

16. INFORMATION TECHNOLOGY

Every day, millions of people interact with the Federal Government. Americans expect and deserve these experiences to be simple, fast, and helpful. The President proposes to spend nearly \$95.7 billion for Information Technology to help make this expectation a reality. With this amount, Departments and agencies will continue ongoing work to significantly accelerate development and implementation of modern digital services and technology throughout the Federal Government.

FEDERAL INFORMATION TECHNOLOGY TODAY

Federal Spending on IT

Table 16-1. FEDERAL IT SPENDING
(In millions of dollars)

	2016	2017	2018
Department of Defense	38,061	40,844	42,521
Non-Defense	52,219	53,250	53,168
Total	90,280	94,094	95,688

Note: Defense IT spending includes estimates for IT investments for which details are classified and not reflected on the IT Dashboard. All spending estimates reflect data available as of May 8, 2017.

As shown in Table 16-1, the Federal Government Budget for IT is estimated to be \$95.7 billion in FY 2018, an increase

of 1.7 percent from FY 2017.¹ This figure is based on data collected on 4,087 civilian IT investments at major Federal agencies through the Capital Planning and Investment Control (CPIC) process. Excluded from this total dollar figure are small and independent agencies, national security systems, and all classified spending. The Department of Defense accounts for 44.4 percent of Federal IT spending.

There is significant variation in spending on IT among Executive branch Departments and agencies, as shown in Table 16-2, which displays IT spending by agency. The Department of Health and Human Services is the largest civilian agency by IT spending, while the bottom sixteen agencies only spend 10.7 percent.

IT Investments Overview

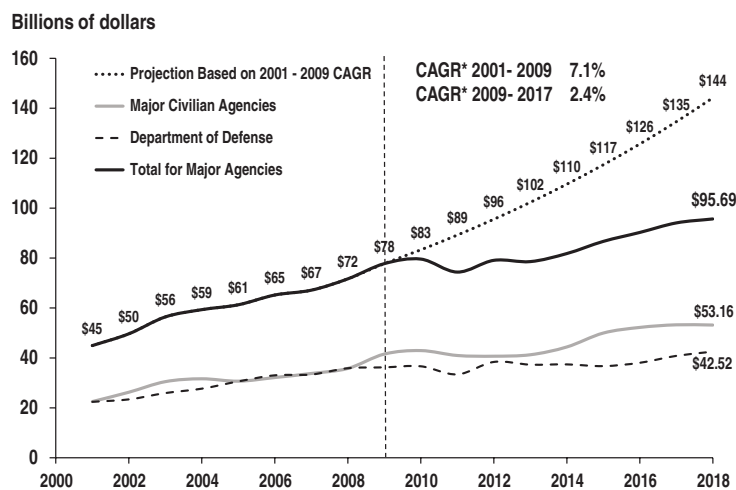
The FY 2018 President's Budget includes funding for 4,087 IT investments.² These investments support four main functions: mission delivery; administrative services and support systems; IT infrastructure, IT security, and IT management; and grants and other transferred funding to non-Federal organizations for IT (see Chart 16-2). As Chart 16-3 shows, IT investments can vary widely in size and scope. As a result, the largest 100 IT investments account for 57 percent of Federal IT spending.³

¹Based on agencies represented on the IT Dashboard, located at <http://itdashboard.gov>.

² This figure excludes the Department of Defense.

³ This does not include the Department of State, Nuclear Regulatory Commission, Department of Commerce, and the Department of Defense.

Chart 16-1. Trends in Federal IT Spending



*Compound Annual Growth Rate.

Source: Total IT spending for agencies reporting to the IT Dashboard. Department of Defense has provided estimates for classified IT investments not shown on the IT Dashboard. Chart reflects data available as of May 9, 2017.

Table 16-2. FY 2018 IT SPENDING BY AGENCY
(In Millions of dollars)

Agency	2018	Percent of Total
Department of Defense*	42,521	44.4%
Department of Health and Human Services	13,833	14.5%
Department of Homeland Security	6,833	7.1%
Department of the Treasury	4,259	4.5%
Department of Veterans Affairs	4,151	4.3%
Department of Transportation	3,425	3.6%
Department of Agriculture	2,958	3.1%
Department of Justice	2,852	3.0%
Department of Commerce	2,560	2.7%
Department of Energy	2,023	2.1%
Department of State	1,864	1.9%
Social Security Administration	1,651	1.7%
National Aeronautics and Space Administration	1,549	1.6%
Department of the Interior	1,185	1.2%
Department of Education	745	0.8%
Department of Labor	703	0.7%
General Services Administration	691	0.7%
U.S. Army Corps of Engineers	451	0.5%
Department of Housing and Urban Development	351	0.4%
Environmental Protection Agency	328	0.3%
Nuclear Regulatory Commission	159	0.2%
United States Agency for International Development	141	0.1%
Office of Personnel Management	141	0.1%
National Science Foundation	115	0.1%
National Archives and Records Administration	101	0.1%
Small Business Administration	100	0.1%
Total	95,688.00	100.0%

*Represents the total (unclassified and classified) topline estimates as of May 8, 2017.

