19. INFORMATION TECHNOLOGY

Federal Information Technology (IT) provides Americans with important services and information and is the backbone of how Government serves the public in the digital age. The President proposes spending nearly $88 billion on IT at agencies[1], which will be used to deliver critical citizen services, keep sensitive data and systems secure, and to further the vision for modern Government. This budget also supports the Modernize IT to Increase Productivity and Security (IT Modernization) Cross Agency Priority (CAP) Goal of the President's Management Agenda (PMA)[2], Federal laws that enable agency technology planning, oversight, funding, and accountability practices, and OMB guidance to agencies on the strategic use of IT to enable mission outcomes. It also supports the modernization of antiquated and often unsecured legacy systems; 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. These investments will, in alignment with the PMA, 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. This analysis excludes information on classified IT investments by the Department of Defense.

Federal Spending on IT

As shown in Table 19-1, the Federal Government Budget for IT at agencies is estimated to be $88 billion in FY 2020. This figure is an increase from the value reported for FY 2019. Table 19-2 displays IT spending for civilian agencies. The Department of Homeland Security (DHS) is the largest civilian agency in IT spending, while the bottom five agencies represent 1.3 percent of Federal civilian IT spending. Chart 19-1 shows trending information for Federal civilian IT spending through FY 2011.[3]

Table 19–1. OVERVIEW OF FEDERAL IT SPENDING
(In millions of dollars)

	FY 2018	FY 2019	FY 2020
Civilian Agencies	48,747	50,048	51,041
Department of Defense	36,285	37,924	36,749
Total	**85,031**	**87,972**	**87,790**

This analysis excludes Department of Defense classified spending.

Table 19–2. ESTIMATED FY 2020 CIVILIAN FEDERAL IT SPENDING AND PERCENTAGE BY AGENCY
(In millions of dollars)

Agency	FY 2020	Percent of Total
Department of Homeland Security	$7,108	13.9%
Department of Veterans Affairs	$6,118	12.0%
Department of Health and Human Services	$5,646	11.1%
Department of the Treasury	$5,000	9.8%
Department of Commerce	$3,861	7.6%
Department of Justice	$2,995	5.9%
Department of Transportation	$3,699	7.2%
Department of Energy	$2,424	4.7%
Department of Agriculture	$2,217	4.3%
Department of State	$2,272	4.5%
National Aeronautics and Space Administration	$2,157	4.2%
Social Security Administration	$1,969	3.9%
Department of the Interior	$1,283	2.5%
Department of Education	$778	1.5%
Department of Labor	$756	1.5%
General Services Administration	$648	1.3%
U.S. Army Corps of Engineers	$555	1.1%
Department of Housing and Urban Development	$383	0.7%
Environmental Protection Agency	$343	0.7%
U.S. Agency for International Development	$168	0.3%
Office of Personnel Management	$174	0.3%
Nuclear Regulatory Commission	$163	0.3%
National Science Foundation	$132	0.3%
National Archives and Records Administration	$98	0.2%
Small Business Administration	$92	0.2%
Total	**$51,041**	**100.0%**

This analysis excludes the Department of Defense

IT Investments Overview

The FY 2020 budget includes funding for 7,653 IT investments at agencies. These investments support three main functions: mission delivery; IT infrastructure, IT security, and IT management; and administrative services, and mission support (see Chart 19-2). As Chart 19-3 shows, IT investments can vary widely in size and scope. As a result, the largest 100 investments at civilian agencies account for 44 percent of Federal IT spending.

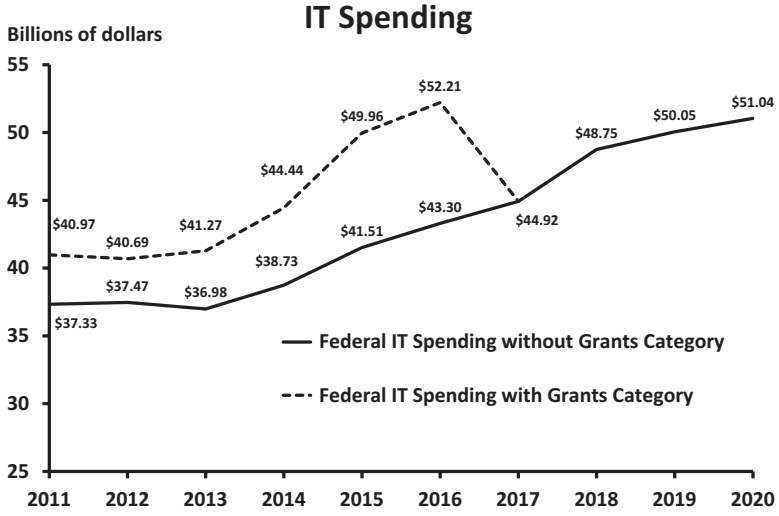
Of those 7,653 IT investments, 584 are major IT investments. As outlined in A-11 and FY 2020 Capital Planning and Investment Control (CPIC) Guidance, agencies determine if an IT investment is classified as major based on whether the associated investment has significant program or policy implications; 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 by CPIC

