

17. INFORMATION TECHNOLOGY

The Administration continues its commitment to building a 21st century Government that is more efficient and effective for the American people. The Budget supports the President's Management Agenda, a comprehensive and forward-looking plan to deliver better, faster, and smarter services to citizens and businesses; increase quality and value in the Government's core administrative functions and continue efforts underway to enhance productivity to achieve cost savings across the Government; open Government-funded data and research to the public to spur innovation and economic growth; and unlock the full potential of today's Federal workforce and build the workforce we need for tomorrow. Delivering smarter information technology (IT) services is critical to achieving the Administration's management goals, and requires a strong emphasis on meeting user needs and delivering on intended impact. The Federal Government for 2015 plans to invest \$79 billion in IT, sustaining efforts on cost savings and effective oversight. To ensure that this investment in IT serves American taxpayers well, the Administration has refined policies and oversight activities to address three key areas: delivering value in Federal IT investments; driving innovation to meet customer needs; and securing and protecting the Government's data.

This chapter describes the Federal IT budget and the Administration's Federal IT initiatives.

DELIVERING VALUE IN FEDERAL IT INVESTMENTS

Federal Spending on IT—For Federal programs to succeed it is critical that agencies view IT as a strategic asset, one that should be harnessed to increase efficiency and effectiveness in program performance and maximize customer service not only for agency users across the Government, but also for non-Federal users of Government information, such as States, localities, businesses, and individuals. Federal IT management policies have recently required agencies to modernize and streamline their IT investments, with a view to delivering on IT management goals of efficiency, effectiveness, customer service, and security. Through policy and oversight, this Administration has rationalized IT spending across the most important national priorities to increase efficiency, arresting the growth in IT spending witnessed prior to 2009, and delivering better value from IT to American taxpayers.

Total planned spending on IT for the FY 2015 Budget is estimated¹ to be \$79.0 billion, 2.9 percent below the 2014

¹ Based on agencies represented on the IT Dashboard, located at: <http://itdashboard.gov>. Agencies for which IT investment information is displayed on the IT Dashboard are: Department of Agriculture, Department of Commerce, Department of Defense, Department of Educa-

tion, Department of Energy, Department of Health and Human Services, Department of Homeland Security, Department of Housing and Urban Development, Department of the Interior, Department of Justice, Department of Labor, Department of State, Department of Transportation, Department of the Treasury, Department of Veterans Affairs, Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Archives and Records Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Smithsonian Institution, Social Security Administration, U.S. Agency for International Development, and U.S. Army Corps of Engineers.

estimated level of \$81.4 billion, as shown in Table 17-1. Spending estimates in Chart 17-1 depict how growth in IT spending of 7.10 percent per year over 2001-2009 has been slowed to 0.27 percent per year for 2009-2015. (This time series has been revised back to 2001, based on a revision of estimates for the Department of Defense.)

As the graph of spending over 2001-2015 shows, the basic trends reported in the past have persisted, despite the recent years showing significantly lower levels for both Defense and non-Defense. The lower spending levels in recent years are due to a number of factors, which may include the lower overall Federal budget levels for discretionary spending, as well as the achievement of improved efficiency in how funds are invested in IT.

Table 17-1. FEDERAL IT SPENDING
(Millions of dollars)

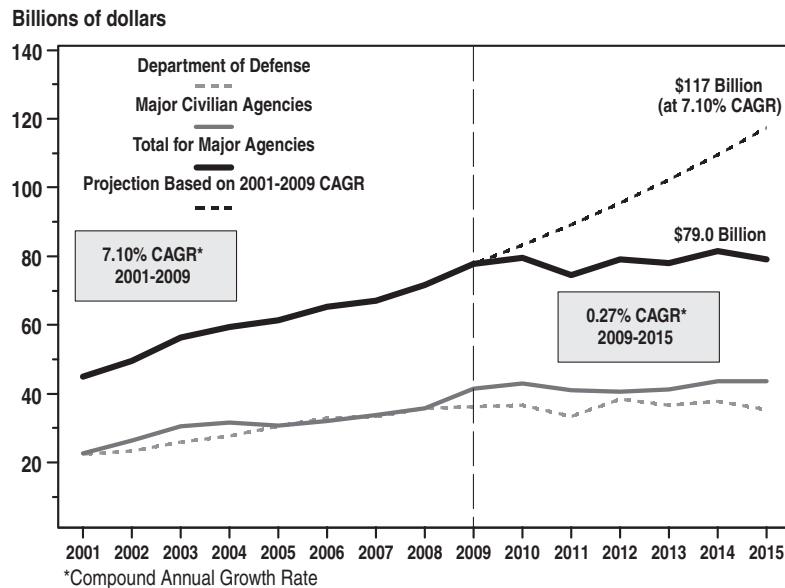
	2013	2014	2015
Department of Defense	36,624	37,644	35,370
Non-Defense	41,273	43,754	43,655
Total	77,897	81,398	79,025

