16. INFORMATION TECHNOLOGY AND CYBERSECURITY FUNDING

Federal Information Technology (IT) provides Americans with important services and information, and is the foundation of how Government serves the public in the digital age. The Budget proposes spending $65 billion on IT at civilian agencies in fiscal year (FY) 2023,[1] which will be used to deliver critical public services, keep sensitive data and systems secure, and further the Administration's vision of an effective and efficient Government. The President's Budget also supports the implementation of Federal laws that enable agency technology planning, oversight, funding, and accountability practices, as well as Office of Management and Budget (OMB) guidance to agencies on the strategic use of IT to enable mission outcomes. It supports IT system modernization; migration to secure, cost-effective commercial cloud solutions and shared services; the recruitment, retention, and reskilling of the Federal technology and cybersecurity workforce to ensure higher value service delivery; and the reduction of cybersecurity risk across the Federal enterprise.

Cyber threats have become a top risk to delivering critical Government services, and this Administration is committed to addressing root cause issues and taking transformational steps to modernize Federal cybersecurity defenses. The President's Budget includes approximately $10.9 billion for civilian cybersecurity funding, which supports the protection of Federal IT and the Nation's most valuable information, including the personal information of the American public. These investments will, in alignment with the Administration's priorities, focus on addressing root cause structural issues, promoting stronger collaboration and coordination among Federal agencies, and addressing capability challenges that have impeded the Government's technology vision.

Federal Spending on IT and Cybersecurity

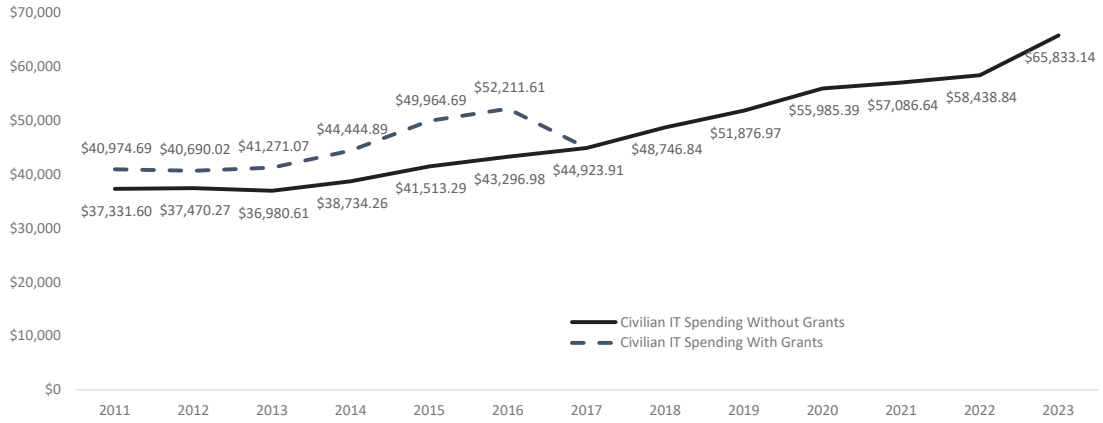
As shown in Table 16-1, the President's Budget for IT at civilian Federal agencies is estimated to be $65 billion in 2023. This figure is an 11 percent increase from the estimate reported for 2022. Chart 16-1 shows trending information for Federal civilian IT spending from 2021 forward.[2] The President's Budget includes funding for 4,290 investments at 24 agencies. These investments support the three IT Portfolio areas shown in Chart 16-2. Of those 4,290 IT investments, 742 are considered major IT investments. As outlined in OMB Circular A-11 and FY 2022 Capital Planning and Investment Control (CPIC) Guidance, agencies determine if an IT investment is classified as major based on whether the associated investment: has significant program or policy implications; has high executive visibility; has high development, operating, or maintenance costs; or requires special management attention because of its importance to the mission or function of the agency. For all major IT investments, agencies are required to submit Business Cases, which provide additional transparency regarding the cost, schedule, risk, and performance data related to its spending. OMB requires that agency Chief Information Officers (CIOs) provide risk ratings for all major IT investments on the IT Dashboard website on a continuous basis and assess how risks for major development efforts are being addressed and mitigated.