Of the 4,087 IT investments within civilian agencies, 758 are major IT investments. IT investments are determined to be major if 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. Agencies are required to submit Business Cases for all major IT investments, which provide additional transparency into the cost, schedule, 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 public 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 16-4 displays the latest CIO risk ratings for all major IT investments government-wide.

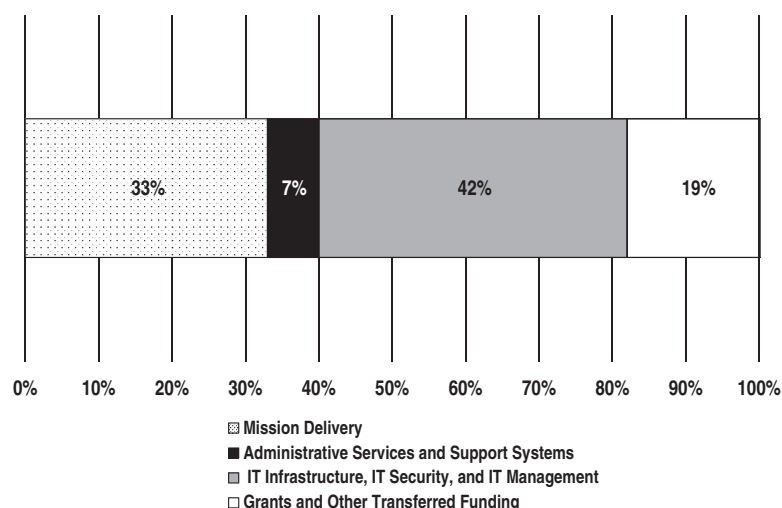
The IT Dashboard shows slight decreases in the general health of IT investments across government, as denoted by the increased proportion of CIO-rated "Green" investments on the IT Dashboard, which comprised 63 percent of all rated investments in March 2017 compared to 69 percent in 2012 (assessments based on total life cycle of investments).

Legacy IT Spending

Federal IT spending is categorized as either Operations & Maintenance (O&M) or Development, Modernization, and Enhancement (DME). Of the \$48.5 billion reported to the IT Dashboard, 78.5 percent (\$38.1 billion) is O&M spending.⁴ Agencies are required to further break down the proportion of O&M spending not dedicated to provisioned services, such as cloud computing, as provisioned

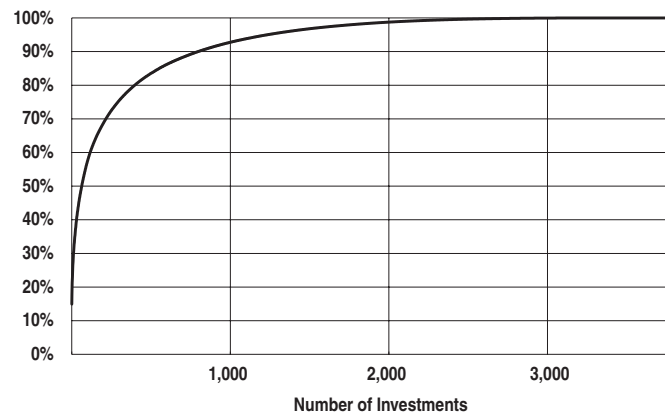
⁴ This does not include the Department of State, Nuclear Regulatory Commission, Department of Commerce, and the Department of Defense.

Chart 16-2. IT Portfolio Summary



Note: The following agencies submitted only topline estimates to OMB and were excluded from this analysis: Department of Defense, Department of Commerce, Department of State, and Nuclear Regulatory Commission.