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

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

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

Chart 19-1. Trends in Federal Civilian IT Spending



Part 06—Grants to State and Local IT Investments" were excluded from 2011 – 2015 figures. Investments labeled "Part 04 - Grants and Other Transferred Funding" were excluded in 2016 figures. The 2017 – 2020 estimates did not include these types of investments.
This analysis excludes the Department of Defense

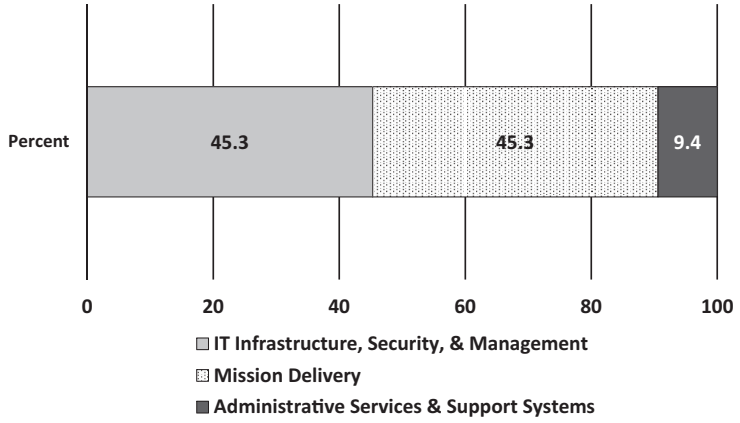
Guidance to submit Business Cases, which provide additional transparency regarding the cost, schedule, risk, and performance data related to its spending.

OMB requires that agency 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. The Agency CIO rates each investment based on his or her best judgment, using a set of pre-established criteria. As a rule, the evaluation should reflect the CIO's assessment of the investment's ability to accomplish its goals. Chart 19-4 summarizes the CIO risk ratings for all major civilian IT investments Government-wide. The IT Dashboard shows slight decreases in the general health of IT investments across Government, as denoted by the decreased proportion of CIO-rated "Green" ("Low Risk" to "Moderately Low Risk") investments. "Green" investments comprised 41 percent of all rated investments in 2019 compared to 58 percent in 2018 (assessments based on total life cycle of investments).

IT Modernization

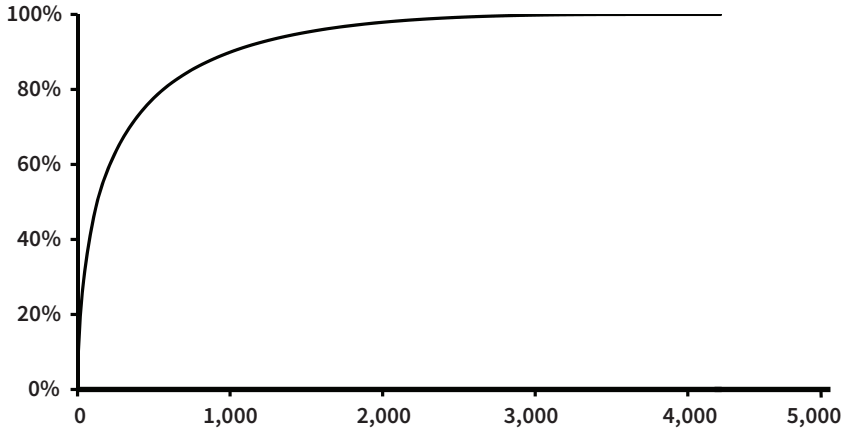
Due to the complexity of the IT landscape, agencies are often inefficient in acquiring, developing, and managing Federal IT investments. This is largely due to both legacy and homegrown, non-standards based systems designed to perform only one function rather than leveraging new commercial off the shelf technologies that allow efficient use of resources. These systems are costly for the federal Government to maintain and secure.