Cybersecurity remains a top priority for this Administration, as our adversaries continue to seek new and creative means to compromise Federal systems. The Administration has engaged top experts from across the Nation to identify leading security practices and set a bold new course to overhaul the Government's approach to securing Federal IT. The President's Budget includes approximately $10.9 billion of budget authority for civilian cybersecurity-related activities. This figure is an 11 percent increase reported for 2022. Cybersecurity budgetary priorities continue to seek to reduce the risk and impact of cyber incidents based on data-driven, risk-based assessments of the threat environment and the current Federal cybersecurity posture. 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 activities that protect agency information systems, and also on activities that broadly involve cybersecurity such as the development of standards, research and development, and the investigation of cybercrimes. Agencies provide funding data at a level of detail sufficient to consolidate information to determine total governmental spending on cybersecurity. Within each agency, FY 2021 actual levels reflect the actual budgetary resources available in the prior year, FY 2022 estimates reflect the estimated budgetary resources available in the current year, and FY 2023 levels are to reflect levels consistent with the President's Budget. Table 16-2 provides an agency-level view of cybersecurity spending. Table 16-3 provides an overview of cybersecurity spending among agencies included in the Chief Financial Officers Act of 1990 (P.L. 101-576) (CFO Act agencies), as aligned to the National Institute of Standards and Technology (NIST)

[1] The scope of the analysis in this chapter refers to agencies represented on the IT Dashboard, located at *https://www.itdashboard.gov/*. This analysis excludes the Department of Defense.

[2] Note that as of the 2020 CPIC guidance, IT related grants made to State and local governments are no longer included in agency IT investment submissions.

CHART 16-1. TRENDS IN FEDERAL CIVILIAN IT SPENDING



Cybersecurity Framework functions: Identify, Protect, Detect, Respond, and Recover.

The remainder of this chapter describes important aspects of the latest initiatives undertaken with respect to Federal IT policies and projects, as well as cybersecurity policy and spending.

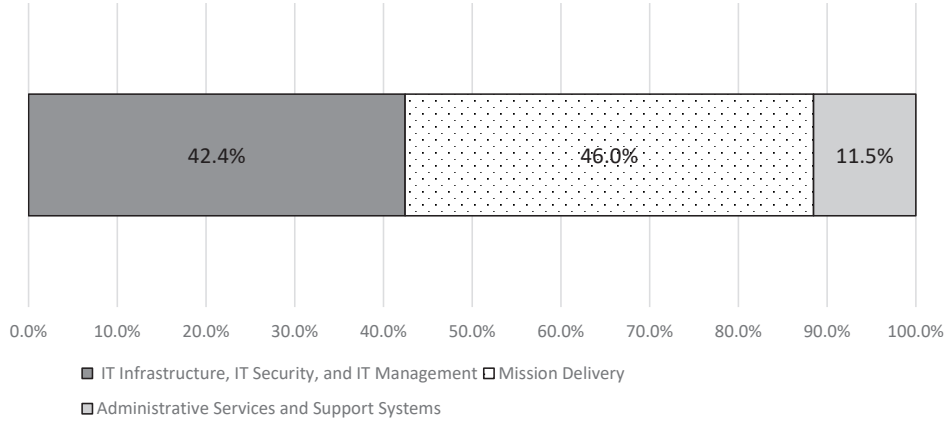
Cybersecurity

The President's Budget supports the Administration's commitment to transforming Federal cybersecurity by addressing root cause issues and pursuing leading security practices designed to defeat the methods of even sophisticated threat actors. In pursuit of these goals, the President signed Executive Order 14028, "Improving the Nation's Cybersecurity" in May 2021. The Executive Order places a strong emphasis on improving information-sharing between the U.S. Government and private sector, enhancing the security of Government-procured software, improving detection of cyber threats and vulnerabilities on Federal systems, and strengthening the United States' ability to respond to incidents when they occur.

