19. CYBERSECURITY FUNDING

Cybersecurity is an important component of the Administration's IT modernization efforts, and the President remains dedicated to securing the Federal enterprise from cyber-related threats. Assessments of the Federal Government's overall cybersecurity risk continue to find the Federal enterprise to be threatened. Cybersecurity budgetary priorities will continue to seek to reduce this risk, based on data-driven, risk-based assessments of the threat environment and the current Federal cybersecurity posture. The President's Budget includes approximately $18.8 billion for cybersecurity funding, which supports the protection of Federal information systems and our Nation's most valuable information including the personal information of the American public. The 2021 Budget funds activities in support of Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,"[1] the outcomes of the Report to the President on Federal IT Modernization, the Modernize IT to Increase Productivity and Security (IT Modernization) Cross Agency Priority (CAP) Goal of the President's Management Agenda (PMA),[2] and the National Cybersecurity Strategy.[3]

National Cybersecurity Strategy

In September 2018, the White House released the National Cyber Strategy, which reinforces ongoing work and provides strategic direction for the Federal Government to take action on short and long-term improvements to cybersecurity for the Government and critical infrastructure. The National Cyber Strategy recognizes that private and public entities have struggled to secure their systems as adversaries have increased the frequency and sophistication of their malicious cyber activities, and directs the Federal Government to do its part to ensure a secure cyber environment for our Nation.

Supply Chain Risk Management

In 2019, as part of the National Cyber Strategy and with the passage of the SECURE Technology Act, agencies are required to assess the risks to their respective information and communications technology supply chains. In addition to agency Supply Chain Risk Management (SCRM) programs, enterprise wide risk is being addressed through the Federal Acquisition Security Council (FASC). The FASC will make recommendations on potential exclusion and removal orders to the Secretaries of Defense and Homeland Security as well as the Director of National Intelligence to address risk to each of their enterprises. These critical steps help agencies safeguard information and communication technology from emerging threats and support the need to establish standards for the acquisition community around SCRM.

Trusted Internet Connections

On September 12, 2019, OMB updated the Trusted Internet Connection (TIC) initiative after more than a decade. The updated policy allows industry to propose, and agencies to adopt, new solutions to take advantage of modern internet capabilities.

Leading up to the release of the new policy, the Small Business Administration (SBA) and the Department of Energy (DOE) worked with OMB and the Department of Homeland Security (DHS) to pilot selected solutions. The success of these pilots shows that solutions using current technologies can continue progress on goals outlined a decade ago. The technologies used DOE's pilot increased the flexibility and reach of the agency users so they are no longer required to be tethered to DOE's Federal computing network. DOE's mobile device users were able to directly access their cloud based systems, saving tax payer funds necessary to support some of DOE's Government operations. SBA's pilot helped transform the Agency's technology platform and improve the ability to scale up. SBA leveraged the technologies used in their TIC pilot in 2018 to help the Agency to rapidly scale up to support victims of natural disasters.

Continuous Diagnostic and Mitigation

Prior to the establishment of the Continuous Diagnostics and Mitigation (CDM) program at the Department of Homeland Security (DHS), Federal Agencies inconsistently implemented Information Security Continuous Monitoring (ISCM) policies. The CDM Program provides a dynamic approach for baselining ISCM efforts: DHS's CDM program provides Federal Agencies with the tools, integration services, and dashboards necessary for identifying cybersecurity risks on a continuous basis. This near real-time monitoring enhances agencies' ability to prioritize cybersecurity risks, enabling cybersecurity personnel to mitigate the most significant problems first. The CDM program also provides DHS with a Federal enterprise view of the cyber threat landscape through the Federal CDM Dashboard that receives summary data from all Federal Agency Dashboards. The CDM objectives are to reduce agency-specific security threats; increase visibility into the Federal enterprise cybersecurity posture;

[1] *https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/*.

[2] See *https://www.perfomance.gov/*.

[3] *https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf*.

improve Federal cybersecurity response capabilities; and streamline Federal Information Security Modernization Act of 2014 (FISMA) reporting.

