

14. INFORMATION TECHNOLOGY AND CYBERSECURITY FUNDING

Information Technology Priorities

Technology serves as the foundation of the Federal Government's ability to deliver on its mission. The Administration is leading on the technology issues of our time—stopping foreign intrusions into U.S. agencies, balancing difficult trade-offs in digital identity and artificial intelligence, redefining security expectations for software and the cloud, and maximizing the impact of taxpayer dollars to drive digital transformation across the Government to deliver a better customer experience for the American people. The Budget supports launching tech policy that meets today's expectations and technology that is secure by design, allowing Federal agencies to deliver on their missions safely, reliably, and easily. The Administration is focused on understanding where agencies are on their IT modernization journeys and making the right investments at the right time to enable secure technology and innovation to advance from year to year. The Budget proposes spending \$74 billion on IT at civilian agencies in 2024, which will be used to deliver simple, seamless, and secure Government services. 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.

In June 2022, OMB released the “Information Technology Operating Plan” that focuses on four strategic priorities all enabled by a strong Federal workforce.¹ The priorities include:

Cybersecurity—Bolstering cybersecurity by ensuring every Department and Agency is increasing the safety and security of public services, and implementing the requirements contained in the Executive Order 14028, “Improving the Nation’s Cybersecurity,” as well as the Federal Zero Trust Strategy. To address this in the 24 Budget, OMB and the Office of the National Cyber Director jointly released M-22-16, Administration Cybersecurity Priorities for the FY 2024 Budget. This memo directed Federal Civilian Executive Branch (FCEB) agencies to prioritize funding in three cyber investment areas: Improving the Defense and Resilience of Government Networks; Deepening Cross-Sector Collaboration in Defense of Critical Infrastructure; and Strengthening the Foundations of Our Digitally-Enabled Future. The memo also provided additional specificity on areas such as zero trust implementation, sector risk management, and investing in a capable IT and cyber workforce.

IT Modernization—Adopting modern technologies, retiring legacy systems, employing methods of continu-

ous improvement, and scaling them across Government, so that Government can run more effectively and improve the delivery and reliability of trusted services. The President's Budget continues to support funding for the Technology Modernization Fund (TMF), 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. 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.

Digital-First Customer Experience—Using design and technology to deliver an exceptional customer experience for the American public that demonstrably meets user needs and is on par with today's customer expectations. The President's Budget reflects funding for multi-year implementation efforts to improve service delivery under the 21st Century Integrated Digital Experience Act (Public Law 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.

Data as a Strategic Asset—Driving key insights into the decision-making process by harnessing accurate, available, and actionable data to power intelligent Government operations and citizen experiences. 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 intended 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.

Federal Spending on IT

As shown in Table 14-1, the President's Budget for IT at civilian Federal agencies is estimated to be \$74 billion in 2024². This figure is a 13 percent increase from the 2023 estimate. Chart 14-1 shows trending information

¹ https://www.whitehouse.gov/wp-content/uploads/2022/06/Federal-IT-Operating-Plan_June-2022.pdf

² 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.

Table 14–1. ESTIMATED FY 2024 CIVILIAN FEDERAL IT SPENDING AND PERCENTAGE BY AGENCY
(In millions of dollars)

Agency	FY 2024	Percent of Total
Department of Veterans Affairs	\$10,991	14.7%
Department of Health and Human Services	\$10,006	13.4%
Department of Homeland Security	\$9,039	12.1%
Department of the Treasury	\$7,137	9.8%
Department of Justice	\$4,805	6.4%
Department of Transportation	\$4,079	5.6%
Department of Agriculture	\$4,069	5.5%
Department of Energy	\$4,024	5.4%
Department of State	\$3,521	4.7%
Department of Commerce	\$2,930	3.9%
Social Security Administration	\$2,502	3.4%
National Aeronautics and Space Administration	\$2,393	3.2%
Department of the Interior	\$1,971	2.5%
Department of Education	\$1,742	2.3%
General Services Administration	\$1,125	1.5%
Department of Labor	\$1,047	1.4%
Department of Housing and Urban Development	\$526	0.7%
Environmental Protection Agency	\$504	0.7%
Small Business Administration	\$445	0.6%
Office of Personnel Management	\$442	0.6%
U.S. Agency for International Development	\$376	0.5%
U.S. Army Corps of Engineers	\$285	0.4%
National Science Foundation	\$192	0.3%
Nuclear Regulatory Commission	\$174	0.2%
National Archives and Records Administration	\$108	0.2%
Total	\$74,435	100%

