17. INFORMATION TECHNOLOGY

With the radical evolution of technology, the Federal Government has an unprecedented opportunity to accelerate the quality and timeliness of services delivered to the American people. Over the past year, agency adoption of emerging technologies has had a dramatic impact. For example, the successful re-launch of HealthCare.gov in its second year, as well as the successful turnaround of the U.S. Department of Agriculture's Conservation Delivery Streamlining Initiative (CDSI), an online system that will provide American farmers and ranchers with real-time digital access to applying for financial assistance and conservation data on an easy and fast platform. To build on these successes, the Administration will continue to integrate modern technology solutions to enhance mission and service delivery by prioritizing three core objectives across the Federal information technology (IT) portfolio: (1) driving value in Federal IT investments, (2) delivering world-class digital services, to include opening Government data to fuel innovation, and (3) protecting Federal IT assets and information. Highlights of activities and initiatives undertaken to advance these objectives are provided in the Government of the Future chapter in the Budget volume, and in additional detail below.

DRIVING VALUE IN FEDERAL IT INVESTMENTS

Federal Spending on IT—Through a combination of policy guidance and oversight, this Administration has optimized IT spending to save taxpayers money by driving value and cost savings in Federal IT investments, and by delivering better services to American citizens. As shown in Table 17-1, the Budget's total planned spending on IT in 2016 is estimated to be $86.4 billion.[1] Chart 17-1 depicts how 7.1 percent annual growth in IT spending over 2001-2009 has been slowed to 1.5 percent annually for 2009-2016, due in part to the Administration's achievements in improving the efficiency of how funds are spent on IT.

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

	2014	2015	2016
Department of Defense.	37,415	36,267	37,314
Non-Defense	44,396	47,910	49,115
Total	81,810	84,177	86,429

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 January 12, 2015.

Focusing Agency IT Oversight on Comprehensive IT Portfolio Reviews—In 2015 and 2016, the Administration will continue to manage Federal IT strategically by implementing an expanded and more rigorous application of PortfolioStat—data driven reviews of agency IT portfolios led by the Office of Management and Budget (OMB). In addition to helping agencies achieve financial savings through reform efforts, PortfolioStat analyzes agency progress using a variety of performance metrics designed to measure whether agencies are delivering their IT investments on budget and on schedule, driving innovation to meet customer needs, and adequately protecting Federal data and systems. As part of its ongoing commitment to transparency, the Administration will make PortfolioStat and other technology reform savings and performance metrics available to the public on the IT Dashboard beginning in 2015.

In addition to PortfolioStat, key IT metrics were included in the first round of benchmarking meetings, held as part of the Benchmark and Improve Mission-Support Operations Cross-Agency Priority (CAP) goal.[2] The purpose of this CAP goal is to improve administrative efficiency and increase the adoption of effective management practices by establishing cost and quality benchmarks in five key areas that support agency mission operations: IT, human capital, financial management, acquisitions, and real property. As a result of the benchmarking effort, each of the 24 CFO Act agencies now has unprecedented access to Government-wide data, as well as visibility into the performance and cost of their IT and other mission support operations relative to other agencies. Armed with this knowledge, agency decision-makers are better equipped to set priorities, allocate resources, and improve processes within their agencies.

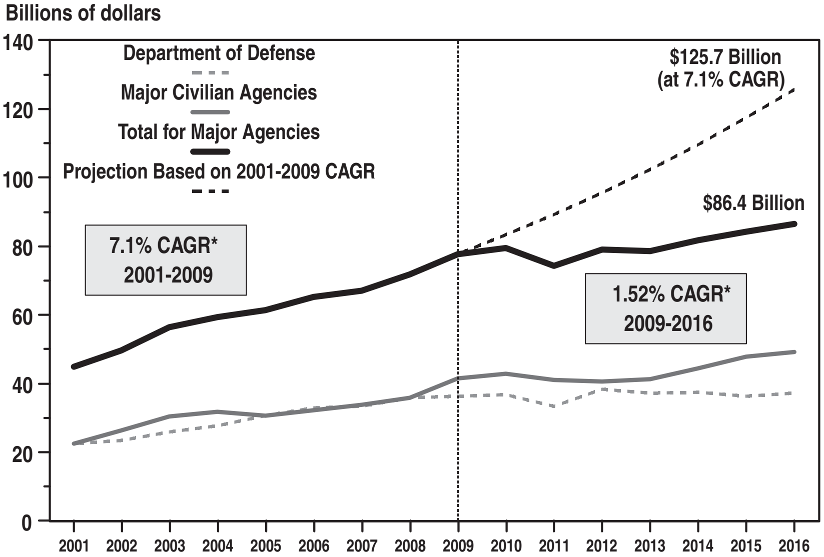
OMB requires that agency Chief Information Officers (CIOs) rate on a continuous basis all major IT investments reflected on the IT Dashboard and assess how well the risks for major development efforts are being addressed and mitigated. The IT Dashboard shows continued improvements in the general health of IT investments across government, as denoted by the increased proportion of CIO-rated "Green" investments on the IT Dashboard, which comprised 74 percent of all rated investments in January 2014, compared to 69 percent in 2012 (assessments based on total life cycle of investments).

