those assets; and mitigate any vulnerabilities DHS finds within 30 days.

[19] Office of Management and Budget, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, Circular A-108, at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A108/omb_circular_a_108_12_12_16.pdf.

[20] 5 U.S.C. §552a.

[21] A SORN is published by an agency when it develops or modifies a system (usually an IT system) that maintains a record about an individual.

[22] Office of Management and Budget, *OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control*, M-16-17, Washington, DC, July 15, 2016, at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf.

[23] Office of Management and Budget, *Appendix A to OMB Circular No. A-123, Management of Reporting and Data*, M-18-16, Washington, DC, June 6, 2018, at https://www.whitehouse.gov/wp-content/uploads/2018/06/M-18-16.pdf.

[24] Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular No. A-130, Washington, DC, July 28, 2016, at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf.

[25] Office of Management and Budget, *Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements*, M-21-02, Washington, DC, November 9, 2020, at https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-02.pdf.

[26] Cybersecurity and Infrastructure Security Agency, Continuous Diagnostics and Mitigation (CDM), website, at https://www.cisa.gov/cdm.

[27] 44 U.S.C. §3553.

[28] Cybersecurity and Infrastructure Security Agency, *Securing High Value Assets,* Binding Operational Directive 18-02, May 7,

BOD 19-02: ***Vulnerability Remediation Requirements for Internet-Accessible Systems***[29] is a DHS order that requires agencies to review and mitigate DHS-found vulnerabilities on internet-accessible IT systems within 30 days of notification.

BOD 20-01: ***Develop and Publish a Vulnerability Disclosure Policy***[30] is a DHS order that requires agencies to create and publish polices on how the public can identify vulnerabilities in federal IT systems and alert the agency of the potential risk. The VA is currently in compliance with the order.[31] Three systems are within scope for security research: va.gov, vets.gov, and ehrm.va.gov. Per the order, VA is expected to add systems to the policy every three months with all agency internet-accessible systems being within scope by September 2022.

VA Guidance

The VA is required to document its IT security practices. The VA accomplishes this through Handbooks and Directives.

VA Directive 6500: ***VA Cybersecurity Program***[32] describes the cybersecurity program for VA systems that the VA operates pursuant to FISMA. VA Directive 6500 establishes governance structures for risk management, including roles, responsibilities, and procedures.

VA Handbook 6500: ***Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program***[33] provides the processes VA IT system owners will follow to identify and select the security and privacy controls applicable to the system(s) for which they are responsible.

VA Handbook 6500.6: ***Contract Security***[34] establishes responsibilities and requirements for IT security in the VA's contracts and acquisitions. It asserts that vendors who access VA information or IT systems must abide by federal and VA guidance, including in the event of a cybersecurity incident such as a data breach.

Standards

The VA is subject to standards and guidance developed by the NIST.[35] NIST standards for federal agencies may be published as a Federal Information Processing Standard (FIPS), NIST Interagency Report (NISTIR), or Special Report (SP). A selection of widely applicable NIST documents is provided below.

2018, at https://cyber.dhs.gov/bod/18-02/.

[29] Cybersecurity and Infrastructure Security Agency, *Vulnerability Remediation Requirements for Internet-Accessible Systems*, Binding Operational Directive 19-02, April 29, 2019, at https://cyber.dhs.gov/bod/19-02/.

[30] Cybersecurity and Infrastructure Security Agency, *Develop and Publish a Vulnerability Disclosure Policy*, Binding Operational Directive 20-01, September 2, 2020, at https://cyber.dhs.gov/bod/20-01/.

[31] Department of Veterans Affairs, "Vulnerability Disclosure Policy: Department of Veterans Affairs," webpage, February 22, 2021, at https://www.va.gov/vulnerability-disclosure-policy/.

[32] Department of Veterans Affairs, *VA Cybersecurity Program*, VA Directive 6500, January 23, 2019, at https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=1003&FType=2.

[33] Department of Veterans Affairs, *Risk Management Framework for VA Information Systems - Tier 3: Information Security Program*, VA Handbook 6500, Washington, DC, March 10, 2015, at https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=793&FType=2.

[34] Department of Veterans Affairs, *Contract Security*, VA Handbook 6500.6, March 12, 2010, at https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=471&FType=2.

[35] 15 U.S.C. §278g–3 and 40 U.S.C. §11331.