A key goal of Executive Order 14028 is to modernize the Federal Government's approach to securing systems and data by adopting zero trust cybersecurity principles. To meet that goal, the Administration released guidance for agencies through OMB Memorandum M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, in January 2022. This Memorandum established a multi-year zero trust strategy and action plan that requires agencies to meet specific cybersecurity standards and objectives by the end of FY 2024, in order to bolster the Government's defenses against increasingly sophisticated and persistent threat campaigns.

In addition to OMB Memorandum M-22-09, OMB had previously taken a series of other actions to increase the resiliency of the Federal Government's digital infrastructure, including the issuance guidance for agencies through OMB Memorandum M-21-30, Protecting Critical Software Through Enhanced Security Measures. This guidance requires agencies to inventory critical software and implement robust security requirements to ensure the security of the software supply chain and protect the use of software in agencies' operational environments. Following that, OMB released further guidance to agen-

CHART 16-2. FY 2022 FEDERAL CIVILIAN IT INVESTMENT PORTFOLIO SUMMARY



cies through OMB Memorandum M-21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents, requiring agencies to implement security logging measures that ensure greater visibility into potential threats, accelerating incident response efforts and enabling more effective defense of Federal information and Executive Branch departments and agencies. Further guidance to agencies followed in OMB Memorandum M-22-01, Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response, which requires agencies to implement real-time continuous monitoring and response capabilities on all endpoints (e.g., phones, desktops, printers, laptops, etc.). The President's Budget shows the Administration's commitment to ensuring these requirements are implemented across the Federal Government, dedicating $10.9 billion to support and upgrade Federal civilian cybersecurity capabilities.

Finally, in the wake of the much-publicized cyber threats to Federal and civilian systems in recent years, in January 2021, the Congress established the Office of the National Cyber Director (ONCD) through the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116-283). Funded by the Infrastructure Investment and Jobs Act, ONCD serves as the principal advisor to the President on cybersecurity policy and strategy. The National Cyber Director is statutorily charged with working to ensure a cohesive and unified cyber posture across the entire Federal enterprise, and coordinating with OMB to ensure agency budgets align with the Administration's vision and priorities. The efforts around the President's Budget supports ONCD's efforts to improve national coordination in the face of escalating cyber-attacks on Government and critical infrastructure.

Supply Chain Risk Management

The Budget includes resources for agencies to invest in building agency capacity to evaluate and mitigate supply chain risk. With the passage of the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE Technology Act) in 2018, 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 evaluated through the Federal Acquisition Security Council (FASC). The FASC will make recommendations on potential exclusion and removal orders to the Secretaries of the Departments 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 communi-

Table 16–1. ESTIMATED FY 2023 CIVILIAN FEDERAL IT SPENDING AND PERCENTAGE BY AGENCY

(In millions of dollars)

Agency	FY 2023	Percent of Total
Department of Homeland Security	$10,296	15.6%
Department of Veterans Affairs	$8,606	13.1%
Department of Health and Human Services	$7,824	11.9%
Department of the Treasury	$5,615	8.5%
Department of Justice	$4,102	6.2%
Department of Transportation	$4,078	6.2%
Department of Energy	$3,545	5.4%
Department of Agriculture	$3,912	5.9%
Department of State	$3,195	4.9%
Department of Commerce	$2,665	4.0%
Social Security Administration	$2,375	3.6%
National Aeronautics and Space Administration	$2,174	3.3%
Department of the Interior	$1,721	2.6%
Department of Education	$1,138	1.7%
General Services Administration	$977	1.5%
Department of Labor	$867	1.3%
Department of Housing and Urban Development	$558	0.8%
Office of Personnel Management	$423	0.6%
Environmental Protection Agency	$413	0.6%
U.S. Agency for International Development	$327	0.5%
U.S. Army Corps of Engineers	$309	0.5%
Small Business Administration	$295	0.4%
National Science Foundation	$164	0.2%
Nuclear Regulatory Commission	$142	0.2%
National Archives and Records Administration	$111	0.2%
Total	**$65,833**	**100.0%**

This analysis excludes the Department of Defense

cation technology from emerging threats and support the need to establish standards for the acquisition community around SCRM. In August 2021, the FASC promulgated a rule[3] that modernizes the Council, as well as enhances information sharing and evaluation of supply chain risk.