This analysis excludes the Department of Defense.

for Federal civilian IT spending from 2021 forward.³ The President’s Budget includes funding for 4,529 investments at 25 agencies. These investments support the three IT Portfolio areas shown in Chart 14-2. Of those 4,529 IT investments, 588 have been designated as major IT investments. As outlined in OMB Circular A-11 Section 55: IT Investments Guidance, agencies are required to determine major IT investment designations based on several factors including, but not limited to, whether the investment under consideration has significant program or policy implications; has high executive or public visibility; has high development, high operating, and/or high maintenance costs; or requires special management attention because of its importance to the agency’s mission or critical functions. For each designated major IT investment, agencies are required to submit a business case analysis which provides additional transparency regarding the major investment’s cost, schedule, risk, and performance. OMB also requires that each reporting agency Chief Information Officer (CIO) provide additional risk ratings for each major IT investment reported on the IT Dashboard website. Throughout the fiscal year, agency CIOs are required to continuously reassess how risks

for their major IT investments are being managed and mitigated.

Federal Spending on Cybersecurity

Cybersecurity is a top priority for this Administration. Our adversaries continue to employ novel and sophisticated methods in an effort to compromise Federal systems. With the release of [Executive Order 14028](#), “Improving the Nation’s Cybersecurity” on May 12, 2021, the Administration initiated a paradigm shift for cybersecurity. The Executive Order sets a framework to aggressively change the cybersecurity strategy and culture across the Federal enterprise to ultimately center around leading industry practices. Through implementation of Executive Order 14028, Federal agencies are enhancing the protection of Federal systems through modernization of cybersecurity defenses, improving information sharing between the U.S. Government and the private sector, and strengthening the United States’ ability to rapidly respond to incidents when they occur. Agencies can no longer rely on a perimeter-based approach or “digital walls” to keep sophisticated actors from gaining unauthorized access to Federal systems. The Administration is focused on making Federal systems more defensible by adopting zero trust principles, a security strategy premised on the idea that trust is never granted implicitly but must be continually evaluated.

³ 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.

To that end, OMB has released several government-wide policies that align to the zero trust vision outlined in Executive Order 14028. On January 26, 2022, OMB released [*OMB Memorandum 22-09*](#), Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, or the Federal Zero Trust Strategy. The strategy requires agencies to invest in technology that is built and deployed with security foremost in mind and move towards a zero trust architecture that provides the vigilance to detect malicious behaviors and react quickly. The Federal Zero Trust Strategy and associated agency implementation plans delineate meaningful milestones in implementing a zero trust architecture.

In September 2022, OMB took new actions to address potential security gaps in the software supply chain. By issuing [*OMB Memorandum 22-18*](#), Enhancing the Security of the Software Supply Chain through Secure Development Practices, the Administration focused agencies on shifting to exclusively utilizing software developed with appropriate security practices in place. This memorandum focuses on minimizing the risks associated with running unvetted technologies on agency networks, increasing the resilience of Federal technology against cyber threats.

Additionally, OMB will carry forward the vision—not just the actions—laid out in Executive Order 14028. The cyber landscape is rapidly evolving, and we will continue to discover new threats and tactics that our adversaries

intend to use against us. This is why agencies must build upon the strategic direction of Executive Order 14028 and take actions to secure Federal systems against all present and future threats as they become known to us. For example, the Administration recognized the future threat that quantum computers may pose to the Federal Government, and consequently published [*OMB Memorandum 23-02*](#), Migrating to Post-Quantum Cryptography, which establishes requirements for agencies to prioritize and identify where they are using cryptography within their most sensitive systems that are vulnerable to decryption by a future quantum computer. This guidance will help prepare our Government for an inevitable shift in security that could ultimately expose securely encrypted secrets to foreign adversaries if we do not act decisively.

In the two years since the release of Executive Order 14028, Federal agencies have made considerable progress towards a more cyber-secure future. Agencies are implementing higher levels of encryption, using the best methods in the industry to verify legitimate users, and utilizing toolsets that create constant vigilance within Federal systems. These efforts to adopt technologies and practices that enhance cybersecurity defenses and ensuring the human capital to maintain these endeavors will and must continue. The President's Budget includes approximately \$12.7 billion of budget authority for civilian cybersecurity-related activities, an increase of 13 percent over the prior year.

