AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

12. 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 President proposes spending $58.4 billion on IT at civilian agencies in FY 2022[1], which will be used to deliver critical citizen services, keep sensitive data and systems secure, and further the vision of digital Government. The Budget also supports the implementation of Federal laws that enable agency technology planning, oversight, funding, and accountability practices and Office of Management and Budget (OMB) guidance to agencies on the strategic use of IT to enable mission outcomes. It supports the modernization of antiquated and often unsecured IT; agency 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.

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. The President's Budget includes approximately $9.8 billion for civilian cybersecurity funding, which supports the protection of Federal IT and our 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 12-1, the Federal Government Budget for IT at civilian Federal agencies is estimated to be $58.4 billion in 2022. This figure is a 2.4 percent increase from the estimate reported for 2021. Chart 12-1 shows trending information for Federal civilian IT spending from 2020 forward.[2] The 2022 Budget includes funding for 4,531 investments at 25 agencies. These investments support the three IT Portfolio areas shown in Chart 12-2.

Of those 4,531 IT investments, 546 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 is a top priority for this Administration, and recent events, such as the SolarWinds cyber incident, have shown that adversaries continue to target Federal systems. Recognizing that this is a critical issue that must be prioritized, the President's Budget includes approximately $9.8 billion of budget authority for civilian cybersecurity-related activities. This figure is a 14 percent increase from the estimate reported for 2021. Cybersecurity budgetary priorities will continue to seek to reduce the risk and impact of cyber incidents (e.g. SolarWinds), based on data-driven, risk-based assessments of the threat environment and the current Federal cybersecurity posture. Table 12-2 provides an agency level view of cybersecurity spending. Table 12-3 provides an overview of civilian Chief Financial Officers (CFO) Act Agency cybersecurity spending as aligned to the National Institute of Standards and Technology (NIST) 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.

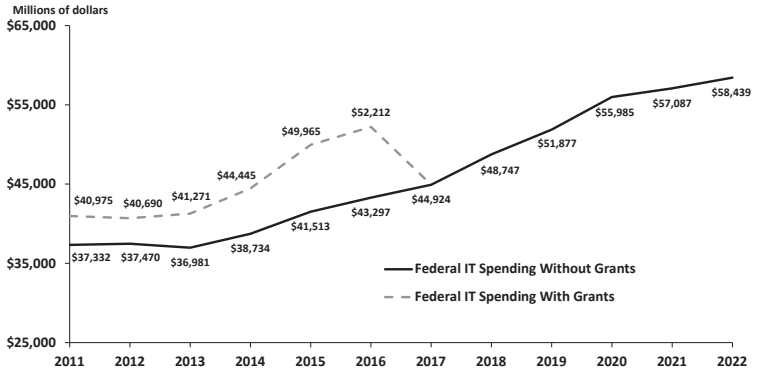
IT Modernization

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 has been 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 sus-

[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 12-1. Trends in Federal Civilian IT Spending



Notes: Investments labeled as 'Part 06 – Grants to State and Local IT Investments' were excluded from FY 2011 – 2015 figures. Investments labeled 'Part 04 - Grants and Other Transferred Funding' were excluded in FY 2016 figures. FY 2017 – 2020 estimates did not include these types of investments.

tained change in Federal technology, deployment, security, and service delivery.

Notable IT Modernization efforts include Cloud Adoption, Shared Services, and IPv6, among other efforts. The Federal Government will continue to accelerate the adoption of cloud technologies to improve the efficiency of Government business and communications. Cloud Adoption positioned Federal agencies to convert to maximum telework during the COVID-19 pandemic, rapidly and proficiently enabling the continuity of their missions. 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. The Federal Government is also continuing its transition to Internet Protocol 6 (IPv6), replacing IPv4. The global demand for IP addresses has grown exponentially with the ever-increasing number of users, devices, and virtual entities connecting to the Internet, resulting in the exhaustion of readily available IPv4 addresses in all regions of the world. While stop-gap measures have served to extend IPv4's viability thus far, it is imperative that IPv6, with its vastly larger address space, sees widespread adoption in the near future. This will accommodate Internet growth and innovation, giving better support to mobility, security, and virtualized network services.