IT Modernization

Agencies prioritize the modernization of Federal IT systems to better deliver their mission and services to the American public in an effective, efficient, and secure manner. Agencies are continuing to deploy standards-based platforms and systems, leveraging commercial capabilities that replace highly-customized Government technology. The Federal Government is focused on enhancing Federal IT and digital services, reducing cybersecurity risks to the Federal mission, and building a modern IT and cybersecurity workforce. Federal agencies' ongoing efforts to modernize their IT will enhance mission effectiveness and reduce mission risks through a series of complementary initiatives that will drive sustained change in Federal technology, deployment, security, and service delivery.

Notable IT Modernization efforts include the Technology Modernization Fund, Enterprise Infrastructure Solutions (EIS), and improving the IT and cyber workforce, among other efforts.

Technology Modernization Fund

The President's Budget includes $300 million for the Technology Modernization Fund (TMF), building on the fund's initial seed funding and the $1 billion provided in the American Rescue Plan Act of 2021 (Public Law 117-2, "ARP"). With the continuously evolving IT and cyber landscape, these investments are an important down payment on delivering modern and secure services to the American public, and continued investment in IT will be necessary to ensure the United States meets the accelerated pace of modernization. The funding provided to the TMF through the ARP recognized the critical need to address urgent IT modernization challenges, bolster cybersecurity defenses following the SolarWinds incident, and improve the delivery of COVID-19 relief. To implement the ARP funding, the TMF model was updated to accelerate agency modernization efforts to better serve the American public. The updated model includes repayment flexibilities to ensure a diverse set of project proposals, a streamlined review process to accommodate the increased volume of applications, and an evolved TMF Board to sustain the strategic evaluation of and investment in proposals. Since the release of the ARP guidance, the TMF Board has received over 120 proposals requesting more than $2.5 billion from over 40 agencies, and proposals continue to be submitted on a rolling basis. The Administration is maximizing the flexibility of the TMF to modernize high-priority systems, elevate the foundational security of Federal agencies, accelerate the growth of public-facing digital services, and scale cross-Government collaboration and shared services.

Since its start in March 2019, the TMF Board has invested 20 initiatives across 12 Federal agencies, totaling approximately $400 million.[4] Of this amount, over $320 million[5] was invested by the TMF Board, through the $1 billion provided in the ARP. This tranche of ARP-funded investments, and the seventh round of TMF investments since the fund was established, represents a set of strategic investments to improve technology at scale across all of the high priority areas. These investments reflect the Administration's strong commitment to improving the American public's interactions with Government and bolstering the security of those interactions. These investments will transform authentication for the Federal Government, and provide for multi-factor authentication across the board. They will also fund the development of an identity proofing solution that prevents fraud, ensures equitable access to government services, and protects individual privacy. This tranche is directly responsive to Executive Order 14028, protecting the data and privacy of 100 million students and borrowers, two million civilian Federal employees, millions of users of Government-wide shared services, and the security of hundreds of facilities. These investments are also directly responsive to the COVID-19 pandemic that has fundamentally changed how the Federal Government operates and interacts with the public.

