FY 2016 ANNUAL REPORT TO CONGRESS:

E-GOVERNMENT ACT IMPLEMENTATION

OFFICE OF MANAGEMENT AND BUDGET
August 2017

TABLE OF CONTENTS

INTRODUCTION

Since the passage of the E-Government Act of 2002 44 U.S.C. § 3601 (E-Gov Act), Federal agencies have made significant progress in using the internet and other technologies to enhance citizen access to Government information and services improving Government transparency and decision making. The E-Gov Act requires Federal agencies and the Office of Management and Budget (OMB) to report annually on their progress implementing the various provisions of the E-Gov Act, as described in more detail below.

OMB developed this report in accordance with 44 U.S.C. § 3606, which requires OMB to provide a summary of the information reported by Federal agencies and a description of compliance by the Federal Government with the provisions of the E-Gov Act. The E-Gov Act includes numerous requirements for OMB and Federal agencies to ensure effective implementation of the Act. For example, the Act requires agencies to provide OMB with links to various websites including the agency's Freedom of Information Act (FOIA) information and agency activities on www.USA.gov. This report provides a summary of OMB and agency compliance with these requirements. Additionally, in an effort to streamline this year's report, OMB has utilized the Federal IT Dashboard (IT Dashboard) to provide agency implementation data. The information on the IT Dashboard reflects the information agencies provided to OMB.

Additionally, consistent with previous E-Gov Act reports, this report includes information required under the Federal Funding Accountability and Transparency Act of 2006, Pub. L. No. 109-282, codified at 31 U.S.C. § 6101 note. Under this Act, OMB is required to oversee and report to Congress on the development of a website through which the public can readily access information about grants and contracts provided by the Federal agencies.[1]

This report is structured in numerical order according to the required sections of the E-Gov Act. For a description of reporting requirements and the corresponding report sections, please see Appendix I. This report is organized as follows:

- **Section I – Office of E-Government Initiatives**
  In accordance with Section 101 of the E-Gov Act (44 U.S.C. §§ 3604 and 3606), this section describes the status of the E-Government fund in Fiscal Year (FY) 2016. Since FY 2015, appropriations for the E-Government Fund (E-Gov Fund) have been appropriated to the General Services Administration's (GSA) Federal Citizen Services Fund (FCSF). Any remaining balances in the E-Gov Fund were authorized to be transferred to the FCSF. This section describes some of the initiatives that the Office of E-Gov (Office of the Federal Chief Information Officer (OFCIO)) leads in

[1] Federal Funding Accountability and Transparency Act of 2006, 31 U.S.C. § 6101 note provides:

REPORT.— (1) IN GENERAL.—The Director of the Office of Management and Budget shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Government Reform of the House of Representatives an annual report regarding the implementation of the website established under this section. (2) CONTENTS.—Each report submitted under paragraph (1) shall include—(A) data regarding the usage and public feedback on the utility of the site (including recommendations for improving data quality and collection); (B) an assessment of the reporting burden placed on Federal award and subaward recipients; and (C) an explanation of any extension of the subaward reporting deadline under subsection (d)(2)(B), if applicable. (3) PUBLICATION.—The Director of the Office of Management and Budget shall make each report submitted under paragraph (1) publicly available on the website established under this section.

order to drive innovation in Government operations and using IT to improve the transparency, efficiency and effectiveness of Federal operations, and increase citizen participation in Government.

- **Section II – Government-wide Information Technology (IT) Workforce and Training Policies**
  This section provides a summary of activities related to IT workforce policies, evaluation, training, and competency assessments pursuant to Section 209 of the E-Gov Act (44 U.S.C. § 3501 note).

- **Section III – Disaster Preparedness**
  In accordance with Section 214 of the E-Gov Act (44 U.S.C. § 3501 note), this section provides a summary of how IT is used to further the goal of maximizing the utility of IT in disaster management.

- **Section IV – Geospatial**
  In accordance with Section 216 of the E-Gov Act (44 U.S.C. § 3501 note), this section provides a summary of activities on geographic information systems and initiatives and an overview of the Geospatial Platform.

- **Appendices – Compliance with Other Goals and Provisions of the E-Gov Act**
  The appendices contain broad overviews of activities agencies are undertaking to comply with the goals of the E-Gov Act, including highlights of some agency-specific efforts. Full agency descriptions of compliance with each provision of the Act can be found on the IT Dashboard.

  - *Appendix A - Enhanced Delivery of Information and Services to the Public:* In accordance with Section 101 of the E-Gov Act, (44 U.S.C. § 3602(f)(9)), this appendix describes agency activities that enhance delivery of information and services to the public.

  - *Appendix B - Performance Integration:* In accordance with Section 202(b) of the E-Gov Act (44 U.S.C. § 3501 note), this appendix describes what performance metrics are used and tracked for IT investments, and how these metrics support agency strategic goals and statutory mandates.