Technology Modernization Fund

The Budget includes $500 million for the Technology Modernization Fund (TMF), building on the $1 billion provided in the American Rescue Plan, to strengthen Federal cybersecurity and retire antiquated technology systems. 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 TMF through the American Rescue Plan recognizes the critical need to provide funding to address urgent IT modernization challenges, bolster cybersecurity defenses following the SolarWinds incident, and improve the delivery of COVID-19 relief. The Administration will prioritize projects that focus on high-priority systems modernization, cybersecurity, public-facing digital services, and cross-government services and infrastructure. To implement the TMF funding provided through the American Rescue Plan, the TMF model has been updated to include repayment flexibilities that may accelerate modernization efforts to better serve the American public.

The TMF is an innovative funding vehicle that gives agencies additional ways to deliver services to the

Chart 12-2. 2022 Federal Civilian IT Investment Portfolio Summary

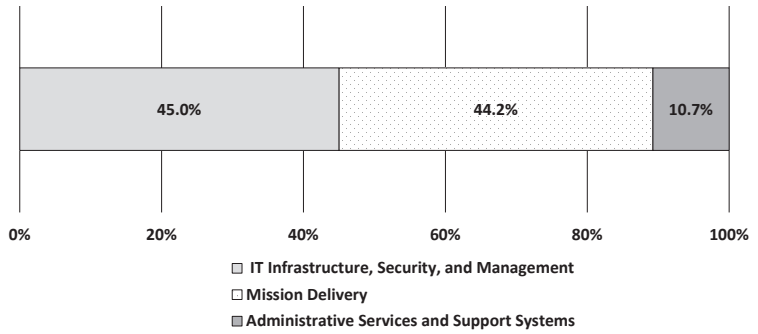


Table 12–1. ESTIMATED FY 2022 CIVILIAN FEDERAL IT SPENDING AND PERCENTAGE BY AGENCY
(In millions of dollars)

Agency	FY 2022	Percent of Total
Department of Veterans Affairs	$8,495	14.5%
Department of Homeland Security	$8,150	13.9%
Department of Health and Human Services	$6,956	11.9%
Department of the Treasury	$5,967	10.2%
Department of Transportation	$3,694	6.3%
Department of Justice	$3,475	5.9%
Department of Energy	$3,245	5.6%
Department of Agriculture	$2,762	4.7%
Department of State	$2,756	4.7%
Department of Commerce	$2,598	4.4%
Social Security Administration	$2,157	3.7%
National Aeronautics and Space Administration	$2,145	3.7%
Department of the Interior	$1,502	2.6%
Department of Education	$982	1.7%
Department of Labor	$819	1.4%
General Services Administration	$702	1.2%
Department of Housing and Urban Development	$437	0.7%
Environmental Protection Agency	$370	0.6%
U.S. Army Corps of Engineers	$269	0.5%
U.S. Agency for International Development	$263	0.4%
National Science Foundation	$165	0.3%
Nuclear Regulatory Commission	$152	0.3%
Office of Personnel Management	$141	0.2%
National Archives and Records Administration	$127	0.2%
Small Business Administration	$109	0.2%
Total	**$58,439**	**100.0%**

This analysis excludes the Department of Defense

American public more quickly, to better secure sensitive systems and data, and to use taxpayer dollars more efficiently.[3] 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. The TMF awards are levers to accelerate modernization across the Government in a manner that demonstrates efficient management of taxpayer resources.

Since its start in March 2019, the TMF Board has awarded ten initiatives a total of approximately $79.4 million. In 2020, the TMF Board awarded $15 million for one new modernization project – the Automated Commercial Environment Collections Module (ACE). This project serves to update the Customs and Border Protection's (CPB's) 30-year old collection tool, the Automated Commercial System (ACS), to meet the demands of the CBP mission and provide the agency with a flexible secure platform to support the growing complexities of global trade and CBP enforcement.

Improving the IT and Cyber Workforce

Maintaining and securing Federal IT requires a large, highly capable IT and Cyber workforce. A current focus for policies guiding the strengthening of the Federal IT workforce is the direction given to Federal agencies to build a workforce 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, 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 Government-wide.

The President's Budget continues to invest in the IT and Cyber 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 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 who can work in areas like 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, and drive more user-centric services to the American people.

United States Digital Service

Americans expect and deserve their interactions with the Federal Government to be simple, fast, and responsive. The United States Digital Service (USDS) is enhancing the Federal Government's most critical public-facing digital services through design and technology expertise. USDS recruits some of the country's top technical talent and partners directly with Federal Agencies to ensure that critical services reach the public. USDS projects not only provide the public with better digital services, but also help streamline agency processes and save taxpayer dollars. Recognizing this, the Administration requested and Congress appropriated $200 million through the American Rescue Plan for USDS that is being used to increase the number of USDS personnel. This will allow USDS to quickly address technology emergencies, ensure access and equity are integrated into products and processes, and help agencies modernize their systems for long-term stability.