Table 14–2. ESTIMATED CIVILIAN FEDERAL CYBERSECURITY SPENDING BY AGENCY
(In millions of dollars)

Organization	FY 2022	FY 2023	FY 2024
Civilian CFO Act Agencies	\$9,554	\$10,700	\$12,170
Department of Agriculture	\$269	\$239	\$248
Department of Commerce	\$442	\$478	\$427
Department of Education	\$194	\$217	\$313
Department of Energy	\$785	\$788	\$928
Department of Health and Human Services	\$695	\$813	\$947
Department of Homeland Security	\$2,578	\$2,920	\$3,097
Department of Housing and Urban Development	\$52	\$74	\$88
Department of Justice	\$957	\$1,174	\$1,353
Department of Labor	\$82	\$96	\$124
Department of State	\$565	\$570	\$748
Department of the Interior	\$145	\$164	\$192
Department of the Treasury	\$749	\$963	\$1,042
Department of Transportation	\$358	\$414	\$443
Department of Veterans Affairs	\$645	\$611	\$927
Environmental Protection Agency	\$58	\$37	\$67
General Services Administration	\$103	\$127	\$129
National Aeronautics and Space Administration	\$174	\$198	\$196
National Science Foundation	\$278	\$295	\$300
Nuclear Regulatory Commission	\$32	\$38	\$37
Office of Personnel Management	\$40	\$45	\$53
Small Business Administration	\$31	\$26	\$37
Social Security Administration	\$254	\$330	\$376
U.S. Agency for International Development	\$69	\$82	\$97
Non-CFO Act Agencies	\$459.6	\$489.1	\$548.5
Access Board	\$0.3	\$0.8	\$0.8
American Battle Monuments Commission	\$1.3	\$1.3	\$1.3
Armed Forces Retirement Home	*	*	*
U.S. Agency for Global Media	\$5.9	\$6.0	\$10.7
Chemical Safety and Hazard Investigation Board	\$1.6	\$0.7	\$0.7
Commission on Civil Rights	\$0.8	\$0.6	\$1.0
Commodity Futures Trading Commission	\$12.6	\$13.6	\$15.4
Consumer Product Safety Commission	\$3.2	\$4.7	\$3.8
Corporation for National and Community Service	\$4.1	\$6.8	\$11.2
Council of the Inspectors General on Integrity and Efficiency	\$0.4	\$0.8	\$0.8
Court Services and Offender Supervision Agency for the District	\$4.0	\$4.0	\$4.0
Defense Nuclear Facilities Safety Board	\$2.1	\$3.3	\$3.8
Equal Employment Opportunity Commission	\$6.4	\$8.8	\$8.7
Export-Import Bank of the United States	\$5.4	\$4.6	\$5.0
Farm Credit Administration	\$3.8	\$4.0	\$4.0
Federal Communications Commission	\$35.5	\$27.3	\$30.5
Federal Deposit Insurance Corporation	\$82.6	\$83.7	\$83.7
Federal Election Commission	*	*	*
Federal Financial Institutions Examination Council	*	*	*
Federal Labor Relations Authority	\$0.5	\$0.5	\$0.6
Federal Maritime Commission	\$0.3	\$0.3	\$0.4
Federal Retirement Thrift Investment Board	\$57.8	\$29.0	\$24.3
Federal Trade Commission	\$16.0	\$25.0	\$41.1
Gulf Coast Ecosystem Restoration Council	*	*	*
Institute of Museum and Library Services	\$0.5	\$0.7	\$0.9
African Development Foundation	\$2.1	\$2.4	\$2.5
Inter-American Foundation	*	*	*
Millennium Challenge Corporation	\$1.5	\$2.2	\$2.3
Overseas Private Investment Corporation	*	*	*
Peace Corps	\$8.8	\$12.3	\$23.0
Trade and Development Agency	\$1.3	\$1.3	\$1.3

Table 14-2. ESTIMATED CIVILIAN FEDERAL CYBERSECURITY SPENDING BY AGENCY—Continued
(In millions of dollars)