The TMF is an innovative funding vehicle that gives agencies additional ways to deliver services to the American public more quickly, to better secure sensitive systems and data, and to use taxpayer dollars more efficiently.[6] The mission of the TMF is to enable agencies to accelerate transformation of the way they use technology to deliver their mission and services to the American public in an effective, efficient, and secure manner. Agencies must apply and compete for TMF funds. Investments are funded incrementally and tied to delivery of milestones, which enables more agile and dynamic IT modernization project implementation and ensures taxpayers dollars are used effectively and efficiently. To ensure successful project execution and improve program outcomes, the TMF Board and the TMF Program Management Office support project teams throughout the life of the investment. Once a project has been funded, the TMF Board meets with the agency project team on a quarterly basis to confirm projects are on schedule and milestones are being met. Technical experts from General Services Administration (GSA), as well as other entities such as the U.S. Digital Service, are also available to provide hands-on support to project teams in design, acquisition, and cybersecurity to improve team capability, troubleshoot issues, and guarantee successful execution.

Enterprise Infrastructure Solutions

The broader IT modernization effort within the Federal Government and transition to cloud services is underpinned by the modernization of Government communications networks. OMB designated the GSA Enterprise Infrastructure Solutions (EIS) contract as "Best-in-Class," or the preferred Government-wide solution to leverage

[3] https://www.govinfo.gov/app/details/FR-2021-08-26/2021-17532

[4] See *https://tmf.cio.gov/projects/* for project descriptions.

[5] This does not include funding for classified projects.

[6] See *https://tmf.cio.gov/* for more information.

Table 16–2. ESTIMATED CIVILIAN FEDERAL CYBERSECURITY SPENDING BY AGENCY

(In millions of dollars)

Organization	FY 2021	FY 2022	FY 2023
Civilian CFO Act Agencies	**$8,173**	**$9,387**	**$10,462**
Department of Agriculture	$223	$239	$248
Department of Commerce	$472	$422	$437
Department of Education	$165	$225	$231
Department of Energy	$711	$793	$722
Department of Health and Human Services	$598	$715	$818
Department of Homeland Security	$2,097	$2,409	$2,621
Department of Housing and Urban Development	$81	$76	$99
Department of Justice	$934	$1,241	$1,281
Department of Labor	$109	$105	$100
Department of State	$320	$447	$635
Department of the Interior	$124	$144	$165
Department of the Treasury	$653	$829	$970
Department of Transportation	$334	$345	$391
Department of Veterans Affairs	$472	$450	$587
Environmental Protection Agency	$28	$29	$54
General Services Administration	$80	$78	$108
National Aeronautics and Space Administration	$155	$187	$243
National Science Foundation	$244	$256	$287
Nuclear Regulatory Commission	$27	$25	$21
Office of Personnel Management	$44	$44	$45
Small Business Administration	$17	$17	$17
Social Security Administration	$243	$266	$302
U.S. Agency for International Development	$44	$43	$77
Non-CFO Act Agencies	**$468.5**	**$454.7**	**$653.1**
Access Board	$0.6	$0.6	$0
African Development Foundation	$1.0	$1.0	*
American Battle Monuments Commission	$1.3	$1.3	$0
Armed Forces Retirement Home	*	*	$0
Chemical Safety and Hazard Investigation Board	$2.7	$2.6	$1.2
Commission on Civil Rights	$0.5	$0.8	$0.6
Commodity Futures Trading Commission	$9.2	$9.6	$13.3
Consumer Product Safety Commission	$3.1	$3.2	$3.9
Corporation for National and Community Service	$4.8	$4.8	$7.7
Council of the Inspectors General on Integrity and Efficiency	$0.6	$0.6	*
Court Services and Offender Supervision Agency for the District	$4.0	$4.0	$0
Defense Nuclear Facilities Safety Board	$2.8	$2.6	$2.0
Denali Commission	*	*	$1.0
Election Assistance Commission	*	*	$2.3
Equal Employment Opportunity Commission	$5.4	$5.5	$6.1
Export-Import Bank of the United States	$4.6	$3.9	$4.6
Farm Credit Administration	$3.6	$3.8	$4.0
Federal Communications Commission	$26.0	$27.0	$18.1
Federal Deposit Insurance Corporation	$109.8	$109.8	$83.7
Federal Election Commission	$1.0	$1.0	$0
Federal Financial Institutions Examination Council	*	*	*
Federal Labor Relations Authority	*	*	*
Federal Maritime Commission	*	$0.9	$0.7
Federal Mediation and Conciliation Service	*	*	$1.6
Federal Mine Safety and Health Review Commission	*	*	$0
Federal Retirement Thrift Investment Board	$85.5	$67.3	$30.3
Federal Trade Commission	$12.6	$12.8	$16.9
Gulf Coast Ecosystem Restoration Council	*	*	*
Institute of Museum and Library Services	*	*	$0
Inter-American Foundation	*	*	*
International Trade Commission	$5.4	$6.3	$5.5