[3] See *https://tmf.cio.gov/*

Table 12–2. ESTIMATED CIVILIAN FEDERAL CYBERSECURITY SPENDING BY AGENCY
(In millions of dollars)

Organization	FY 2020	FY 2021	FY 2022
Civilian CFO Act Agencies	**$7,383**	**$8,184**	**$9,402**
Department of Agriculture	$223	$223	$239
Department of Commerce	$701	$472	$422
Department of Education	$123	$165	$225
Department of Energy	$590	$711	$793
Department of Health and Human Services	$544	$598	$715
Department of Homeland Security	$1,613	$2,097	$2,409
Department of Housing and Urban Development	$73	$81	$76
Department of Justice	$903	$934	$1,241
Department of Labor	$101	$109	$105
Department of State	$284	$320	$447
Department of the Interior	$106	$124	$144
Department of the Treasury	$556	$653	$829
Department of Transportation	$267	$334	$345
Department of Veterans Affairs	$426	$472	$450
Environmental Protection Agency	$29	$28	$29
General Services Administration	$77	$80	$78
National Aeronautics and Space Administration	$162	$155	$187
National Science Foundation	$241	$244	$256
Nuclear Regulatory Commission	$28	$27	$25
Office of Personnel Management	$47	$44	$44
Small Business Administration	$16	$17	$17
Social Security Administration	$216	$243	$266
U.S. Agency for International Development	$57.7	$54.2	$58.1
Non-CFO Act Agencies	**$442.2**	**$466.4**	**$452.1**
Access Board	$0.6	$0.6	$0.6
American Battle Monuments Commission	$0.8	$1.3	$1.3
Armed Forces Retirement Home	*	*	*
U.S. Agency for Global Media	$7.6	$7.8	$8.0
Chemical Safety and Hazard Investigation Board	$0.8	$2.7	$2.6
Commission on Civil Rights	$0.5	$0.5	$0.8
Commodity Futures Trading Commission	$8.7	$9.2	$9.6
Consumer Product Safety Commission	$3.5	$3.1	$3.2
Corporation for National and Community Service	$2.5	$4.8	$4.8
Council of the Inspectors General on Integrity and Efficiency	$0.6	$0.6	$0.6
Court Services and Offender Supervision Agency for the District	$4.0	$4.0	$4.0
Defense Nuclear Facilities Safety Board	$2.1	$2.8	$2.6
Equal Employment Opportunity Commission	$4.8	$5.4	$5.5
Export-Import Bank of the United States	$4.2	$4.6	$3.9
Farm Credit Administration	$3.2	$3.6	$3.8
Federal Communications Commission	$20.0	$26.0	$27.0
Federal Deposit Insurance Corporation	$109.8	$109.8	$109.8
Federal Election Commission	$1.0	$1.0	$1.0
Federal Financial Institutions Examination Council	*	*	*
Federal Labor Relations Authority	*	*	*
Federal Maritime Commission	*	*	$0.9
Federal Retirement Thrift Investment Board	$84.3	$85.5	$67.3
Federal Trade Commission	$12.5	$12.6	$12.8
Gulf Coast Ecosystem Restoration Council	*	*	*
Institute of Museum and Library Services	*	*	*
African Development Foundation	$1.0	$1.0	$1.0
Inter-American Foundation	*	*	*
Millennium Challenge Corporation	$1.7	$1.5	$1.5
Peace Corps	$8.0	$9.4	$10.8
Trade and Development Agency	$1.3	$1.3	$1.3
International Trade Commission	$3.13	$3.36	$3.67

Table 12–2. ESTIMATED CIVILIAN FEDERAL CYBERSECURITY SPENDING BY AGENCY—Continued
(In millions of dollars)