Chart 19-2. 2020 Federal Civilian IT Investment Portfolio Summary



This analysis excludes the Department of Defense

Chart 19-3. Percentage of 2020 Federal Civilian IT Spending by Number of Investments



This analysis excludes the Department of Defense

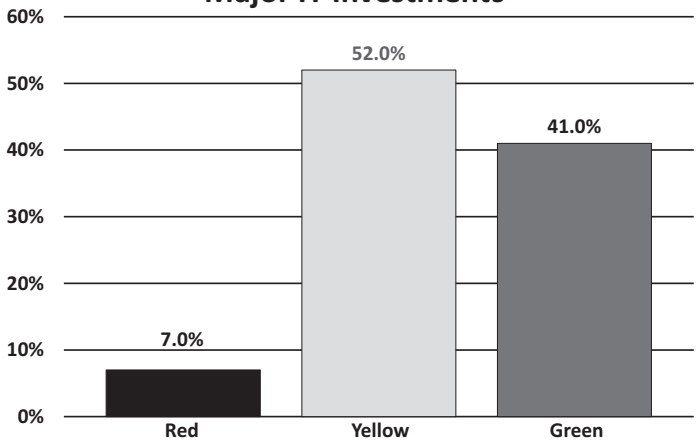
The *Report to the President on IT Modernization*[4] outlined 52 tasks, all of which were completed by December 2018. The outcomes from these activities informed the priorities and next steps included in the IT Modernization CAP Goal, which features a three pronged approach that focuses on enhancing federal IT and digital services, reducing cybersecurity risks to the federal mission, and by building a modern IT and cybersecurity workforce. Federal agencies are increasing efforts to modernize their IT in a way that 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. Though a substantial amount of work is still required, below are several specific detailed efforts of the Administration's IT modernization strategy.

OMB continues to support the adoption and evolution of the Federal IT Acquisition Reform Act (FITARA)[5] to provide agency CIOs with the authority, accountability, and support to deliver IT services across their agency enterprise. OMB continues to work with the Congress and the Government Accountability Office to improve the FITARA Scorecard to ensure consistent, effective metrics-based evaluation of agency progress and outcomes. Through the Chief Information Officers Council (CIO Council), OMB and agency CIOs will direct discreet projects, coordination efforts, and problem solving to unleash the effectiveness of CIOs.

[4] See *https://itmodernization.cio.gov/*.

[5] National Defense Authorization Act for Fiscal Year 2015, Title VIII, Subtitle D, H.R. 3979.

Chart 19-4. CIO Risk Ratings for Federal Civilian Major IT Investments



Technology Modernization Fund

The Technology Modernization Fund (TMF) is an innovative funding vehicle that gives agencies additional ways to deliver services to the American public more quickly, better secure sensitive systems and data, and use taxpayer dollars more efficiently.[6] The mission of the TMF is to enable agencies to reimagine and transform 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 to and compete for TMF funds. Effective evaluation, selection, and monitoring of approved projects by the TMF Board will provide strong incentives for agencies to develop comprehensive, high quality modernization plans. Funds will be distributed in an incremental manner, tied to milestones and objectives. Agencies that receive funds from the TMF will work with the General Services Administration (GSA) and the Office of Management and Budget (OMB) to ensure that projects make maximum use of commercial products and services in their planning and execution and have a high likelihood of success.

To date, the TMF has received nearly 50 proposals totaling over $500 million in requested funding. Of the $100 million appropriated to the TMF in its first year of operation, the Board has funded seven projects totaling almost $90 million, and continues to review additional projects in the pipeline. TMF funds will be repaid over a period not to exceed five years, aided through cost savings and avoidance, subject to a written agreement and the availability of out-year agency appropriations. In addition, incremental funds transfers will be tied to successful delivery of products. Successful projects will operate as proofs of concept and will provide valuable insights to the Board, which may recommend prioritizing the selection of more comprehensive modernization projects that can serve the interests of the Executive Branch as a whole. This Budget requests additional TMF funding to meet the demand generated by agencies and to invest strategically in modernizing agency systems through commercial solutions and improving the adoption and delivery of shared services.