Government-Wide Successes—The Administration's continued focus on driving value in Federal IT investments has led to key successes across the Federal IT portfolio. Specific examples include:

[1] Based on agencies represented on the IT Dashboard, located at: *http://itdashboard.gov*.

[2] For more information on CAP goals, see *http://www.performance.gov*.

Chart 17-1. 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 January 12, 2015.

- Government-wide cost savings—Since 2012, the Federal Government has saved at least $2.7 billion[3] as a result of the Administration's IT reform efforts, including initiatives such as PortfolioStat, the Federal Cloud Computing Strategy,[4] commodity IT consolidation, migration to shared services, and the Federal Data Center Consolidation Initiative (FDCCI).[5]

- Increased use of modern, agile development practices[6]—Agencies have increased their use of agile development practices and are delivering value 21 days (11 percent) faster since May 2013. Evidence in the IT portfolio shows that these agile projects have been nearly twice as likely to deliver on time as those using "waterfall" development techniques,[7] and have been 40 percent more likely to deliver planned capabilities on budget.[8] Using agile development ultimately increases the ability to deliver a better product to citizens faster. For example, the Department of State, a leader in adopting agile development, has improved its average project delivery time from 235 days in May 2013 to 111 days today, thereby delivering projects 53 percent faster than they were just months ago.

- Shifting to more efficient computing services—the Federal Government now spends approximately 8.5 percent of its IT budget on provisioned services such as cloud, on par with leading private sector companies. For example, the National Science Foundation has made exemplary strides in cloud usage. Since 2014, the agency has prioritized moving its data to the cloud, and has already migrated several key services including email, financial systems, and backups of critical information. The agency has already saved $450,000 through its cloud initiatives, and it is aiming for complete migration by 2016.

- Data Center Consolidation—As part of FDCCI, agencies have closed 1,136 data centers as of August 2014, reversing the previous unsustainable data center growth trends, reducing energy consumption and the Federal real estate footprint, and enhancing the Federal IT security posture. The General Ser-

[3] As reported by agencies. Savings described in this chapter 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] *http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf*

[5] http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fdcci-update-memo-07202011.pdf

[6] Agile development is an incremental, fast-paced style of software development to reduce the risk of failure by getting working software into users' hands quickly by releasing bundles of features in frequent sprints based on evolving user needs. For additional information on the benefits of agile development, see *http://www.whitehouse.gov/sites/default/files/omb/procurement/guidance/modular-approaches-for-information-technology.pdf*.

[7] Waterfall development typically proceeds in sequential phases of consistent, fixed duration to produce a complete system. Such full system development efforts can take several years, potentially resulting in a product that is either outdated by the time it is released or contains features that are not aligned with user needs.

[8] Projects which are "on time" and "on budget" have schedule and cost variance of less than 10 percent and are depicted as "green" on the IT Dashboard.

vices Administration (GSA) leads the Government in data center closures, having closed 46 out of 125 total data centers. In addition, the Administration expanded FDCCI to better capture the effectiveness of data centers by establishing optimization metrics measuring energy, facility, labor, storage and virtualization of agency core data centers.

The Administration will build on these successes by strengthening Federal IT through its implementation of the Federal Information Technology Acquisition Reform Act (FITARA), which seeks to maximize the return on investment for IT services and supplies.[9]

[9] See *http://www.gpo.gov/fdsys/pkg/CPRT-113HPRT91496/pdf/CPRT-113HPRT91496.pdf* , page 355.