Organization	FY 2020	FY 2021	FY 2022
Marine Mammal Commission	*	*	*
Merit Systems Protection Board	$1.0	$0.7	$0.6
Morris K. Udall and Stewart L. Udall Foundation	*	*	*
National Archives and Records Administration	$7.7	$7.8	$7.8
National Credit Union Administration	$7.4	$7.3	$7.3
National Endowment for the Arts	$1.3	$1.2	$1.2
National Endowment for the Humanities	$1.0	$1.2	$1.2
National Labor Relations Board	$2.2	$2.3	$3.3
National Transportation Safety Board	$1.5	$1.7	$1.8
Nuclear Waste Technical Review Board	*	*	*
Occupational Safety and Health Review Commission	$1.0	$1.0	$1.1
Office of Government Ethics	*	*	*
Office of Special Counsel	*	*	*
Presidio Trust	*	*	*
Privacy and Civil Liberties Oversight Board	$1.4	$1.4	$1.4
Securities and Exchange Commission	$52.8	$44.3	$52.1
Selective Service System	*	$2.0	$5.0
Smithsonian Institution	$8.4	$9.9	$12.8
Surface Transportation Board	$2.3	$1.5	$1.4
Tennessee Valley Authority	$41.4	$53.5	$37.8
U.S. Army Corps of Engineers	$18.8	$20.3	$20.4
United States Holocaust Memorial Museum	$1.6	$1.7	$2.2
United States Institute of Peace	*	*	*
National Gallery of Art	$2.1	$2.1	$2.1
Postal Regulatory Commission	*	*	*
Total	$7,825.6	$8,650.1	$9,854.5

* $500,000 or less

Federal Data Strategy

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 implement existing and future data initiatives. It lays out an overarching and iterative plan on how the Federal Government will accelerate the use of data to deliver on mission and serve the public while promoting data accountability and transparency over the next ten years. Agency progress can be viewed at *https://strategy.data.gov/progress/*.

Table 12–3. NIST FRAMEWORK FUNCTION CIVILIAN CFO ACT AGENCY FUNDING TOTALS
(In millions of dollars)

NIST Framework Function	FY 2022
Identify	$2,894
Protect	$3,622
Detect	$1,108
Respond	$1,488
Recover	$290
Total	**$9,402**

This analysis excludes Department of Defense spending.

Cybersecurity

The President's Budget supports the Administration's commitment to secure Federal networks, protect our Nation's infrastructure, and support efforts to share information, standards, and best practices with our critical infrastructure partners and American businesses. The COVID-19 pandemic and recent cybersecurity incidents continue to highlight the urgent need to modernize and secure Federal technology, and the President's Budget includes resources for Federal civilian agencies to protect their networks and safeguard citizens' sensitive information. This includes critical government-wide protections provided by DHS through the Continuous Diagnostics and Mitigation (CDM) Program. The Budget also fully supports the Department of Defense (DOD) cyber efforts, which include safeguarding DOD's networks, information, and systems; supporting military commander objectives; and defending the nation against cyber threats. In addition to approximately $9.8 billion for civilian cybersecurity funding, the Budget includes $20 million for a new Cyber Response and Recovery Fund to improve national critical infrastructure cybersecurity response.

Assessments of the Federal Government's overall cybersecurity risk continue to find the Federal enterprise to be vulnerable, and the President's Budget provides resources to agencies to continue to implement key cybersecurity hygiene capabilities which are necessary to

defend against cyber criminals and nation-state actors. This section addresses various areas of cybersecurity, including supply chain risk management, Coordinated Vulnerability Disclosure (CVD), and data methodology for assessing the threat environment and the current Federal cybersecurity posture.

With the passage of the 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 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.

Among the most effective methods for obtaining new insights to improve agency information-security programs, CVD enables agencies to coordinate with cybersecurity talent from outside the government to resolve and disclose cybersecurity vulnerabilities in affected products and services, while providing protection for those who uncover these vulnerabilities through good-faith security research. In Fiscal Year 2020, OMB, in coordination with the Department of Homeland Security (DHS), issued memorandum M-20-32, Improving Vulnerability Identification, Management, and Remediation, providing guidance for agencies on management of vulnerability research and CVD programs, as well as Binding Operational Directive 20-01 (BOD-20-01), Develop and Publish a Vulnerability Disclosure Policy, which directed agencies to develop implementation plans providing timelines and milestones for CVD to cover all Federal information systems by May 2, 2021.

Section 630 of the Consolidated Appropriations Act, 2017 (P. L. 115–31) as 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 2020 actual levels reflect the actual budgetary resources available in the prior year, FY 2021 estimates reflect the estimated budgetary resources available in the current year, and FY 2022 levels are to reflect levels consistent with the President's Budget.