FIPS Publication 199: ***Standards for Security Categorization of Federal Information and Information System***[36] is a standard federal agencies must follow to assess the agency's information and the IT systems, so that appropriate security measures may be applied.

FIPS Publication 200: ***Minimum Security Requirement for Federal Information and Information Systems***[37] is a complementary standard to FIPS PUB 199. It provides the 17 minimum security requirements agencies must follow for IT systems.

NISTIR 8170: ***Approaches for Federal Agencies to use the Cybersecurity Framework***[38] provides examples that agencies may follow to use the *Framework for Improving Critical Infrastructure Cybersecurity*[39] in accordance with Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.*[40]

SP 800-37: ***Risk Management Framework for Information Systems and Organizations***[41] provides a risk management framework for agencies to follow to determine a security categorization for an IT system. Security categorizations are based on the information security principles of confidentiality, availability, and integrity[42] and are recorded as *low*, *moderate*, or *high.* The security categorizations inform which security measures an IT system must use.

SP 800-53: ***Security and Privacy Controls for Information Systems and Organizations***[43] provides agencies with a catalog of security and privacy requirements agencies must implement for their IT systems.

[36] National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS Pub 199, Gaithersburg, MD, February 2004, at https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

[37] National Institute of Standards and Technology, *Minimum Security Requirements for Federal Information and Information Systems*, FIPS Pub 200, Gaithersburg, MD, March 2006, at https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf.

[38] Matt Barrett et al., *Approaches for Federal Agencies to Use the Cybersecurity Framework*, National Institute of Standards and Technology, NISTIR 8170, March 2020, at https://doi.org/10.6028/NIST.IR.8170.

[39] National Institute of Standards and Technology, *Framework for Improving*, April 16, 2018, at https://doi.org/10.6028/NIST.CSWP.04162018.

[40] Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," 82 *Federal Register* 22391-22397, May 16, 2017.

[41] National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, SP 800-37, December 2018, at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

[42] The terms *Information Security*, *Confidentiality, Availability,* and *Integrity* are defined in 44 U.S.C. §3552 as follows:
"The term "information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide-
(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
(C) availability, which means ensuring timely and reliable access to and use of information."

[43] National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, SP 800-53, September 2020, at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

Options for Congress

In addition to increasing oversight on VA's cybersecurity program, Congress may choose to alter how VA executes that program. In doing so, Congress may choose to assess and change resource levels, require the use of external cybersecurity service, or use adaptive cybersecurity services.

Assess Resource Levels

During the fiscal years 2021, 2020, and 2019, presidential budget requests OMB submitted to Congress included an Analytical Perspective on "Cybersecurity Funding." These documents describe the Administration's goals for cybersecurity with the President's Budget and how much agencies have spent (during the past year), plan on spending (during the current year), and plan to spend (during the next year) on cybersecurity. Much of the spending reported to OMB for cybersecurity spending is for the protection of federal IT systems and data.

Some agencies have cybersecurity-related spending that serves a cross-governmental or national cybersecurity mission. For instance, DHS reports on spending for government-wide cybersecurity capabilities (e.g., the National Cybersecurity Protection System) and the Department of Justice reports on cybercrime investigations. This spending is also reflected in OMB's reports.

The **Appendix** contains tables presenting federal agency base discretionary budget and their cybersecurity spending (as reported by OMB) for fiscal years 2017-2021. **Table 1**, drawn from the data in the Appendix, shows VA's base discretionary budget, the agency's cybersecurity spending and what that spending is as a percentage of the base discretionary budget.[44]

Table 1. Department of Veterans Affairs Cybersecurity Spending Relative to the Base Discretionary Budget

Fiscal Years 2017-2021, in millions

Fiscal Year	Base Discretionary Budget	Cybersecurity Spending	Cybersecurity Spending as a % of the Budget
2017 (Enacted)	$74,400	$386	0.52%
2018 (Estimate)	$77,300	$386	0.50%
2019 (Actual)	$86,600	$497	0.57%
2020 (Enacted)	$92,700	$525	0.57%
2021 (Request)	$105,000	$460	0.44%

Source: CRS Analysis of the Budget of the United States Government, as recorded by the U.S Government Publishing Office at https://www.govinfo.gov/app/collection/budget.