Chart 16-3. Number of Investments by Percentage of IT Spending, 2018



Note: The following agencies submitted only topline estimates to OMB and were excluded from this analysis: Department of Defense, Department of Commerce, Department of State, and Nuclear Regulatory Commission.

services are encouraged by OMB policies. This area of spending is often referred to as “legacy” spending, given that it is dedicated to maintaining agencies’ existing physical IT investments. From FY 2015 through FY 2018, government-wide legacy spending as a percentage of total IT spending rose slightly from 68 percent to 70.3 percent. Aging legacy systems may pose efficiency and mission risk issues, such as ever-rising costs to maintain and an inability to meet current or expected mission requirements. Legacy systems may also operate with known security vulnerabilities that are either technically difficult or prohibitively expensive to address and thus may hinder agencies’ ability to comply with critical statutory and policy cybersecurity requirements.

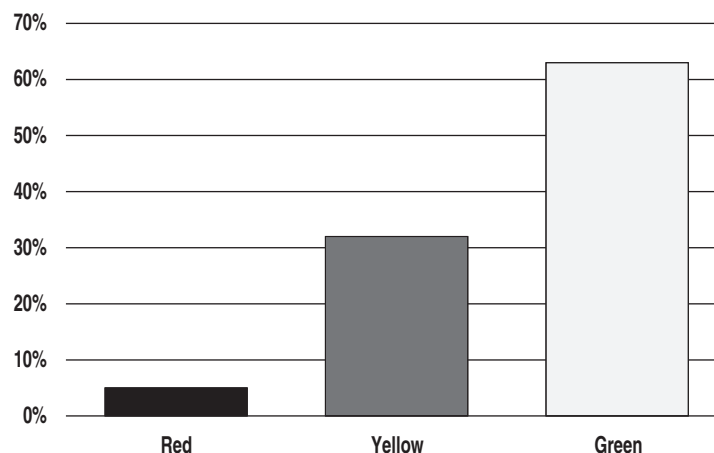
Chart 16-5 displays the percent of the government-wide IT funding going toward new capabilities (referred

to as non-provisioned Development, Modernization and Enhancement or DME), O&M, and provisioned services.

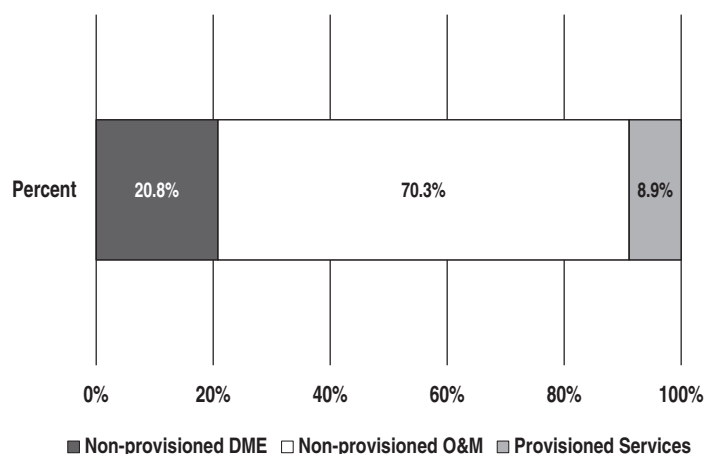
MODERNIZING GOVERNMENT TECHNOLOGY

The Administration will work to modernize and improve government operations and service delivery by building modern citizen-facing digital services, buying more like a business, improving cybersecurity, investing in improved data analytics, and generating greater cost efficiencies. Modernization, in this sense, is not simply replacing individual outdated IT systems with newer ones; rather, it is a holistic approach to Federal IT that fundamentally transforms how agencies accomplish their missions. This approach entails reengineering underlying business processes and leveraging modern IT solutions,

Chart 16-4. CIO Risk Ratings for Investments



Note: Only 686 of the 719 business cases had CIO ratings associated with them as of 03/01/2017. The remaining business cases were associated with security investments and did not necessarily need to report CIO Ratings. Furthermore, DOD is not represented in this time period.

Chart 16-5. IT Spending by Category

Note: The following agencies submitted only topline estimates to OMB and were excluded from this analysis: Department of Defense, Department of Commerce, Department of State, and Nuclear Regulatory Commission.

such as cloud and shared services that drive efficiency and scale to address common business challenges across the Federal Government.

Modern Citizen-Facing Services

Americans expect and deserve their interactions with the Federal Government to be simple, fast, and helpful. The FY 2018 President's Budget provides funding for Federal civilian agencies to spend on IT focused primarily on providing services to the American public, including systems that will ensure veterans can easily access the benefits and services they have earned, students can receive financial aid, and small business owners can access affordable financing to start or expand their businesses.

The Administration will leverage the country's best private sector ideas, services, and vendors to deliver these projects efficiently and effectively. In addition, the Administration will accelerate efforts to recruit some of the country's top technical talent to modernize key services via programs such as the U.S. Digital Service (USDS).