Cloud Adoption

Keeping up with the fast paced innovation is critical to staying in front of the needs of Americans. Agency adaption of cloud solutions is essential to keep up with technology, but too few Federal agencies are able to move their services quickly to take advantage of the cloud. In 2018, the Administration released a draft version of its Cloud Smart document for public comment, which focuses on equipping agencies with the tools needed to make informed technology decisions in accordance with their mission needs, and leverages private sector solutions to provide the best services to the American people. As part of this strategy, OMB has also posted a draft memorandum for public comment which establishes a new Data Center Optimization Initiative (DCOI), focusing on achievable closure of data centers, areas for cost savings, and the reduction of agency reporting burden. The PMA also includes a focus on the adoption of cloud email services which are more secure and efficient than legacy on-premise solutions, setting a target of 95 percent of civilian email inboxes being hosted by cloud email services. The Federal Government has made significant improvements in this effort, where as of November 2018, 66 percent of email inboxes at Federal civilian CFO Act agencies are now hosted on cloud services, a 23 percent improvement from December 2017 (46 percent).

The Administration is also making significant efforts to reduce technical and process barriers to adopting cloud. In FY 2018, DHS and OMB conducted multiple pilots using commercial, off-the-shelf cloud technology to test alternative architectures that provide the cybersecurity controls required by the Trusted Internet Connection (TIC) program. OMB has released a draft version of the TIC policy update for public comment, which will enable agencies to utilize these alternative architectures and revolutionize the way agencies access the internet securely by removing barriers to cloud adoption. OMB and GSA are evaluating the best mechanisms for normalizing Federal security requirements for the Authority to Operate (ATO) process run by the Federal Risk and Authorization Management Program (FedRAMP), so that approval of cloud providers can be more readily reused. This evolution aims to make the program a more rapid, efficient, and effective in order to securely deploy commercial cloud technology.

Improving the IT & Cybersecurity Workforce

Maintaining and securing Federal IT requires a large, well-educated IT workforce. However, current Federal hiring practices are not in line with the needs to acquire the best talent industry has to offer. The Government needs more nimble and effective approaches to keep technologies and workforce skills current and to ensure that the Federal workforce can meet future needs. The FY 2020 President's Budget outlines a vision for change that would streamline the hiring and dismissal processes, modernize human resources technology, better utilize data to inform workforce management, rebalance labor-management relations, align Federal workforce management authorities with private sector best practices, and reduce unnecessary red tape to bring the Federal workforce into the 21st Century.

In addition to efforts to revamp hiring processes, OMB also looks to leverage the dedicated workforce already employed within Federal agencies. OMB along with the Department of Education, and the CIO Council announced the launch of the Federal Cybersecurity Reskilling Academy (FCRA) pilot program, an exciting new opportunity for federal employees to advance their careers and develop new skills in the fast growing field of cybersecurity.[7] This Academy is designed to give federal employees, who have no prior experience working in IT, hands-on training to become qualified Cyber Defense Analysts. The Academy received over 1,500 applicants for its initial pilot class of 25. OMB also continues to look for new and innovative ways to leverage top talent in the

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

[7] See *https://www.cio.gov/reskilling*.

private sector. Strategies include incentivizing cybersecurity talent to rotate into government to work on high priority IT and cybersecurity initiatives, encouraging improved disclosure and information sharing from security researchers, and developing more inclusive fora to bring best practices and new solutions to Federal technology and cybersecurity leaders.

This year, in celebration of Women's History Month, the Federal Government hosted a Women in Federal Information Technology and Cybersecurity event, bringing together the nation's top Federal information technology executives to celebrate the successes of women in Federal IT and to discuss strategies that engage, inspire, and motivate more women to pursue a career in IT.

Reduce Cybersecurity Risks to the Federal Mission

Strengthening the cybersecurity of Federal networks, systems, and data is one of the most important challenges we face as a nation. Risk management assessments carried out under the President's Executive Order 13800[8], *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, demonstrated that the majority of Federal agencies could not appropriately manage their cybersecurity risk. These assessments found enterprise-wide gaps in network visibility, IT tool standardization, and common operating procedures, all of which negatively affect Federal cybersecurity and put our nation at risk. Bold approaches are needed to improve Federal-wide governance processes and implement cybersecurity capabilities "commensurate with risk and magnitude of the harm"[9] that a compromise of Federal information systems and information would entail. As part of the larger effort to utilize modern solutions to drive more effective and efficient IT, the Federal Government will move to better utilize threat information in its decision-making processes, implement improved baseline security capabilities, and enhance accountability for the management of information security risks.