Organization	FY 2022	FY 2023	FY 2024
International Trade Commission	\$3.4	\$5.5	\$6.5
Marine Mammal Commission	*	*	*
Merit Systems Protection Board	\$0.5	\$0.8	\$1.7
Morris K. Udall and Stewart L. Udall Foundation	\$0.1	\$0.2	\$0.2
National Archives and Records Administration	\$10.0	\$10.8	\$21.6
National Credit Union Administration	\$10.6	\$13.2	\$14.2
National Endowment for the Arts	\$1.5	\$5.2	\$4.3
National Endowment for the Humanities	\$1.1	\$1.3	\$1.6
National Labor Relations Board	\$3.3	\$4.1	\$5.8
National Transportation Safety Board	\$4.8	\$5.8	\$7.3
Nuclear Waste Technical Review Board	\$0.4	\$0.4	\$0.5
Occupational Safety and Health Review Commission	\$1.1	\$1.1	\$1.1
Office of Government Ethics	\$0.3	\$0.7	\$3.4
Office of Special Counsel	\$1.2	\$1.1	\$1.1
Presidio Trust	\$0.6	*	*
Privacy and Civil Liberties Oversight Board	\$2.1	\$2.0	\$2.0
Railroad Retirement Board	\$5.1	\$6.1	\$7.6
Securities and Exchange Commission	\$59.8	\$58.0	\$58.0
Selective Service System	\$2.0	\$0.5	\$0.0
Smithsonian Institution	\$9.8	\$13.3	\$14.9
Surface Transportation Board	\$1.2	\$1.4	\$1.1
Tennessee Valley Authority	\$44.9	\$74.7	\$57.3
U.S. Army Corps of Engineers	\$4.0	\$4.0	\$15.0
United States Holocaust Memorial Museum	\$1.7	\$2.8	\$3.0
United States Institute of Peace	*	*	*
National Gallery of Art	\$3.7	\$3.9	\$4.3
Postal Regulatory Commission	\$1.0	\$1.1	\$2.1
Pension Benefit Guaranty Corporation	\$26.9	\$26.6	\$32.2
Total	\$10,014	\$11,189	\$12,718

* \$500,000 or less

CHART 14-1. TRENDS IN FEDERAL CIVILIAN IT SPENDING

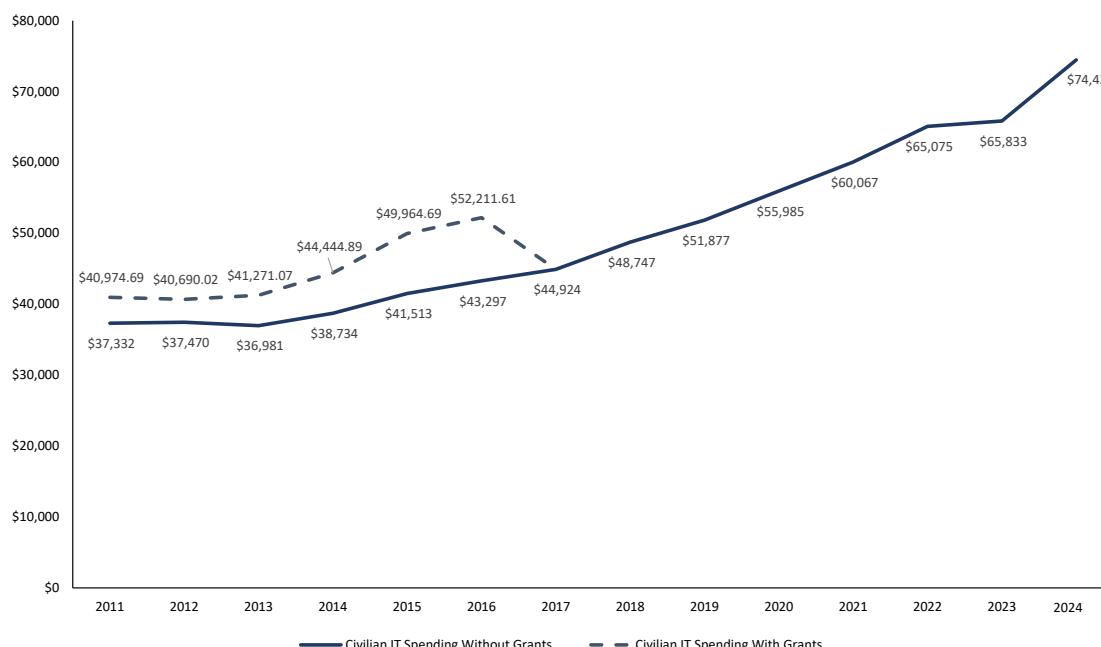


Table 14–3. NIST FRAMEWORK FUNCTION CIVILIAN CFO ACT AGENCY FUNDING TOTALS
 (In millions of dollars)

NIST Framework Function	FY 2023	FY 2024
Identify	3,435	3,500
Protect	4,392	5,058
Detect	1,148	1,266
Respond	1,410	1,637
Recover	315	344
M-22-16 Priorities	366
Total	10,700	12,170

This analysis excludes Department of Defense spending.

CHART 14-2. FY 2024 CIVILIAN IT INVESTMENT PORTFOLIO SUMMARY