Notes: Because of delays in agencies receiving appropriations to start a fiscal year, and delays in reporting expenditures to OMB, each year's base discretionary budget could not use the same accounting of the budget. Instead, priority was given to an "Actual" budget report, then "Estimate," followed by "Enacted," and the "Request" for the most recent fiscal year. While the calculations for each of these budgets differs from year to year, their share of cybersecurity spending should not, and still provide a useful tool for comparison.

[44] Most of this data is reported to OMB in the respective years using accounting criteria prescribed by OMB. As such, it may be different than what the agency reports as part of it its annual congressional budget justification.

VA requested $113.1 billion in discretionary funding for FY2022.[45] Using past years' calculations, this may equate to an estimated cybersecurity expenditure of between $498 million and $645 million (using the FY2021 minimum of 0.44% and the FY2020 maximum of 0.57% of cybersecurity as a percent of the base discretionary budget).

Relative to other agencies, VA spends more money on cybersecurity than most others. (This is expected as VA has the second largest agency budget, behind the Department of Defense). As a percentage of the overall budget, VA spends less—even when discounting agencies with significant cybersecurity expenditures for national cybersecurity missions.

Congress may choose to direct VA to change its cybersecurity spending. In evaluating resource levels for cybersecurity, Congress may choose to set a baseline for spending (e.g., 0.75% or 1.0% of the base discretionary budget). Minimum spending levels may help to improve the agency's overall cybersecurity investment and provide opportunities to address historically under-resourced projects. However, general requirements for cybersecurity spending are not a guarantee that additional investments will be appropriately spent, or that the investments will result in significant improvements to the VA's cybersecurity posture.

Identification of areas of greatest risk is crucial to developing cybersecurity investment strategies. The Trump Administration required OMB to evaluate and report on federal cybersecurity risk.[46] Additionally, the VA IG[47] and GAO[48] have evaluated cybersecurity risks at VA. These documents can provide a framework for assessing current risk and provide potential options for increased investment.

Beyond required evaluations and periodic assessments, VA may require assistance in evaluating cybersecurity risk and developing strategies to mitigate those risks. Executive Order 14028 *Improving the Nation's Cybersecurity* directs certain agencies to provide the .gov domain with technical assistance, such as: developing security principles for cloud services use; providing standards for supply chain security; and mandating cyber incident reporting. [49] This assistance from agencies like CISA, NIST, and OMB can provide VA with justifications for future cybersecurity resource requests and requirements.

Require the VA Use Cybersecurity Shared Services

The Government Accountability Office (GAO) identified multiple key issues facing the VA as part of the GAO's 2021 High Risk List.[50] Three of these risk areas include:

- managing risks and improving VA health care;
- VA acquisition management; and

[45] Shalanda Young, "FY 2022 Discretionary Request," letter, April 9, 2021, at https://www.whitehouse.gov/wp-content/uploads/2021/04/FY2022-Discretionary-Request.pdf.

[46] Office of Management and Budget, *Federal Cybersecurity Risk Determination Report and Action Plan*, May 2018, at https://www.whitehouse.gov/wp-content/uploads/2018/05/Cybersecurity-Risk-Determination-Report-FINAL_May-2018-Release.pdf.

[47] Department of Veterans Affairs Office of Inspector General, *Federal Information Security Modernization Act Audit for Fiscal Year 2020*, Report #20-019727-104, Washington, DC, March 31, 2020, at https://www.va.gov/oig/pubs/VAOIG-20-01927-104.pdf.

[48] U.S. Government Accountability Office, *Veterans Affairs: VA Needs to Address Persistent IT Modernization and Cybersecurity Challenges*, GAO-20-719T, September 16, 2020, https://www.gao.gov/assets/gao-20-719t.pdf.

[49] Executive Office of the President, "Improving the Nation's Cybersecurity," 86 *Federal Register* 26633-26647, May 12, 2021.

[50] U.S. Government Accountability Office, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most Risk Areas*, GAO-21-119SP, March 2, 2021, https://www.gao.gov/products/gao-21-119sp.

- ensuring the cybersecurity of the nation.

Additionally, the VA IG highlighted challenges both with VA's cybersecurity program and its IT management.[51]

Concerning the risks federal agencies face in managing IT and the security risks to IT systems and information, Congress and the President have taken actions to alleviate managerial deficiencies at agencies by promoting shared services among agencies. By using shared services, organizations seek to achieve cost-savings, consolidate expertise necessary for the services, and improve efficiencies and performance for those services.