To further support the CDM program, the Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements (M-20-04) requires Federal Agencies to provide sufficient justification prior to purchasing and using tools purchased outside of the CDM acquisition vehicles. Additionally, M-20-04 requires that Federal Agencies fund long-term operations and maintenance (e.g., licensing costs) of their CDM-related tools and capabilities as CDM-specific line items in their annual congressional budget justification documents.

Federal Information Security Modernization Act

FISMA designates OMB as responsible for overseeing Federal Agencies' information security and privacy practices and for developing and directing implementation of policies and guidelines that support and sustain those practices. The President's Budget provides funding for agencies to implement cybersecurity defenses that are necessary to protect the data of the American people and sensitive national security information.

These cybersecurity defenses include key capabilities identified as targets for progress in the President's Management Agenda. For example, as of October 2019 all 23 of the civilian CFO Act agencies reported the ability to remotely wipe agency-owned mobile devices of agency data in the event that they are lost or stolen. Additional details on these Government-wide targets can be found on *performance.gov*. Furthermore, OMB leverages a quarterly Risk Management Assessment (RMA) process to help agencies understand and decrease their cybersecurity risk by focusing on high priority controls, tracking improvements over time. A complete set of agency cybersecurity performance summaries, which provide a high-level overview of RMA and Inspector General ratings, will be available in the forthcoming annual FISMA report.

Data Collection Methodology and Adjustments

Section 630 of the Consolidated Appropriations Act, 2017 (P.L. 115–31) amended 31 U.S.C. § 1105 (a)(35) to require that an analysis of Federal cybersecurity funding be incorporated into the President's Budget. The Federal spending estimates in this analysis utilize funding and programmatic information collected on the Executive Branch's cybersecurity efforts, including cybersecurity activities and funding for all Federal Agencies, not just those carried out by DHS and DOD.

Agencies provide funding data at a level of detail sufficient to consolidate information to determine total governmental spending on cybersecurity. OMB provided the following guidance to agencies regarding the reporting of cybersecurity budget information for each fiscal year (FY): FY 2019 Actual levels should reflect the actual budgetary resources available for that year, FY 2020 Estimate levels should reflect the estimated budgetary resources available that year, and FY 2021 levels should reflect the President's Budget. Agencies were directed to coordinate responses between their Chief Financial Officers, Chief Information Officers, and Chief Information Security Officers.

Cybersecurity Workforce

FISMA requires every Federal Agency to protect its information and information systems against an ever-changing array of cybersecurity threats. The Federal cybersecurity workforce is responsible for staying abreast of the latest threat intelligence, developing new and innovative ways to protect Federal information resources, and administering the tools that identify and protect against cyber attacks. However, the Federal Government is not alone in needing to protect and defend against these threats, and the demand for cyber professionals throughout the American economy exceeds the supply. This makes it critical for the Government to continue investing in new ways to recruit and retain cybersecurity talent. These challenges are addressed in both the Administration's "Delivering Government Solutions in the 21st Century" paper on "Solving the Federal Cybersecurity Workforce Shortage," as well as as well as Executive Order 13800 on America's Cybersecurity Workforce.

Over the last year, the Administration has seen success in programs like the Federal Cybersecurity Reskilling Academy, which showed that agencies can reskill existing employees to fill critically needed skills gaps. The Administration also piloted a new hiring process that will allow agencies to better evaluate the capabilities of applicants to highly technical positions, such as in the cybersecurity field, accelerating the hiring process and improving agencies' ability to find and hire the best candidates. These types of programs are the innovative work that the Federal Government needs to remain a competitive employer for our highest-need skillsets.

The President's Budget continues to build on these successes, investing in additional reskilling, as well as professional development for the existing cybersecurity workforce. Through centralized programs at the Cybersecurity and Infrastructure Security Agency designed to benefit all agencies, as well as making targeted investments in individual agencies' workforce budgets, the Administration is committed to an enterprise-wide effort to build a workforce to protect and defend the Government's information assets. There are multiple programs across agencies which address recruitment, retention, reskilling, and overall advancement of cyber skills in the American workforce. The 2021 Budget also supports efforts to develop technical skills within the national workforce through educational programs, science and technology research, and grants to STEM fields.

Federal Budget Authority

The President's Budget includes $18.8 billion of budget authority for cybersecurity-related activities, consistent with the 2020 estimate. Due to the sensitive nature of some activities, this amount does not represent the entire cyber budget.