DELIVERING WORLD CLASS DIGITAL SERVICES

Smarter IT Delivery—In 2014, the Administration established the Smarter IT Delivery CAP goal,[10] making an aggressive commitment to world class customer satisfaction with the Government's highest-impact customer-facing digital services. The Administration has invested in a portfolio of Government-wide efforts to ensure that all agencies have access to the best partners, people, and digital practices. These efforts have included central resources positioned to support digital services teams and CIO organizations at all agencies, including: the new U.S. Digital Service (USDS) at OMB; GSA's 18F, a digital service delivery unit to help with projects throughout government; numerous tools and services offered by GSA's Office of Citizen Services and Innovative Technologies (OCSIT);[11] and ongoing policy leadership from the U.S. Chief Information Officer and U.S. Chief Technology Officer. To ensure the best partners are working with agencies in reaching our Smarter IT Delivery goal, the Administration is working to strengthen vendor relationships and bring innovative companies into the marketplace. The Administration has already piloted feedback systems in which vendors can rate their experience in dealing with Federal acquisitions, and has also made it simpler for agencies to view and analyze vendor performance information. These efforts will be expanded in 2015 and 2016. The 2016 Budget includes legislative proposals to make it easier for small startup and other innovative companies to break into the Federal marketplace and to make it easier and less bureaucratic for agencies to purchase goods and services. The Administration has also made a number of major investments to bring the best people and best digital practices into the Federal Government, as described below.

Scaling the U.S. Digital Service— In 2014, the Administration piloted the U.S. Digital Service (USDS)[12] by recruiting a group of select public and private sector innovators, entrepreneurs, and engineers to Government service. Since standing up, this team of America's best digital experts has worked in collaboration with Federal agencies to implement cutting edge digital and technology practices on the nation's highest impact programs, including the successful re-launch of *HealthCare.gov* in its second year, the Veterans Benefits Management System, and an improved process for online visa applications, among others. In 2015 and 2016, the Administration will strengthen and expand USDS's engagement with agencies to institutionalize modern digital services principles and practices across the Federal Government. Specifically, the Budget includes $105 million to incubate digital service teams within 25 major agencies across Government. These teams will be dedicated to driving the quality, effectiveness, and cost savings of each agency's highest-impact digital services. In 2015 and 2016, the core team of digital service experts at USDS will support these agency teams through shared recruiting, coordination, and Government-wide platforms for digital service tools. Some agencies took the initiative to begin to build such teams in 2014 and are already seeing results: a team of three in-house digital service experts at the Department of Veterans Affairs (VA) spent three months building the Veterans Employment Center, which delivered the functionality of three different planned IT systems one year early and allowed the VA to cancel a planned $2.4 million procurement, eliminate another ongoing $9 million per year contract, and save $3.3 million per year on a separate ongoing contract. To fully support the launch and ongoing operations of the agency teams, the 2016 Budget also includes enhanced funding for core OMB USDS operations.

Digital Services Playbook and TechFAR Handbook— To guide agency engagements and to provide all Federal IT projects with a common set of best practices for effective digital service delivery, USDS published the Digital Services Playbook and TechFAR Handbook.[13] The Playbook outlines key "plays," drawn from private and public-sector best practices, which will help Federal agencies deliver services that work well for users and require less time and money to develop and operate. The TechFAR Handbook explains how agencies can execute key plays in the Playbook in ways consistent with the Federal Acquisition Regulation (FAR), which governs how the Government must buy goods and services from the private sector. Federal agencies are already seeing the benefit of these plays: today, planned Federal IT projects are three times more likely to use agile methodologies like those described in the playbook, rather than outdated monolithic waterfall methodologies. Federal projects which use agile techniques are much more likely to be on track to deliver value on time and on budget, compared to projects using waterfall approaches. In 2015, the

[10] The mission of the Smarter IT CAP goal is to improve outcomes and customer satisfaction with Federal services through smarter IT delivery and stronger agency accountability for success. For more information on CAP goals, see *http://www.performance.gov*.

[11] OCSIT is responsible for providing the public access to data, information, and services offered by the Federal Government and assists agencies in identifying and applying new technologies to effective government operation. For more information, see *http://www.gsa.gov/portal/category/25729*.