Congress passed the Modernizing Government Technology Act (MGT Act, P.L. 115-91, Title X, Subtitle G) which established a government-wide fund and authorized agency-specific modernization funds. Allocations from these funds are prioritized to IT modernization efforts to purchase cloud services and services shared among multiple agencies. OMB provided additional guidance to agencies seeking to use or establish these funds.[52] While agency-specific funds are authorized, few agencies have received appropriations for those funds.[53] The VA's budget request for fiscal year 2021 reports neither an existing agency-specific fund nor a request to initiate such a fund.[54] The American Rescue Plan Act of 2021 (P.L. 117-2) provided around $2 billion for federal IT and cybersecurity, of which $1 billion is available to the Technology Modernization Fund until the end of FY2025.

OMB directed agencies to consolidate certain capabilities with Memorandum 19-16 (M-19-16) *Centralized Mission Support Capabilities for the Federal Government*.[55] The memorandum establishes a process for designating agencies as Quality Services Management Offices (QSMO). The Cybersecurity and Infrastructure Security Agency (CISA) was selected as the QSMO for cybersecurity and is offering capabilities to federal agencies to supplement or supplant their current capabilities.[56] CISA also offers federal agencies additional tools to help secure their IT systems, such as (i) the National Cybersecurity Protection System (NCPS)[57] which scans internet traffic coming into and out of federal agencies, and (ii) the Continuous Diagnostics and Mitigation Program (CDM)[58] which scans agency networks to determine the hardware, software, users, and data on those networks and their vulnerabilities.

Congress may choose to direct the VA to pursue use of shared services. GAO and the IG have highlighted shortcomings in the VA's management of IT systems. While the responsibility to manage the IT risks to an agency ultimately lies with the agency head and their designees, an agency may lack the expertise to assess its IT risk, appropriate IT security solutions, or have funding necessary to address its IT risk. One

[51] Department of Veterans Affairs Office of Inspector General, *Federal Information Security Modernization Act Audit for Fiscal Year 2019*, Report #19-06935-96, Washington, DC, March 31, 2020, at https://www.va.gov/oig/pubs/VAOIG-19-06935-96.pdf.

[52] Office of Management and Budget, *Implementation of the Modernizing Government Technology Act*, M-18-12, Washington, DC, February 27, 2018, at https://www.whitehouse.gov/wp-content/uploads/2017/11/M-18-12.pdf.

[53] U.S. Congress, House Committee on Oversight and Reform, Subcommittee on Government Operations, *FITARA 10.0*, 116th Cong., 2nd sess., August 3, 2020.

[54] Department of Veterans Affairs, *FY 2021 Budget Submission: Medical Programs and Information Technology Programs*, Volume 2 of 4, February 2020, at https://www.va.gov/budget/docs/summary/fy2021VAbudgetVolumeIImedicalProgramsAndInformationTechnology.pdf.

[55] Office of Management and Budget, *Centralized Mission Support Capabilities for the Federal Government*, M-19-16, April 26, 2019, at https://www.whitehouse.gov/wp-content/uploads/2019/04/M-19-16.pdf.

[56] Cybersecurity and Infrastructure Security Agency, "Cybersecurity Quality Services Management Office," website, at https://www.cisa.gov/cyber-qsmo.

[57] Cybersecurity and Infrastructure Security Agency, "National Cybersecurity Protection System," website, at https://www.cisa.gov/national-cybersecurity-protection-system-ncps.

[58] Cybersecurity and Infrastructure Security Agency, "Continuous Diagnostics and Mitigation," website, at https://www.cisa.gov/cdm.

way to address this issue is to shift the provisioning of cybersecurity services from VA to another agency. CISA may provision technical capabilities for the VA such as Domain Name Services (DNS) resolution, security operations center services, and CDM. In this arrangement, CISA's expertise is used to acquire the capability while the VA retains responsibility for its security, so VA can continue to apply specialized expertise (e.g., risks to veterans' data) on the newly provided tools. If policymakers opt to pursue this option, agency concerns may include funding arrangements (i.e., from a working capital fund, from the CISA budget, from the VA budget, an MGT Act fund, or a combination) and the duration of an authorization to use shared services.