Agencies estimated cybersecurity budget authority for 2021 reflects planned investments to protect information and information systems commensurate with the risk and magnitude of potential harm. However, a number of agencies also have cybersecurity-related spending that is not dedicated to the protection of their own networks, serving instead a broader cybersecurity mission. For instance, there are a number of programs that provide tools and capabilities Government-wide, such as DHS's Continuous Diagnostics and Mitigation (CDM) program. Additionally, numerous programs exist that further enhance national and Federal cybersecurity focused on areas such as standards, research, and the investigation of cyber-crimes rather than specific technical capabilities.

Table 19-1 provides an overview of civilian CFO Act Agency cybersecurity spending as aligned to the NIST Cybersecurity Framework functions, Identify, Protect, Detect, Respond, and Recover. Table 19-2 provides an agency level view of cybersecurity spending.

Table 19–1. NIST FRAMEWORK FUNCTION CIVILIAN CFO ACT AGENCY FUNDING TOTALS
(In millions of dollars)

NIST Framework Function	FY 2021
Identify	2,461
Protect	2,740
Detect	918
Respond	2,189
Recover	206
Total	**8,514**

Note: This analysis excludes Department of Defense spending.

Non-Federal Cybersecurity Spending

While it is difficult to estimate how much the U.S. private sector spends on cybersecurity, the research firm Gartner releases routine estimates of cybersecurity spending globally and forecasts that cybersecurity spending is anticipated to reach $170.4 billion in 2022.[4] The International Data Corporation predicts that information security spending would increase worldwide by 10.7 percent in 2019 to $106.6 billion, forecasting that it could reach an estimated $151.2 billion in 2023. [5]

Additional Information

The President's Budget is also required to include an analysis of fee-based cybersecurity costs as well as gross and net appropriations or obligational authority and outlays. Agencies have not historically reported their cybersecurity budgets in this manner, and OMB continues to work with the broader Federal community to capture this information in a way that is helpful to both agencies and the Congress.

[4] Source: Gartner, "Forecast Analysis: Information Security, Worldwide, 2Q18 Update," September 14, 2018, at *https://www.gartner.com/en/documents/3889055*.

[5] Source: International Data Corporation, "New IDC Spending Guide Sees Solid Growth Ahead for Security Products and Services," October 16, 2019, at *https://www.idc.com/getdoc.jsp?containerId=prUS45591619*.

Table 19–2. CYBERSECURITY FUNDING BY AGENCY

(In millions of dollars)