Buying as a Business

The Federal Government is the world's largest buyer, yet does not adequately leverage its buying power or price information. Significant contract duplication means that agencies award multiple contracts for similar goods and services, and experience significant price variance for the exact same item. At the same time, acquisition processes remain slow and complicated, reflecting strategies that were designed more than a half-century ago for a paper-based world and fail to leverage modern private sector practices.

In FY 2018, the Administration will drive adoption of Category Management practices, which enable Federal agencies to buy targeted categories of products and services as a single enterprise using Best in Class solutions. Close to 70 percent of FY 2016 spending for laptop and desktop computers utilized these solutions, which re-

duced the number of standalone contracts by 5 percent. In addition, 47 percent of spending in this area went to small businesses, higher than the government-wide goal of 23 percent. In FY 2018, the Administration will continue to drive spending through approved vehicles, reduce the number of contracts, and meet small business goals.

Additional opportunities exist to modernize IT and human capital used in shared administrative processes. The Federal Government can modernize and share IT and services for common administrative functions by: (1) adopting government-wide standards; (2) using the standards to reduce contract duplication for IT and professional services; and (3) replacing legacy systems with modern solutions and services.

Implementation of these strategies has the potential to drive numerous benefits, including generating cost savings, increasing the Federal Government's ability to rapidly deploy best-in-class industry solutions, and enhancing cybersecurity.

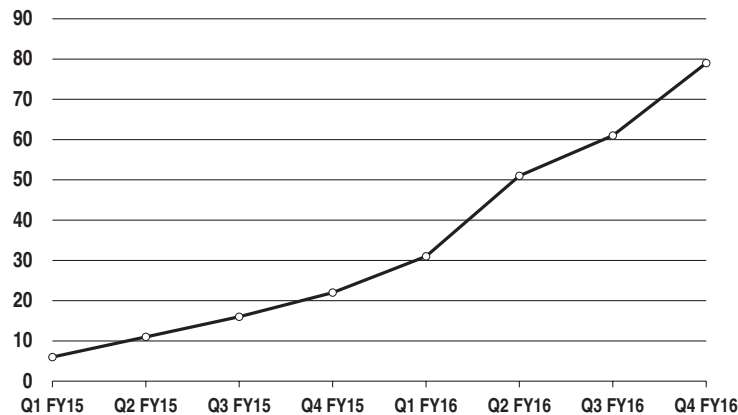
Cybersecurity

Strengthening the cybersecurity of Federal networks, systems, and data is one of the most important challenges we face as a nation. For the first time, this Budget includes discrete cyber program investments that align budget resources with the National Institute of Standards and Technology (NIST) Cybersecurity Framework. This will enable the alignment of budget, risk, and performance data in a consistent way across all Federal agencies.

Cybersecurity Risk and National Institute of Standards and Technology (NIST) Framework

The FY 2018 President's Budget recognizes the increasing interconnectedness of Federal information and information systems and provides resources for agency heads to manage the cybersecurity risk across their enterprise to ensure these risks do not impact the Federal Government as a whole. In particular, agency heads are required to manage risk commensurate with the magni-

Chart 16-6. Digital Projects in Production to Which Digital Experts have Contributed



tude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems.

An effective enterprise risk management program promotes a common language to recognize and describe potential risks that can impact the agencies' missions and services to the public, including cybersecurity risk. The Federal Government leverages the NIST Cybersecurity Framework, which provides a standard for managing and reducing cybersecurity risks, and organizes capabilities around the five function areas: Identify, Protect, Detect, Respond, and Recover.

Accordingly, OMB and DHS continue to work with CIOs and Inspectors General (IG) across the Federal Government to align Federal Information Security Management Act (FISMA) metrics to the Framework. OMB also worked with agencies to align the FY 2018 Information Technology Capital Planning and Investment Control (CPIC) Guidance with the Framework to provide agencies with a tool to budget for cybersecurity capabilities that effectively manage risk. Comprehensive adoption of the NIST Framework will provide agencies with a common view and understanding of cybersecurity risk with other agencies, suppliers and vendors, and broader industry. This shared language around cybersecurity risk can lead to more sharing of best practices, common language for requirements and capabilities, and more joint efforts between public and private sectors to improve cybersecurity risk.