Mandate Next-Generation Cybersecurity Systems

Many traditional cybersecurity tools are built around protecting unauthorized access at the perimeter of an agency's network. Tools such as firewalls, intrusion detection and prevention systems (IDS and IPS), and identify, credential, access management systems (ICAM) are predominantly deployed between an agency's resources and external resources (e.g., between an agency's headquarters local-area-network, or LAN, and the public internet). However, cybersecurity experts have touted next-generation cybersecurity tools as necessary to adequately combat the increased sophistication of adversaries in cyberspace. Some next generation cybersecurity tools include endpoint detection and response (EDR) systems, highly adaptive cybersecurity services (HACS), and zero trust architecture. These next generation tools move away from applying security based on a prescribed set of rules or signatures and toward constantly assessing what normal and appropriate system behavior should be and rapidly identifying anomalous behavior and potential threats.

Traditional antivirus systems block potentially malicious code by matching indicators of that code (e.g., a hash value) against a library of known malware. While this system helps to stop some attacks, it is trivial for adversaries to alter the indicators of their malware at scale and deploy seemingly unique attacks upon their victims. EDR systems seek to address the limitation of signature-based security systems with heuristic-based security. EDR systems install a small program on all of an organization's endpoints (e.g., host machines such as laptops and connected devices such as Wi-Fi access points) and services (e.g., cloud servers) to identify normal behavior by authorized users of those endpoints and services. That data is combined with data from other endpoints to create an organization-wide view of the organization's network security. This combination of data requires high-performance computing and artificial intelligence systems to analyze data at wire-speed. As such, most of the processing of potential threats does not happen on the endpoint, but through a cloud service provider. If an EDR application detects anomalous and potentially malicious software or activities on an endpoint, it can automatically take actions to block it, report it, and look for it across other endpoints.

While agencies are free to pursue EDR capabilities through individual contracts, the federal government currently does not have a central EDR program. To address this, EO 14028 directs CISA to recommend options for EDR implementation by June 11, 2021 and to issue requirements to agencies on EDR use by August 10, 2021.

The General Services Administration (GSA) provides government-wide contract vehicles to federal agencies. One area of GSA's contract offerings is in highly adaptive cybersecurity services (HACS). HACS are proactive and reactive cybersecurity services, including risk and vulnerability assessments, security architecture reviews, continuous monitoring services, threat actor hunting, penetration testing, and incident response.[59] These services are designed to allow agencies greater visibility into their IT inventory, network operations, and cybersecurity posture by moving agencies from static assessments of

[59] General Services Administration, "Highly Adaptive Cybersecurity Services (HACS)," webpage, May 11, 2021, at https://www.gsa.gov/technology/technology-products-services/it-security/highly-adaptive-cybersecurity-services-hacs.

cybersecurity risk to dynamic and continual assessments allowing agencies to quickly identify risk and take steps to mitigate them.

Gaining attention among federal cybersecurity managers is the concept of *Zero Trust*.[60] Zero Trust Architectures move away from protecting the boundary of an IT network and toward limiting access within a network and continually assessing whether or not a presented user is authorized to access a particular resource or not. NIST defines Zero Trust as follows:

> Zero trust (ZT) provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. Zero trust architecture (ZTA) is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan.[61]

During testimony before the Homeland Security and Governmental Affairs Committee on May 11, 2021, Acting CISA Director Brandon Wales touted Zero Trust as the future of federal IT architecture, which will require significant investment but also create significant barriers to adversaries seeking to penetrate and exploit federal IT and data.[62] Executive Order 14028 creates policy around the move to Zero Trust by requiring agencies to develop a plan to implement Zero Trust Architecture by July 11, 2021.

Congress may choose to accelerate plans VA has for moving toward next generation cybersecurity services. In examining this option, Congress may choose to create statutory requirements for VA, reports to Congress on their adoption, or provide explicit resources to support their adoption. Congress may also target specific systems for next-generation cybersecurity services adoption, such as those related to the electronic health records or financial management systems.

Congress has required VA to implement cybersecurity requirements in addition to those broadly applicable to the federal government. For example, the data breach notification requirement in the Veterans Affairs Information Security Act is in addition to the data loss notification requirements in FISMA and the Privacy Act of 1974.

Conclusion

VA has unique attributes to its mission and IT enterprise which complicate its efforts for cybersecurity. There are established policies and programs in place to assist with implementing a successful cybersecurity program, and Congress has options to accelerate cybersecurity at VA.

Thank you for the opportunity to testify today, and I look forward to your questions.