Organization	FY 2019	FY 2020	FY 2021
CFO Act Agencies	**$16,552.7**	**$18,398.1**	**$18,360.4**
Department of Agriculture	$208.2	$231.2	$230.1
Department of Commerce	$446.4	$514.3	$378.1
Department of Defense	$8,527.0	$10,075.0	$9,846.0
Department of Education	$119.0	$166.2	$162.6
Department of Energy	$578.4	$550.4	$665.6
Department of Health and Human Services	$512.5	$475.7	$519.4
Department of Homeland Security	$2,590.8	$2,574.1	$2,604.3
Department of Housing and Urban Development	$60.8	$68.2	$69.0
Department of Justice	$837.2	$900.5	$929.2
Department of Labor	$86.6	$92.2	$89.1
Department of State	$381.5	$405.8	$488.6
Department of the Interior	$103.8	$121.4	$133.3
Department of the Treasury	$510.8	$588.4	$688.8
Department of Transportation	$216.4	$262.1	$249.2
Department of Veterans Affairs	$491.7	$524.6	$460.4
Environmental Protection Agency	$42.1	$32.5	$46.8
General Services Administration	$72.6	$82.4	$79.2
National Aeronautics and Space Administration	$167.6	$166.6	$163.8
National Science Foundation	$246.4	$226.3	$212.0
Nuclear Regulatory Commission	$28.8	$27.5	$26.9
Office of Personnel Management	$40.9	$47.1	$53.8
Small Business Administration	$16.3	$15.7	$16.1
Social Security Administration	$204.0	$207.6	$205.0
U.S. Agency for International Development	$62.6	$42.5	$43.3
Non-CFO Act Agencies	**$384.3**	**$393.6**	**$418.4**
Access Board	$0.8	$0.6	$0.6
American Battle Monuments Commission	$0.4	$0.8	$1.3
Armed Forces Retirement Home	$0.3	$0.3	$0.3
Chemical Safety and Hazard Investigation Board	$0.8	$0.8	$2.7
Commission on Civil Rights	$0.4	$0.4	$0.5
Commodity Futures Trading Commission	$7.6	$10.8	$11.0
Consumer Product Safety Commission	$3.0	$2.9	$4.3
Corporation for National and Community Service	$3.0	$3.2	$3.2
Council of the Inspectors General on Integrity and Efficiency	$0.6	$0.6	$0.6
Court Services and Offender Supervision Agency for the District	$3.4	$3.5	$3.5
Defense Nuclear Facilities Safety Board	$1.8	$2.3	$2.3
Equal Employment Opportunity Commission	$4.0	$3.9	$2.5
Export-Import Bank of the United States	$3.4	$3.1	$3.2
Farm Credit Administration	$3.0	$3.3	$3.5
Federal Communications Commission	$15.3	$12.0	$13.9
Federal Deposit Insurance Corporation	$109.8	$109.8	$109.8
Federal Election Commission	$1.0	$1.0	$1.0
Federal Financial Institutions Examination Council	$0.1	$0.1	$0.1
Federal Labor Relations Authority	*	*	*
Federal Maritime Commission	$0.1	$0.1	$0.2
Federal Retirement Thrift Investment Board	$66.2	$66.1	$77.4
Federal Trade Commission	$11.4	$12.3	$12.6
Gulf Coast Ecosystem Restoration Council	$0.2	$0.2	$0.2
Institute of Museum and Library Services	$0.3	$0.3	$0.3
International Assistance Programs	$16.7	$17.6	$17.6
African Development Foundation	$1.0	$1.0	$1.0
Inter-American Foundation	$0.4	$0.4	$0.4
Millennium Challenge Corporation	$1.6	$1.7	$1.5
Overseas Private Investment Corporation	$1.7	$2.0	$2.3
Peace Corps	$10.9	$11.2	$11.2

Table 19–2. CYBERSECURITY FUNDING BY AGENCY—Continued

(In millions of dollars)

Organization	FY 2019	FY 2020	FY 2021
Trade and Development Agency	$1.1	$1.3	$1.3
International Trade Commission	$3.0	$4.2	$5.4
Marine Mammal Commission	$0.1	$0.1	$0.1
Merit Systems Protection Board	$0.2	$1.0	$1.0
Morris K. Udall and Stewart L. Udall Foundation	*	*	*
National Archives and Records Administration	$9.7	$7.7	$7.8
National Credit Union Administration	$6.7	$7.4	$7.3
National Endowment for the Arts	$2.2	$1.6	$1.4
National Endowment for the Humanities	$1.1	$1.1	$1.1
National Gallery of Art	$2.0	$2.0	$2.0
National Labor Relations Board	$2.1	$2.2	$2.3
National Transportation Safety Board	$1.0	$1.5	$1.5
Nuclear Waste Technical Review Board	$0.3	$0.3	$0.3
Occupational Safety and Health Review Commission	$1.3	$1.3	$1.3
Office of Government Ethics	$0.3	$0.4	$0.4
Office of Special Counsel	$0.3	$0.3	$0.4
Postal Regulatory Commission	$0.2	$0.6	$0.7
Presidio Trust	$0.7	$0.7	$0.7
Privacy and Civil Liberties Oversight Board	$1.4	$1.4	$1.4
Securities and Exchange Commission	$38.3	$41.8	$46.6
Selective Service System	$4.1	$2.5	$2.0
Smithsonian Institution	$7.8	$8.7	$10.3
Surface Transportation Board	$1.8	$0.9	$0.9
Tennessee Valley Authority	$21.0	$21.6	$21.6
U.S. Agency for Global Media	$8.1	$7.9	$7.3
U.S. Army Corps of Engineers	$15.2	$18.8	$20.3
United States Holocaust Memorial Museum	$1.4	$1.6	$1.7
United States Institute of Peace	$0.3	$0.3	$0.3
Total	**$16,936.9**	**$18,791.6**	**$18,778.8**

* $50 thousand or less