Continuous Diagnostics and Mitigation (CDM)

Additionally, the FY 2018 President's Budget continues to invest in the CDM Program. This program, managed by DHS and implemented across Federal agencies, is intended to create a common baseline of cybersecurity capability and protection across the Federal Government. The program provides Federal Departments and agencies with CDM-certified capabilities and tools that identify and prioritize cybersecurity risks on an ongoing basis and enable cybersecurity personnel to mitigate the most significant problems first. CDM tools also allow departments

and agencies to better manage their IT assets, helping to reduce the risk to agencies' perimeters while providing near real-time awareness of agency networks and environments that can be aggregated into one enterprise-level dashboard.

Improving Data Analytics and IT Portfolio Management

Good decision-making requires useful data. Consistent, mission-oriented metrics create meaningful data for agencies to evaluate and enhance their performance. On the other hand, inconsistent metrics, unclear definitions, or metrics that do not align to agencies' missions create a compliance culture that ultimately inhibits performance. Currently, many reporting requirements are viewed as mere compliance exercises that are not consistently used to improve IT management and oversight. Thus, in FY 2018, the Administration will drive transformation of the Capital Planning and Investment Control (CPIC) process. This effort will increase the strategic value of IT and empower CIOs to better support agency missions through more effective IT management. The CPIC process is being redesigned as a strategic tool for agencies to implement the requirements set forth in the Federal Information Technology Acquisition Reform Act (FITARA).

To better utilize Federal IT spending data, the Federal Government must integrate data collection efforts, standardize reporting data, and find new opportunities to simplify, automate, and consolidate reporting. Such efforts can build on existing Federal initiatives such as the Digital Accountability and Transparency (DATA) Act of 2014 (Public Law 113–101), which improves government-wide financial reporting and data standards. Moreover, the Federal adoption of industry standards for tracking IT spending will improve the consistency, granularity, and quality of Federal IT spending information and thus drive more meaningful analysis, benchmarking, and planning.

Improving data quality and usability is the first step towards a more data-driven, responsive, and accountable Government.

Facilitating Modernization Efforts

Federal agencies have a poor track record of appropriately planning and budgeting for continuous modernization of their legacy IT systems. Further, transition to provisioned services, such as cloud and shared services, remains slow. The lack of proactive adoption of cloud and shared services has resulted in agencies accumulating billions of dollars in technical debt. To improve the traditional budget process, the FY 2018 President's Budget requires agencies to identify and budget for the modernization of specific high-risk legacy IT systems, with a particular focus on transitioning these systems to cloud and shared services.

Technology Modernization Fund

Beyond improvements to the traditional budget process, the FY 2018 President's Budget proposes placing a portion of the Federal Government's \$95.7 billion in annual IT spending into a central Technology Modernization Fund designed to improve the management and oversight of Federal IT modernization projects. The Technology Modernization Fund will be dedicated to transitioning Federal agencies from IT infrastructure, systems, and services that are not cost-effective or secure to more efficient and secure technologies.

The Technology Modernization Fund will improve the success of the Federal Government's efforts to modernize its IT portfolio in multiple ways:

- First, an independent board of experts will evaluate agency proposals to ensure the Federal Government's most inefficient, ineffective, and highest-risk systems are targeted for modernization.
- Second, a repayment requirement will ensure the Technology Modernization Fund is self-sustaining and can continue to support modernization projects well beyond the initial infusion of capital.
- Third, experts in IT acquisition and development will provide integrated modernization expertise to

agencies in implementing their modernization plans. Every project will benefit from centralized oversight and expertise, increasing the probability of success.

- Fourth, funding for all projects will be tied to real-world delivery of products. This approach ensures that agencies employ agile development techniques and prevents sunk costs.

Finally, by establishing a central fund that agencies must apply to and compete for, the Technology Modernization Fund will provide strong incentives for agencies to develop comprehensive, high quality modernization plans.

Cloud Adoption/Email Migration

Email and collaboration tools are essential to the day-to-day operations of Federal agencies; yet too few Federal agencies have basic collaboration tools such as real-time document sharing or video conferencing. In many cases, the tools being used by agencies are more than a decade old and run on legacy systems with growing maintenance costs. This situation is a hidden tax on productivity: it wastes time, creates missed opportunities, and slows coordination and creativity.

The majority of agencies who moved to cloud-based collaboration solutions experienced cost savings after just a few years of investment. These cost savings ranged from \$500,000 per year for smaller agencies to \$10 million per year for a larger agency such as the Department of Justice. For example, the National Oceanic and Atmospheric Administration (NOAA) was able to migrate to cloud-based email within six months and decommission its legacy servers over the next two years to achieve a total of \$3.1 million dollars of cost savings per year.

Migrating the remaining Federal agencies from agency owned-and-operated email systems to cloud-based email will result in significant cost savings, improved security, and greater productivity.