[60] MeriTalk, "CIO Briefing Room: Zero Trust," webpage, May 14, 2021, at https://www.meritalk.com/news/cio-briefing-room/zerotrust/.

[61] National Institute of Standards and Technology, *Zero Trust Architecture*, NIST Special Publication 800-207, August 2020, at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

[62] U.S. Congress, Senate Committee on Homeland Security and Governmental Affairs, *Prevention, Response, and Recovery: Improving Federal Cybersecurity Post-SolarWinds*, 117th Cong., 1st sess., May 11, 2021, at https://www.hsgac.senate.gov/hearings/prevention-response-and-recovery-improving-federal-cybersecurity-post-solarwinds.

Appendix. Agency Cybersecurity Funding

For fiscal years (FY) 2019-2021, OMB included an Analytical Perspective on "Cybersecurity Funding," which includes agency reported expenditures and planned expenditures for cybersecurity. Using that data, combined with OMB's reporting of agency base discretionary funding, one can analyze agency budgets to see how much money an agency is spending on cybersecurity.

The base discretionary funding is not the total budget an agency may have to spend in a given fiscal year. Overseas Contingency Operations, emergency funding, and other ad-hoc additions could increase an agency's overall budget. Since not all agencies may receive additional funding, and since emergency funding is rarely for the purposes of cybersecurity, base discretionary funding is used for comparison to enable cross-agency analysis. Tables 2-6 present agency cybersecurity spending, respectively, for each fiscal year beginning with 2017 running through 2021.

Table 2. FY2017 Agency Cybersecurity Spending

Cybersecurity Spending Relative to Base Discretionary Funding, in millions

Agency	Base Discretionary (Enacted)	Cybersecurity Spending (Actual)	Cybersecurity Spending as a % of the Budget
Agriculture	$22,700	$115	0.50%
Commerce	$9,300	$274	2.94%
Defense	$523,200	$7,224	1.38%
Education	$66,900	$74	0.11%
Energy	$30,200	$371	1.23%
HHS	$87,100	$320	0.37%
Homeland Security	$42,400	$1,614	3.81%
HUD	$48,000	$15	0.03%
Interior	$13,500	$84	0.62%
Justice	$28,400	$735	2.59%
Labor	$12,000	$83	0.70%
State	$38,700	$254	0.66%
Transportation	$19,300	$185	0.96%
Treasury	$12,700	$458	3.61%
Veterans Affairs	$74,400	$386	0.52%
EPA	$8,200	$25	0.31%
NASA	$19,700	$148	0.75%
NSF	$7,500	$183	2.44%
SBA	$800	$20	2.44%

Source: Office of Management and Budget, *Efficient, Effective, Accountable: An American Budget*, Fiscal Year 2019, Washington, DC, February 12, 2018, p. 144, https://www.govinfo.gov/content/pkg/BUDGET-2019-BUD/pdf/BUDGET-2019-BUD.pdf. Office of Management and Budget, *Analytic Perspectives*, Fiscal Year 2019, Washington, DC, February 12, 2018, p. 274, https://www.govinfo.gov/content/pkg/BUDGET-2019-PER/pdf/BUDGET-2019-PER-7-8.pdf.

Notes: At the time that the FY2019 budget was being prepared, the FY2018 appropriations were incomplete and agencies were delayed in reporting the FY2017 outlays. The base discretionary column reflects the enacted appropriations and includes many post appropriation changes, such as transfers and rebasing.

Table 3. FY2018 Agency Cybersecurity Spending

Cybersecurity Spending Relative to Base Discretionary Funding, in millions

Agency	Base Discretionary (Estimate)	Cybersecurity Spending (Actual)	Cybersecurity Spending as a % of the Budget
Agriculture	$22,500	$262	1.16%
Commerce	$9,300	$350	3.76%
Defense	$574,500	$8,048	1.40%
Education	$67,800	$104	0.15%
Energy	$30,000	$448	1.49%
HHS	$86,300	$359	0.42%
Homeland Security	$44,100	$1,859	4.22%
HUD	$47,700	$15	0.03%
Interior	$13,400	$88	0.66%
Justice	$28,100	$821	2.92%
Labor	$12,000	$93	0.78%
State	$38,100	$362	0.95%
Transportation	$19,200	$185	0.96%
Treasury	$12,600	$445	3.53%
Veterans Affairs	$77,300	$386	0.50%
EPA	$8,000	$21	0.26%
NASA	$19,500	$171	0.88%
NSF	$7,400	$247	3.34%
SBA	$800	$9	1.13%