Table 16–2. ESTIMATED CIVILIAN FEDERAL CYBERSECURITY SPENDING BY AGENCY—Continued
(In millions of dollars)

Organization	FY 2021	FY 2022	FY 2023
Marine Mammal Commission	*	*	*
Merit Systems Protection Board	$0.7	$0.6	$0.8
Millennium Challenge Corporation	$1.5	$1.5	$1.6
Morris K. Udall and Stewart L. Udall Foundation	*	*	*
National Archives and Records Administration	$7.8	$7.8	$8.4
National Council on Disability	*	*	*
National Credit Union Administration	$7.3	$7.3	$0
National Endowment for the Arts	$1.2	$1.2	$4.7
National Endowment for the Humanities	$1.2	$1.2	$1.4
National Gallery of Art	$2.1	$2.1	$2.3
National Labor Relations Board	$2.3	$3.3	$6.2
National Mediation Board	*	*	$2.1
National Transportation Safety Board	$1.7	$1.8	$5.7
Nuclear Waste Technical Review Board	*	*	$0
Occupational Safety and Health Review Commission	$1.0	$1.1	$1.1
Office of Government Ethics	*	*	*
Office of Special Counsel	*	*	$1.1
Office of the Comptroller of the Currency	*	*	$0
Overseas Private Investment Corporation	*	*	$0
Peace Corps	$9.4	$10.8	$8.0
Pension Benefit Guaranty Corporation	*	*	$26.3
Postal Regulatory Commission	*	*	$1.1
Presidio Trust	*	*	$0
Privacy and Civil Liberties Oversight Board	$1.4	$1.4	$0
Railroad Retirement Board	*	*	$7.5
Securities and Exchange Commission	$44.3	$52.1	$52.1
Selective Service System	$2.0	$5.0	*
Smithsonian Institution	$9.9	$12.8	$11.5
Surface Transportation Board	$1.5	$1.4	$1.4
Tennessee Valley Authority	$53.5	$37.8	$64.1
Trade and Development Agency	$1.3	$1.3	$1.3
U.S. Agency for Global Media	$7.8	$8.0	$7.0
U.S. Army Corps of Engineers	$20.3	$20.4	$4.0
United States Holocaust Memorial Museum	$1.7	$2.2	$2.8
Total	$8,641.7	$9,841.6	$10,890

* $500,000 or less

the Government's buying power for telecommunications and IT infrastructure requirements. As Federal agencies transition to the EIS contracts, they are taking the opportunity to develop a holistic approach towards achieving a zero-trust architecture via software defined networking that encompasses cloud infrastructure, enhanced mobility capabilities, and embedded cybersecurity and satellite communications. EIS is the only Federal network services contract to include requirements from OMB policy directives and NIST and Department of Homeland Security (DHS) cybersecurity requirements. Through aggregated Federal buying, if agencies modernize their services, EIS is projected to result in an average of 13 percent cost savings over the expiring Networx contract and an average of 30 percent less than large commercial contracts to the Federal Government once agencies finish their transition. Modern, secure, and cost-effective communications networks are enabling Federal agencies to continue to adopt a modern IT infrastructure and improve public services. As of December 31, 2021, Federal agencies have awarded more than 180 EIS task orders and are in the process of transitioning their existing legacy circuits to new solutions offered by EIS. Agencies have identified an additional 28 task orders to be awarded by FY 2023. The EIS team estimates that when all transitions are completed, agencies will have transitioned more than 9 million legacy circuits off the expiring contracts.