[12] See *http://www.whitehouse.gov/usds/*

[13] The Digital Services Playbook and TechFAR Handbook are available at *https://playbook.cio.gov/*.

Administration will work to develop IT acquisitions training for the Federal IT acquisitions workforce based on the principles and techniques provided in the Playbook and TechFAR. In 2016, the Administration will begin broad implementation of these training sessions for agency personnel, resulting in agencies throughout Government having personnel on hand trained in innovative acquisition practices. The Playbook and TechFAR will also serve as the backbone and guiding principles for the operations of the agency digital services teams.

Information as an Asset—Government Open Data— The Administration has placed a high priority on transparency and, in particular, on opening Government data as fuel for private sector innovation and public use. The Administration has released over 75,000 data sets to the public since 2009, of which over 67,000 data sets were released in the last year alone. The use of these data sets has had a wide impact: from job creation through innovative start-up companies, to increasing the transparency of retirement plans, to assisting citizens in making informed housing decisions. In fact, a recent study[14] estimated more than $1 trillion dollars of annual potential economic benefit stemming from the opening of U.S. data. The Administration's open data agenda includes a number of initiatives and Open Data Policy directives, including:

- Executive Order 13642[15] and OMB Memorandum 13-13,[16] which have made "open and machine-readable" the new default for Government information.
- The continuing evolution of *Data.gov*, the U.S. Government's catalog for open data, tools, and resources, which currently contains tens of thousands of datasets and hundreds of Federal application programming interfaces (APIs).[17]
- The Open Data CAP goal,[18] which sets forth action plans, milestones, and targets for agencies to make Federal data open and machine-readable by default, and to fuel economic growth and innovation with open data.
- Project Open Data,[19] a central repository of free, open source tools, case studies, and best practices. Project Open Data includes a public dashboard[20] showing how Federal agencies are performing on the Open Data Policy and CAP goal.
- Workshops and summits with companies, data owners, and other innovators to foster community engagement, highlight open data successes and share best practices.

The 2016 Budget provides $16 million for E-Government initiatives in the General Service Administration's Federal Citizen Services Fund, supporting important IT investments including open data and digital government initiatives. While emphasizing the opening of Federal data, safeguarding the privacy, confidentiality, and security of sensitive information is of the utmost importance, and agencies are required to do thorough reviews of their data prior to publication to ensure no sensitive information is released.

[14] *http://www.mckinsey.com/insights/business_technology/open_data_unlocking_innovation_and_performance_with_liquid_information*

[15] 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.*

[16] 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.*

[17] *http://www.data.gov*

[18] The mission of the Open Data CAP goal is to fuel entrepreneurship and innovation and improve Government efficiency and effectiveness by unlocking the value of government data and adopting management approaches that promote interoperability and openness of these data. For more information on CAP goals, see *http://www.performance.gov*.

[19] *https://project-open-data.cio.gov/*

[20] *http://labs.data.gov/dashboard/*

CYBERSECURITY: PROTECTING FEDERAL IT ASSETS AND INFORMATION

As the Government continues to increase the accessibility of Federal resources and information available to the public online, governmental systems and data are increasingly exposed to the growing and evolving threat posed by cyber-based attacks. To ensure the safety and security of Government information, the Administration has adopted a multifaceted approach to protect Federal resources while maintaining individual privacy and civil liberties. Some key cybersecurity focus areas for the Federal Government in 2015 and 2016 include:

Managing Information Security Risk on a Continuous Basis— Building on previously granted authorities,[21] the Department of Homeland Security (DHS) has continued to develop its Continuous Diagnostics and Mitigation (CDM) program. CDM enables agencies to invest in a centralized continuous monitoring program that will allow them to quickly and efficiently identify cybersecurity vulnerabilities and mitigate risk. CDM moves the Government toward real-time monitoring in order to combat cyber threats in the civilian and national security networks. CDM tools and services provide Government agencies at all levels with the ability to enhance and automate their existing continuous network monitoring capabilities, analyze critical security-related information, and enhance risk-based decision making. The Administration will begin deploying CDM capabilities to certain agencies in 2015, and in 2016 will expand the features of CDM's state of the art tools and services and scale them across Government. In addition to CDM, OMB recently enacted a new policy that will require regular and proactive scans of public facing segments of Federal civilian agency networks. OMB directed DHS to