Source: Office of Management and Budget, *Efficient, Effective, Accountable: An American Budget*, Fiscal Year 2019, Washington, DC, February 12, 2018, p. 144, https://www.govinfo.gov/content/pkg/BUDGET-2019-BUD/pdf/BUDGET-2019-BUD.pdf. Office of Management and Budget, *Analytic Perspectives*, Fiscal Year 2020, Washington, DC, March 18, 2019, p. 306, https://www.govinfo.gov/content/pkg/BUDGET-2020-PER/pdf/BUDGET-2020-PER-5-8.pdf.

Notes: The FY2020 budget did not include an accounting of the FY2018 actuals. Instead, the estimated budget from FY2019 is used. At the time that the FY2019 budget was being prepared, the FY2018 appropriations were incomplete. The base discretionary column reflects appropriations from the continuing resolutions and estimates for the complete year.

Table 4. FY2019 Agency Cybersecurity Spending

Cybersecurity Spending Relative to Base Discretionary Funding, in millions

Agency	Base Discretionary (Actual)	Cybersecurity Spending (Actual)	Cybersecurity Spending as a % of the Budget
Agriculture	$24,400	$208	0.85%
Commerce	$11,600	$446	3.85%
Defense	$616,200	$8,527	1.38%
Education	$70,500	$119	0.17%
Energy	$30,200	$578	1.92%
HHS	$100,800	$522	0.52%
Homeland Security	$47,300	$2,591	5.48%
HUD	$53,800	$61	0.11%
Interior	$14,100	$104	0.74%
Justice	$30,800	$837	2.72%
Labor	$12,000	$87	0.72%
State	$48,200	$382	0.79%
Transportation	$26,500	$216	0.82%
Treasury	$15,000	$511	3.41%
Veterans Affairs	$86,600	$497	0.57%
EPA	$8,900	$42	0.47%
NASA	$21,500	$168	0.78%
NSF	$8,100	$246	3.04%
SBA	$700	$16	2.33%

Source: Office of Management and Budget, *A Budget for America's Future*, Fiscal Year 2021, Washington, DC, February 10, 2020, p. 123, https://www.govinfo.gov/content/pkg/BUDGET-2021-BUD/pdf/BUDGET-2021-BUD.pdf. Office of Management and Budget, *Analytic Perspectives*, Fiscal Year 2021, Washington, DC, February 10, 2020, p. 268, https://www.govinfo.gov/content/pkg/BUDGET-2021-PER/pdf/BUDGET-2021-PER-6-6.pdf.

Notes: The FY2021 budget included an accounting of FY2019 actual spending. These figures were used.

Table 5. FY2020 Agency Cybersecurity Spending

Cybersecurity Spending Relative to Base Discretionary Funding, in millions

Agency	Base Discretionary (Enacted)	Cybersecurity Spending	Cybersecurity Spending as a % of the Budget
Agriculture	$23,800	$231	0.97%
Commerce	$12,900	$514	3.99%
Defense	$633,300	$10,075	1.59%
Education	$72,200	$166	0.23%
Energy	$38,500	$550	1.43%
HHS	$105,800	$476	0.45%
Homeland Security	$48,100	$2,574	5.35%
HUD	$56,500	$68	0.12%
Interior	$14,700	$121	0.83%
Justice	$32,400	$901	2.78%
Labor	$12,400	$92	0.74%
State	$47,700	$406	0.85%
Transportation	$24,800	$262	1.06%
Treasury	$15,500	$588	3.80%
Veterans Affairs	$92,700	$525	0.57%
EPA	$9,100	$33	0.36%
NASA	$22,600	$167	0.74%
NSF	$8,300	$226	2.73%
SBA	$800	$16	1.96%

Source: Office of Management and Budget, *A Budget for America*'s *Future*, Fiscal Year 2021, Washington, DC, February 10, 2020, p. 123, https://www.govinfo.gov/content/pkg/BUDGET-2021-BUD/pdf/BUDGET-2021-BUD.pdf. Office of Management and Budget, *Analytic Perspectives*, Fiscal Year 2021, Washington, DC, February 10, 2020, p. 268, https://www.govinfo.gov/content/pkg/BUDGET-2021-PER/pdf/BUDGET-2021-PER-6-6.pdf.