To protect privacy, prevent fraud, and mitigate high impact data breaches of Personally Identifiable Information (PII), the Federal Government is working to implement modern digital identity management processes, technologies, and remediation techniques. In FY 2018, OMB collected input on a draft Federal identity policy, receiving feedback from over 500 individuals and organizations and is currently incorporating the public's feedback.

The Continuous Diagnostics and Mitigation (CDM) Program is a dynamic approach to fortifying the cybersecurity of Government networks and systems. The CDM Program provides DHS, along with Federal Agencies, with capabilities and tools to identify cybersecurity risks on an ongoing basis, prioritize these risks based on potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. Congress established the CDM program to provide adequate, risk-based, and cost-effective cybersecurity and more efficiently allocate cybersecurity resources. This year, OMB issued M-19-02, which empowers agencies to use existing tools and capabilities acquired outside of CDM acquisition vehicles, provided the agency meets all CDM reporting requirements to the Federal Dashboard.

For more information on the Cybersecurity funding of Federal agencies, please see Chapter 24.

United States Digital Service

Americans expect and deserve their interactions with the Federal Government to be simple, fast, and helpful. The United States Digital Service (USDS) is among those leading the charge to enhance 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, leading to cost savings and a more efficient Federal workforce. Because of that, congressional investments in USDS have led to both better outcomes for the public and significant budget savings for agencies.

To successfully modernize technical systems, USDS developed an entirely new approach through the Digital Services Playbook.[10] In the past, the government has developed products without paying adequate attention to how the American people interact with those products. USDSworks with the people digitally interacting with the Federal Government e—such as farmers, service members, or doctors—to ensure that its tools and processes are meeting their needs. For instance, USDS partnered with the Department of Veterans Affairs (VA) to develop the new VA.gov, which digitizes the top 80% of tools veterans need and places it in one easy to access and understand location. USDS has dozens of similar projects underway across the Federal Government that not only help update and modernize legacy systems, but also change the culture of how the government delivers technical products.

USDS is also introducing modern best practices that can be replicated across the government. For instance, USDS is aggressively helping the VA and Centers for Medicare and Medicaid Services (CMS) migrate to the cloud. In addition, both of these agencies are at the forefront of leveraging industry standard technology known as application programming interfaces (APIs) that allow software to interact with other software. Through the Blue Button 2.0 initiative, CMS developed APIs that make it easy for Medicare recipients to manage their own health information and share it with doctors, caregivers, and others.

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

[9] FISMA requires agencies to implement information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of "information collected or maintained by or on behalf of [an] agency" and "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency". 44 U.S.C. § 3554.

[10] See *https://playbook.cio.gov/*.

Importantly, USDS is helping drive the adoption and implementation of information security best practices. In a combined project with GSA, USDS launched Login.gov, which makes managing Federal benefits, services, and applications easier and more secure through the use of modern identity management solutions such as two-factor authentication. Since its launch, Login.gov has scaled to over 12 million users and it continues to grow rapidly as additional government agencies adopt it. Likewise, the USDS team at the Department of Defense (DOD) has successfully scaled the use of bug bounty and vulnerability disclosure programs that are commonplace at nearly all major technology companies. Bug bounty programs leverage private security researchers to identify and exploit system vulnerabilities in an approved environment, paying a bounty for each vulnerability identified. Bug bounties yield more prolific results than traditional approaches at a better price point, delivering both value and improved security. The DOD also pioneered a Vulnerability Disclosure Policy (VDP) that allows a pathway for anyone to report a security vulnerability to the department. At the time of this accountingt, more than 5,000 vulnerabilities have been discovered and reported. Other agencies including the Departments of Homeland Security, State, and CMS are pursuing their own VDPs and bug bounty programs, leveraging the knowledge and expertise that USDS pioneered within government.

In addition to enhancing technology solutions and integrating private sector best practices, USDS has also worked to improve Federal IT procurement practices. Traditional procurement practices often do not provide the flexibility required to buy and deliver modern digital services. Meanwhile, the pace of technological change continues to accelerate while citizen demand for Federal digital services increases. To meet this demand, the Office of Federal Procurement Policy (OFPP) and USDS developed the Digital IT Acquisition Professional Program (DITAP) training program to enhance digital service acquisition expertise across government agencies. Graduates of the training receive the Federal Acquisition Certification in Contracting Core-Plus Specialization in Digital Services (FAC-C-DS). By July 2019, 194 people will have graduated from the program. OFPP and USDS are working with Federal training institutions and training companies to scale this program to the rest of the government.