Note: Defense IT spending includes estimates for IT investments for which details are classified, and not reflected on the IT Dashboard. DoD estimates shown for 2013-2015 also reflect improved internal accounting. Historical data in Chart 17-1 have been adjusted for DoD, to reflect the agency's judgment that previously reported 2001-2012 data should be adjusted down by 3 percent annually, to account for past overstatements in amounts for the Defense Working Capital Fund. All spending estimates reflect data available as of Feb. 26, 2014.

Focusing Agency IT Oversight on Comprehensive IT Portfolio Reviews—Information technology is essential to everything the Government does. The approximately \$80 billion we invest each year in Federal IT helps airplanes land safely, small businesses secure loans, and retirees receive their Social Security benefits. As with any investment, we must ensure we get the maximum return on the Government's investment. In 2014-2015, the Administration will build on its approach strategically manage Federal IT by implementing a more rigorous application of its PortfolioStat model, which employs data-driven reviews of agency IT portfolios led by the Office of Management and Budget (OMB).

tion, Department of Energy, Department of Health and Human Services, Department of Homeland Security, Department of Housing and Urban Development, Department of the Interior, Department of Justice, Department of Labor, Department of State, Department of Transportation, Department of the Treasury, Department of Veterans Affairs, Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Archives and Records Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Smithsonian Institution, Social Security Administration, U.S. Agency for International Development, and U.S. Army Corps of Engineers.

Chart 17-1. Trends in Federal IT Spending



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. Data for 2001-2012 for DOD reflect the agency's current determination that estimates should be adjusted down by 3 percent for past overstatements of Defense Working Capital Fund amounts. Chart reflects data available as of Feb. 26, 2014.

PortfolioStat assessments in 2012 and 2013 required agencies to collect and analyze baseline data on 13 common types of commodity IT investments, including infrastructure, business systems, and enterprise IT. OMB worked with agencies to review this data and compare spending levels with other agencies and private-sector benchmarks. This analysis resulted in the development of a list of opportunities to reduce inefficiencies, duplication, and unnecessary spending, and to reinvest those funds in the modernization of obsolete legacy systems. Since 2012, PortfolioStat reviews have helped agencies realize savings through strategic sourcing, the optimization of data centers, the consolidation of multiple email systems, the migration of services to cloud platforms, and the reduction of duplicative mobile device and desktop contracts. Agencies regularly report on these savings, which are summarized in OMB's quarterly reports to Congress and address the cost savings achieved by the Administration's reform initiatives. Recently, agencies have been able to report cumulative savings stemming from PortfolioStat of approximately \$1.6 billion -- nearly 2/3 of the total potential savings identified through the initial PortfolioStat sessions conducted in 2012². Examples of savings³ reported by agencies include:

- Federal Aviation Administration (FAA) Procurement Consolidation: \$20 million.
- Department of Veterans Affairs Renegotiated Enterprise Licenses: \$50 million.
- Department of Commerce (DOC) Data Center Consolidation: \$21 million.

In addition, the FY 2013 PortfolioStat reviews also identified improvement opportunities in the areas of IT governance, transparency, program management, and IT talent management. These efforts range from ensuring higher visibility of major IT investments monitored on the Federal IT Dashboard, sourcing of qualified hires to fill critical IT skill gaps, and increasing the use of modular development and delivery approaches.

Strategic Sourcing of Commodity IT—OMB will continue to work with the Strategic Sourcing Leadership Council to drive greater efficiencies in the acquisition of commodity IT. Through the PortfolioStat process, OMB will continue to work with agencies to improve agency IT procurement processes, and find lower prices on specific commodities that agency IT managers buy. Actions to secure better value for each IT dollar spent will include:

- Reducing mobile device costs by comparing prices paid by agencies against the Federal Strategic Sourcing Initiative (FSSI)'s government-wide Wireless program prices⁴.

² The potential savings identified by agencies in the initial round of agency PortfolioStat sessions was \$2.5 billion.