Notes: At the time of publication, the complete FY2022 budget was not released. To continue the comparison, the FY2020 enacted budget was used as reported in the FY2021 budget.

Table 6. FY2021 Agency Cybersecurity Spending

Cybersecurity Spending Relative to Base Discretionary Funding, in millions

Agency	Base Discretionary (Requested)	Cybersecurity Spending	Cybersecurity Spending as a % of the Budget
Agriculture	$21,800	$230	1.06%
Commerce	$8,100	$378	4.67%
Defense	$636,400	$9,846	1.55%
Education	$66,600	$163	0.24%
Energy	$35,400	$666	1.88%
HHS	$96,400	$519	0.54%
Homeland Security	$49,700	$2,604	5.24%
HUD	$47,900	$69	0.14%
Interior	$12,700	$133	1.05%
Justice	$31,700	$929	2.93%
Labor	$11,000	$89	0.81%
State	$41,100	$489	1.19%
Transportation	$21,600	$249	1.15%
Treasury	$15,700	$689	4.39%
Veterans Affairs	$105,000	$460	0.44%
EPA	$6,700	$47	0.70%
NASA	$25,200	$164	0.65%
NSF	$7,700	$212	2.75%
SBA	$700	$16	2.30%

Source: Office of Management and Budget, *A Budget for America*'s *Future*, Fiscal Year 2021, Washington, DC, February 10, 2020, p. 123, https://www.govinfo.gov/content/pkg/BUDGET-2021-BUD/pdf/BUDGET-2021-BUD.pdf. Office of Management and Budget, *Analytic Perspectives*, Fiscal Year 2021, Washington, DC, February 10, 2020, p. 268, https://www.govinfo.gov/content/pkg/BUDGET-2021-PER/pdf/BUDGET-2021-PER-6-6.pdf.

Notes: At the time of publication, the complete FY2022 budget was not released. To continue the comparison, the FY2021 requested budget was used as reported in the FY2021 budget.

Table A-1 includes an overview of the percent of each agency's base discretionary budget that the agency spends on cybersecurity funding, as reported to OMB. The reported cybersecurity spending does not separate between internal spending to protect agency IT resources and external spending to ensure national cybersecurity. Certain agencies (e.g., Commerce, Defense, Homeland Security, and Justice) have major programs for ensuring national cybersecurity, and can report substantial portions of their budgets for cybersecurity spending. The Department of Homeland Security has the highest percentages year-over-year because the department is simultaneously spending to protect its own networks, protect other agency networks and the .gov domain, and ensure national cybersecurity.

Table A-1. Percent of Agency Cybersecurity Spending as a Portion of Base Discretionary Funding

FY2017-2021

Agency	FY17	FY18	FY19	FY20	FY21
Agriculture	0.50%	1.16%	0.85%	0.97%	1.06%
Commerce	2.94%	3.76%	3.85%	3.99%	4.67%
Defense	1.38%	1.40%	1.38%	1.59%	1.55%
Education	0.11%	0.15%	0.17%	0.23%	0.24%
Energy	1.23%	1.49%	1.92%	1.43%	1.88%
HHS	0.37%	0.42%	0.52%	0.45%	0.54%
Homeland Security	3.81%	4.22%	5.48%	5.35%	5.24%
HUD	0.03%	0.03%	0.11%	0.12%	0.14%
Interior	0.62%	0.66%	0.74%	0.83%	1.05%
Justice	2.59%	2.92%	2.72%	2.78%	2.93%
Labor	0.70%	0.78%	0.72%	0.74%	0.81%
State	0.66%	0.95%	0.79%	0.85%	1.19%
Transportation	0.96%	0.96%	0.82%	1.06%	1.15%
Treasury	3.61%	3.53%	3.41%	3.80%	4.39%
Veterans Affairs	0.52%	0.50%	0.57%	0.57%	0.44%
EPA	0.31%	0.26%	0.47%	0.36%	0.70%
NASA	0.75%	0.88%	0.78%	0.74%	0.65%
NSF	2.44%	3.34%	3.04%	2.73%	2.75%
SBA	2.44%	1.13%	2.33%	1.96%	2.30%
SSA	1.68%	1.80%	2.24%	2.26%	1.02%
Average	1.38%	1.52%	1.65%	1.64%	1.73%

Source: CRS analysis of agency budgets.