Improving the IT and Cybersecurity Workforce

Maintaining and securing Federal IT requires a large, highly capable IT and cybersecurity workforce. A current focus for policies guiding the strengthening of the Federal IT workforce is the direction given to Federal agencies to build a diverse workforce, representative of the population they serve, able to leverage data as a strategic asset to support economic growth, increase the effectiveness

of the Federal Government, facilitate oversight, and promote transparency.

To accomplish this goal, agencies need a workforce that is highly trained and equipped with modern-day technical skills in areas such as data science, cybersecurity, machine learning, and artificial intelligence. As technology is a rapidly-changing field, the Administration is committed to investing in the Federal workforce to ensure they are equipped to adapt and develop their skills. To date, the Government has taken steps to expand the IT workforce, and provide training and other professional development opportunities to build skillsets and capacity across the Federal enterprise. Filling cybersecurity positions is a priority in the Administration's efforts to strengthen and safeguard the digital infrastructure for the public and private sectors. The Government will continue to evaluate processes and practices related to recruiting, hiring, and retention, as well as applying the lessons learned from the COVID-19 pandemic.

The President's Budget continues to invest in the IT and cybersecurity workforce to make the Government an attractive employer for top-tier talent, improve our ability to oversee and administer Government-wide programs, and better deliver services to the American people. For example, a diverse, highly skilled IT workforce is essential for the Government's ability to innovate in artificial intelligence and machine learning. Agencies need staff who understand these technologies, both to generate the foundational data needed for them to operate, as well as to manage the automated services to ensure they are accurate, fair, and aligned to the needs of the Government and the American people. Agencies also need cross-functional professionals to work in areas such as financial management, acquisition, and privacy protections, to drive value across a range of Government domains. Ultimately, a strong cadre of cybersecurity and IT professionals will allow the Government to run more efficiently and effectively, ensure Government networks and data are protected and secure, and drive more user-centric services to the American people.

Digital First Customer Experience

Americans expect and deserve their interactions with the Federal Government to be simple, seamless, and secure. The Administration is dedicated to providing the public with better digital services, streamlining agency processes, integrating access and equity into products, and saving taxpayer dollars. Technology powers an outstanding customer experience and is essential to excellent service delivery. The Federal technology environment needs to supports delivering secure, best-in-class products that actually meet the needs of their customers, the American people.

Toward this endeavor, the President's Budget reflects the needs of the Federal Government to modernize websites and digitize forms and processes which improve customer experience, and supports ongoing, multi-year implementation efforts to improve service delivery under the 21st Century Integrated Digital Experience Act (P.L. 115-336). The President's Budget also supports technology resources for high impact service providers and other Government-wide customer experience improvements under Executive Order 14058, "Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government," including increases to Government-wide common products, platforms, and services that enable interactions that are consistent across Government. This includes products and platforms such as login.gov, U.S. Web Design System, Digital Analytics Program, Touchpoints, and Federalist; increases to the use and availability of funding vehicles (e.g., the TMF) or incubator programs (e.g., 10x); and continued efforts to bring top digital service delivery talent to the Federal Government.

Table 16–3. NIST FRAMEWORK FUNCTION CIVILIAN CFO ACT AGENCY FUNDING TOTALS
(In millions of dollars)

NIST Framework Function	FY 2022	FY 2023
Identify	$2,891	$3,046.0
Protect	$3,617	$4,741.3
Detect	$1,106	$1,483.8
Respond	$1,485	$1,208.4
Recover	$289	$410.6
Total	**$9,387**	**$10.890**

This analysis excludes Department of Defense spending.