³ Savings can be recognized in two different ways, as defined in OMB Circular A-131: (a) Cost-Savings: A reduction in actual expenditures below the projected level of costs to achieve a specific objective; and, (b) Cost-Avoidance: An action taken in the immediate timeframe that will decrease costs in the future. For example, an engineering improvement that increases the mean time between failures and thereby decreases operation and maintenance costs is a cost-avoidance action.

⁴ For the FSSI's Wireless program, see: <http://www.gsa.gov/portal/category/100931>.

- Synchronizing the acquisition of desktops across agencies to ensure purchases at the lowest possible price.
- Rationalizing the licensing of software so that the Government is paying only for solutions it is utilizing and is acquiring that software at bulk purchase rates.
- Moving agencies from the acquisition of system-specific hardware in support of IT investments to service based solutions; for example, moving optimized data centers that support many investments to FedRAMP⁵-certified cloud computing services.

Improved Transparency of IT Management Information—Under the direction of the Federal CIO, the funding provided through the Information Technology Oversight and Reform (ITOR) appropriation will continue to be used to support enhanced availability and visibility of IT management data. Improved data collection and analytics to better assess the Government's approximately \$80 billion investment in IT will build on information from the IT Dashboard, and PortfolioStat's integrated agency data collection process. In support of the Federal CIO and agencies, for use in PortfolioStats and other decision venues, funding will help identify underperforming and duplicative investments, and facilitate corrective actions. Funds will also support greater IT productivity through the optimization of Federal IT infrastructure investments and enhanced agency use of shared services.

Smarter IT Delivery—While the Government continues to put significant focus on efficiency gains, opportunities remain to refashion how we procure and implement technology in the Government. Accordingly, funding from ITOR will be used to incubate and scale new approaches to developing Federal digital services that provide a world-class customer experience to citizens and businesses. Additional strategies may include standards and policy to drive more effective citizen experience, improved tactics to measure customer satisfaction and performance of Federal digital services, and solutions to increase technology talent inside government.

A PLATFORM FOR INNOVATION - OPENING GOVERNMENT DATA

During a time of fiscal constraint and economic uncertainty, it is important to open access to Government data and to provide a platform for innovation that can improve opportunities and service quality for all Americans. By opening up taxpayer-financed assets such as data, and the policies and processes surrounding this data, we can empower individuals and businesses to significantly increase the public's return on this investment. Opening up Federally-housed data can spur innovation, scientific discovery, and job creation, enhancing growth and pub-

lic welfare across sectors of the economy, and improving public administration through improved information exchange and interaction with an involved public. The Administration's open data/innovation agenda builds on the following initiatives:

Open Data Policy and Initiatives—The information maintained by the Federal Government is a national asset with tremendous potential value to the public, entrepreneurs, and to our own Government programs. As a model, decades ago, the National Oceanic and Atmospheric Administration (NOAA) began making weather data available for free electronic download by anyone. Entrepreneurs utilized this data to create weather newscasts, websites, mobile applications, insurance, and much more, resulting in a multi-billion dollar industry. Similarly, the Government's decision to make the Global Positioning System (GPS) freely available resulted in private sector innovations ranging from navigation systems to precision crop farming, creating massive public benefits and contributing significantly to economic growth.

The Obama Administration is committed to responsibly unleashing data from the vaults of Government to fuel innovation that fuels economic growth while also advancing government efficiency and accountability. On May 9, 2013, President Obama signed an Executive Order⁶ and OMB issued a policy Memorandum⁷ making "open and machine-readable" the new default for Government information and taking other historic steps to make Government-held data more accessible to the public, entrepreneurs, and innovators while appropriately safeguarding sensitive information and rigorously protecting privacy. To build on this effort to make Government data more accessible, the Administration launched multiple initiatives aimed at scaling up open data efforts across the health, energy, education, financial, public safety, and global development sectors of the economy. These efforts aim to make Government data available to entrepreneurs. Previously, entrepreneurs have used this kind of data to create tools that help Americans find the right health care providers, identify colleges that provide the best value for tuition costs, make better decisions about retirement plans and financial advisors, help farmers around the world protect and improve their farming operations, save money on electricity bills, and keep their families safe by knowing which products have been recalled.

Delivering Mobile Services—During 2012 and 2013, Federal agencies worked to implement the Digital Government Strategy, built upon the proposition that all Americans should be able to access information from their Government anywhere, anytime, and on any device. Looking ahead, agencies will continue to increase the number of Federal services delivered via mobile devices. Such efforts will also improve interactions and

⁵ FedRAMP refers to the Federal Risk and Authorization Management Program, which provides Government agencies with a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. See: <http://www.fedramp.gov>.