[21] OMB Memorandum M-14-03 "Enhancing the Security of Federal Information and Information Systems": *http://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf*

perform these scans and provided DHS and Federal agencies with guidance as to their responsibilities.[22]

Improved Oversight through CyberStat Process—In 2015 and 2016, the Administration, including OMB and National Security Council staff, will coordinate with DHS to continue working with agencies to identify and remediate weaknesses in cybersecurity programs while ensuring agency progress towards the Cybersecurity CAP goal[23] through CyberStat reviews. These reviews provide the opportunity for agencies to identify the cybersecurity areas where they may be facing implementation and organizational challenges.

Coordinating Agency Responses to Cyber Events—Vulnerability to cyber incidents transcends agency boundaries, making strong coordination across the Federal environment essential in order to rapidly respond to threats as they emerge. Cybersecurity events such as Heartbleed[24] and the Bash[25] vulnerability have illustrated the need for the Administration, through OMB and the National Security Council, to play a central coordinating role to ensure agencies are taking appropriate actions to effectively respond to cyber events and address any deficiencies in their cybersecurity programs to reduce overall risk, and prevent future events from occurring. In both instances, the Administration effectively managed the Federal response activities of relevant stakeholders and ensured that agencies implemented appropriate mitigation measures as quickly as practicable.

Implementing and Supporting Enhancements to Legislation—The Federal Information Security Modernization Act of 2014 (FISMA Modernization) was signed into law in December 2014, and it enhances the security of Federal networks placing new requirements on Federal agencies to improve the transparency and performance of their cybersecurity programs, among other things. In 2015, the Administration will be working to ensure FISMA Modernization is implemented effectively throughout Government. Although FISMA Modernization addresses many challenges, additional legislative action is required to improve the overall cybersecurity of the Nation. In January 2015, the Administration proposed legislative changes through a Cybersecurity Legislative Proposal.[26] This proposal covers three critical areas:

- Enabling Cybersecurity Information Sharing: Increased information sharing is a key element in improving our cybersecurity posture and the proposal promotes better information sharing between the private sector and Government.
- Data breach standards: The Administration's updated proposal on security breach reporting helps business and consumers by simplifying and standardizing the existing patchwork of 46 State laws (plus the District of Columbia and several territories) that contain data breach reporting requirements into one Federal statute, and it puts in place a single, clear requirement to ensure that companies notify their employees and customers about security breaches on a timely basis.
- Criminal penalties: The Administration's proposal contains provisions that would allow for the prosecution of the sale of botnets; would criminalize the overseas sale of stolen U.S. financial information like credit card and bank account numbers; would expand Federal law enforcement authority to deter the sale of spyware used to stalk or commit ID theft; and would give courts the authority to shut down botnets engaged in distributed denial of service attacks and other criminal activity.

[22] OMB Memorandum M-15-01 "Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices": *http://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-01.pdf*

[23] The mission of the Cybersecurity CAP goal is to improve cybersecurity performance through ongoing awareness of information security, vulnerabilities, and threats impacting the operating information environment, ensuring that only authorized users have access to resources and information; and the implementation of technologies and processes that reduce the risk of malware. For more information on CAP goals, see *http://www.performance.gov*.

[24] See *https://www.us-cert.gov/sites/default/files/publications/Heartbleed percent20OpenSSL percent20Vulnerability_0.pdf*.

[25] See *https://www.us-cert.gov/ncas/alerts/TA14-268A*.

[26] See *http://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal*

CONCLUSION

Ensuring the efficiency, effectiveness, and security of Federal IT has never been more central to how Americans are served by their Government. Over the past six years, this Administration has focused on driving efficiencies in the way the government buys, builds, and delivers IT solutions to provide improved services to citizens, and these efforts will be strengthened in 2015 and further scaled across Government in 2016. The 21st Century digital service delivery standards being set by this Administration represent an important commitment to future generations. The 2016 Budget includes funding that will launch the Nation on a path to hire the leading digital experts, institutionalize modern digital delivery practices, and establish more effective partnerships both within Government and with the private sector that will ensure our citizens are provided services at a historically unprecedented level of quality and timeliness.