Moreover, while the Federal Government continues efforts to provide world class digital experiences for the American people, care needs to be taken to ensure that "digital first" does not become "digital only." The goal should be to ensure that services are designed for all people of all abilities with a particular focus on those that are underserved. The President's Budget supports accessibility efforts to build and sustain an accessible Federal technology environment for all as directed in Executive Order 13985, "Advancing Racial Equity and Support for Underserved Communities Through the Federal Government," and Executive Order 14035, "Diversity, Equity, Inclusion, and Accessibility in the Federal Workforce."

Shared Services

Shared Services include the Government-wide identification and creation of centralized capabilities, shared governance, and performance expectations that are current for common functions across government. These will lead the way to transform the Federal Government by enabling the delivery of innovative, flexible, and competitive solutions and services that improve mission support service quality and decrease the total cost of services across the Federal enterprise.

Sharing Quality Services provides a framework for modernizing the Federal Government in key function areas that will improve the ability of agencies to deliver mission outcomes, provide improved services, and effectively steward taxpayer dollars. This framework includes a new governance structure where agencies and customers are responsible for driving the future of Federal

service delivery. As agencies work with their customer communities to adopt and establish sharing standards, new Quality Service Management Offices (QSMOs), which are responsible for establishing marketplaces for coordinating solutions in their respective function areas, will be proposed to OMB. Since the release of OMB Memorandum M-19-16, Centralized Mission Support Capabilities for the Federal Government, OMB has formally designated four QSMOs: Cybersecurity, Core Financial Management, Civilian HR Transaction Services, and Grants Management.

In FY 2021, the Cybersecurity QSMO, led by the Department of Homeland Security, introduced two new services: Vulnerability Disclosure Policy (VDP) and Protective Domain Name System (pDNS). The VDP service[7] helps agencies streamline day-to-day operations when the public identifies and reports cyber vulnerabilities of Federal systems to the Government. The pDNS service helps agencies identify and neutralizes malicious DNS content used in cyberattacks.

The Grants Management QSMO, led by the Department of Health and Human Services, also released its initial marketplace in FY 2021, identifying a dozen systems. The Grants QSMO[8] is now working to verify that the functionality of these systems is consistent with the agreed to grants standards.

The remaining QSMOs are working to release their marketplaces as soon as possible, potentially as early as FY 2023.

Data as a Strategic Asset

OMB released the Federal Data Strategy (FDS) in 2019 as a foundational document for enabling agencies to use and manage Federal data to serve the American people. The FDS provides a consistent framework of principles and practices that are in-tended to guide agencies as they continue to leverage, utilize, and implement data as a resource and strategic asset. The FDS provides an overarching and iterative approach to data stewardship through the release of annual action plans that support the implementation of the strategy over an eight-year period.

The FDS and annual action plans continue to align with current OMB guidance, priorities, initiatives, and other relevant interagency councils on data-related equities that promote open data, equity, data sharing, accountability, and transparency. OMB promotes leveraging data as a strategic asset and efforts that align and adhere to the Open, Public, Electronic and Necessary (OPEN) Government Data Act, Administration priorities, and the President's Management Agenda, as well as promoting greater coordination and collaboration with the Chief Data Officers Council.

The Equitable Data Working Group, established through Executive Order 13985 explores ways to leverage Government data in order to measure and promote equity. The intent is to assess long-standing barriers and encourage lasting change in advancing equitable outcomes in underserved communities. Agencies will be able to use what is learned to advance their own efforts while developing and committing to ongoing initiatives to advance equity.

Administration priorities—including strengthening and empowering the Federal workforce, advancing equity and support for underserved communities, delivering excellent, equitable, and secure Federal services transforming customer experience and service delivery, improving the Nation's cybersecurity, and managing the business of Government to build back better—rely on data to improve the ability to deliver the requisite mission critical services for the American public.

[7] *https://bugcrowd.com/programs/organizations/cisa*

[8] *https://ussm.gsa.gov/fibf-gm/*