⁶ Executive Order 13642 "Making Open and Machine Readable the New Default for Government Information": <https://www.federalregister.gov/articles/2013/05/14/2013-11533/making-open-and-machine-readable-the-new-default-for-government-information>.

⁷ OMB Memorandum M-13-13 "Open Data Policy-Managing Information as an Asset": <http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf>.

access to information within Government, empower the Federal workforce, enable the Government to reimagine service delivery by leveraging the power of citizens as co-creators. Examples of recently released mobile applications include:

- **America's Economy Application:** DOC's Census Bureau developed a mobile application called "America's Economy". This application provides real updates for 16 key economic indicators released from the Census Bureau, the Department of Labor's Bureau of Labor Statistics, and DOC's Bureau of Economic Analysis.
- **SaferCar:** The Department of Transportation's National Highway Traffic Safety Administration's (NHTSA) SaferCar application provides important information and functions that will help taxpayers make informed safety decisions involving vehicles, including information on recalls and complaints, 5-star safety ratings, and installing child seats.
- **Arlington National Cemetery Explorer Application:** The Department of Defense has created a mobile application to enable family members and the public to explore the Arlington National Cemetery's events, locate gravesites, or other points of interest.

Open Government Directive—Openness in Government strengthens our democracy and promotes a more efficient, effective, and accountable Government. In support of these principles, the Obama Administration launched the historic Open Government Directive in 2009 and released the first U.S. Open Government National Action Plan (NAP) in 2011 — a set of 26 commitments that have increased public integrity, enhanced public access to information, improved management of public resources, and given the public a more active voice in the U.S. Government's policymaking process. A notable example of the progress made since the release of the first NAP is the successful launch of We the People, the White House petitions platform that gives Americans a direct line to voice their concerns to the Administration via online petitions. In two years, more than 10 million users have generated over 270,000 petitions on a diverse range of topics, including gun violence, which received a video response from the President, and unlocking cell phones for use across provider networks, which led directly to policy action.

Building upon these efforts to create a more efficient, effective, and accountable Government, on December 5, 2013 the Administration issued the second Open Government National Action Plan which includes a wide range of actions the Administration will take over the next two years supported by the Budget, including commitments that build upon past successes as well as several new initiatives. For example, with the Global Initiative on Fiscal Transparency, the United States will join an international network of governments and non-government organizations aimed at enhancing financial transparency, accountability, and stakeholder engagement in domestic and global spending. Additionally, the government will

promote community-led, participatory budgeting as a tool for enabling citizens to play a role in identifying and discussing certain local public spending projects, and for giving citizens a voice in how taxpayer dollars are spent in their communities.

Presidential Innovation Fellows — The Presidential Innovation Fellows program⁸ pairs entrepreneurs from the private sector, non-profits, and academia with top innovators in Government to collaborate on solutions to high-impact challenges and deliver significant results in six to twelve months. The results of these projects are intended to save taxpayer money, fuel job growth, bring private sector best practices to Government, and provide tangible benefits to the American people. Each team of innovators is tasked with working on a specific high-impact issue using a focused, agile approach. What makes this initiative unique is its focus on tapping into the ingenuity, know-how, and patriotism of Americans from every sector of our society. The first round of Fellows was welcomed in August 2012 with 18 inaugural fellows, expanding in round two in the summer of 2013 to over 35 fellows across nine projects. The second class of fellows began in June 2013 with more than 40 Fellows. Examples of projects include:

- **Blue Button**, which is helping more than 150 million veterans and other Americans across the country gain secure electronic access to their own personal health records and increase access to private-sector applications and services.
- **MyUSA**, which is greatly simplifying the online interface that citizens can use to find what they need from the Federal Government.
- **RFP-EZ**, a new system that simplifies how the Federal Government asks for bids on services like building websites and can help save taxpayer money.

PROTECTING DATA AND ASSETS— CYBERSECURITY AND PRIVACY

Cybersecurity—American citizens depend on Federal agencies for essential services, ranging from disaster assistance, to Social Security and national defense. These services, in turn, rely on safe, secure, and resilient Government information and infrastructure. To ensure the safety and security of Government information and infrastructure, as called for by the Federal Information Security Management Act (FISMA)⁹, the Administration will act on many fronts, while protecting individual privacy and civil liberties. Some key cybersecurity focus areas for OMB and the Department of Homeland Security (DHS) for FY 2015 include:

- **Managing Information Security Risk on a Continuous Basis**—To strengthen the nation's cybersecurity posture, OMB issued *Memorandum 14-03 on Enhancing the Security of Federal Information and Information*

⁸ Program description at: <http://www.whitehouse.gov/innovationfellows>.

⁹ FISMA was enacted in Title II of the E-Government Act of 2002 (P.L. 107-347, 116 Stat. 2899).

Systems. This memorandum provides agencies with guidance for managing information security risk on a continuous basis and builds upon efforts towards achieving the Cybersecurity Cross Agency Priority (CAP) Goal. The effort includes the requirement to monitor the security controls in Federal information systems and the environments in which those systems operate on an ongoing basis, which allows agencies to maintain ongoing awareness of information security vulnerabilities and threats to support organizational risk management decisions.

- A key component of managing information security risk on a continuous basis is DHS's Continuous Diagnostics and Mitigation (CDM) program. By FY 2015, DHS anticipates that the CDM Program will provide specialized IT tools to combat cyber threats in the civilian ".gov" networks. The CDM approach moves the Government toward real time monitoring in order to more rapidly respond to threats to the nation's networks. The tools and services delivered through the CDM program will provide DHS, other Federal agencies, and State, local, regional, and tribal governments with the ability to enhance and automate their existing continuous network monitoring capabilities; correlate and analyze critical security-related information; and enhance risk-based decision making across the Government. Information obtained from the automated monitoring tools will allow for the correlation and analysis of security-related information across the Federal enterprise to improve the overall Federal cybersecurity posture.
- FISMA Metrics and FY 2015 Cybersecurity Cross-Agency Priority (CAP) Goal—OMB, in partnership with the National Security Council staff and DHS, will improve FISMA metrics to focus on outcome-oriented measures that are quantitative, specific, automated when possible, and focused on reduction of threats. As part of the work to improve the FY 2015 FISMA metrics, OMB plans to issue an updated Cybersecurity CAP goal, as required by the Government Performance and Results Act Modernization Act (GPRAMA). The updated CAP goal will focus on managing information security risk on a continuous basis; Identity, Credential, and Access Management (ICAM); and Phishing and Malware Defense. Moving forward, OMB will establish baselines and agency targets to monitor agency progress.
- Improved Oversight through CyberStat process—OMB, in partnership with DHS, will continue to

work with agencies to identify and remediate weaknesses in cybersecurity programs, while ensuring agency progress towards the FY 2015 Cybersecurity CAP Goal through CyberStat reviews. The reviews provide the opportunity for agencies to identify the cybersecurity capability areas where they may be facing implementation roadblocks, including technology, organizational culture, processes, human capital, or resource challenges.

Protect Privacy and Confidentiality—The Administration is committed to protecting individual privacy and confidentiality. Federal agencies are expected to demonstrate continued progress in all aspects of privacy and confidentiality protection and to ensure compliance with all privacy and confidentiality requirements in law, regulation, and policy. In particular, Federal agencies must take steps to analyze and address privacy and confidentiality issues at the earliest stages of the planning process, and they must continue to manage information responsibly throughout the life cycle of the information. Moreover, agencies will continue to develop and implement policies that outline rules of behavior, detail training requirements for personnel, and identify consequences and corrective actions to address non-compliance.

Insider Threat Mitigation—In accordance with Executive Order 13587 - *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, the Administration is working with agencies to implement structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks that shall be consistent with appropriate protections for privacy and civil liberties. Agencies bear the primary responsibility for meeting these twin goals. These structural reforms will ensure coordinated interagency development and reliable implementation of policies and minimum standards regarding information security, personnel security, and systems security; address both internal and external security threats and vulnerabilities; and provide policies and minimum standards for sharing classified information both within and outside the Federal Government. These policies and minimum standards will address all agencies that operate or access classified computer networks, all users of classified computer networks (including contractors and others who operate or access classified computer networks controlled by the Federal Government), and all classified information on those networks.

CONCLUSION

The Administration is committed to continuously improving how Federal IT investments are designed, developed, and deployed to deliver increasing value to taxpayers. It will do so by ensuring efficient and effective agency IT investment portfolios, advancing a customer-focused

innovation agenda, and protecting Government data and personal privacy through policies and practices constantly updated to address the dynamic information technology environment in which we all live.