  - *Appendix C - Government-Public Collaboration:* In accordance with Section 202(e) of the E-Gov Act (44 U.S.C. § 3501 note), this appendix describes how agencies utilize technology to initiate Government-public collaboration in the development and implementation of policies and programs.

  - *Appendix D - Credentialing:* In accordance with Section 203 of the E-Gov Act (44 U.S.C. § 3501 note), this appendix describes current activities agencies are undertaking to achieve interoperable implementation of electronic credential authentication for Federal Government transactions.

  - *Appendix E - E-Rulemaking:* In accordance with Section 206 of the E-Gov Act

(44 U.S.C. § 3501 note), this appendix describes agencies' online electronic regulatory submission capabilities, specifically the usage of www.Regulations.gov and the Federal Docket Management System.

- *Appendix F - National Archives Records Administration Recordkeeping:* In accordance with Section 207(d) and (e) of the E-Gov Act (44 U.S.C. § 3501 note), this appendix describes agencies' adherence to the National Archives and Records Administration recordkeeping policies and procedures for electronic information online and other electronic records.

- *Appendix G – Privacy Policy and Privacy Impact Assessments:* In accordance with Section 208(b) of the E-Gov Act (44 U.S.C. § 3501 note), this appendix provides information regarding agencies' privacy impact assessments and privacy policies.

- *Appendix H - Agency Information Technology Training Programs:* In accordance with Section 209(b) of the E-Gov Act (44 U.S.C. § 3501 note), the appendix describes agency training programs for the IT workforce.

- *Appendix I - Description of E-Gov Act Reporting Requirements and Corresponding Report Sections.*

SECTION I: OFFICE OF E-GOVERNMENT INITIATIVES

The E-Government Fund

The E-Gov Act established an E-Gov Fund to provide financial support for the innovative use of information technology in the Federal Government (44 U.S.C. § 3604). Projects supported by the E-Gov Fund included efforts to:

- Make Federal Government information and services more readily available to members of the public;

- Make it easier for the public to apply for benefits, receive services, pursue business opportunities, submit information, and otherwise conduct transactions with the Federal Government; and

- Enable Federal agencies to take advantage of IT in sharing information and conducting transactions with each other and with state and local governments.

Pursuant to the Act, OMB was required to report annually to Congress on the operation of the Fund, including which projects the Director of OMB approved for funding from the Fund, and the results those funded projects that achieved.

Since FY 2015, as first specified in the Consolidated and Further Continuing Appropriations Act 2015, Pub. L. No. 113-235, funding for E-Gov Act projects has been appropriated to the GSA Federal Citizen Services Fund (FCSF) rather than to the E-Gov Fund. Therefore, GSA's FCSF now manages the allocation of funds to support E-Gov Act IT initiatives. The 2015 Appropriations Act also permitted transfer of any funds in the E-Gov Fund from fiscal years prior to FY 2015 that remained unobligated as of September 30, 2014, to the FCSF.

Select Highlights of OFCIO Initiatives for FY 16

The Office of E-Gov (OFCIO) at OMB continues to drive innovation in Government operations, using IT to improve the transparency, efficiency and effectiveness of Federal operations, and increase citizen participation in Government.

Open Source

In August 2016, OMB released M-16-21 Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software. This policy aims to mitigate wasteful spending associated with duplicative software acquisitions, ultimately reducing the $6 billion that the Federal Government spends each year on new software transactions. Following this policy, new custom software developed specifically for or by the Federal Government must be made available for sharing and reuse across all Federal agencies. This has the potential to save significant taxpayer dollars by trimming duplicative acquisitions and avoiding vendor lock-in. In addition, agencies are required to take part in an open source pilot program. Agencies will share 20 percent of new Federally funded custom code as open source software as part of a three-year pilot program designed to maximize the economic benefits associated with code sharing and reuse. This portion of the policy will sunset after three years.

In November 2016, OMB launched Code.gov to facilitate the effective implementation of the Federal Source Code Policy. This platform enables agencies to identify whether their software needs can be satisfied via an existing Government solution prior to procuring new software, thereby cutting wasteful spending and avoiding duplicative acquisitions.

Data Center Optimization

In 2010, OMB launched the Federal Data Center Consolidation Initiative (FDCCI) to reduce the number of Federal data centers and associated costs. Since that time, agencies have closed over 1,900 data centers and saved nearly $1 billion. Still, more than 9,000 data centers remain in the Federal inventory. The *Data Center Optimization Initiative* (DCOI), launched August 1, 2016, set a goal of closing approximately 52% of the remaining 9,000 data centers in the Federal inventory. The initiative also seeks to optimize remaining data centers across five metrics, develop a shared services marketplace in conjunction with the General Services Administration (GSA), and reduce data center spending by $2.7 billion by the end of FY 2018. OMB continues to assist agencies with oversight and implementation support for DCOI goals, with significant progress occurring in FY 2016. The latest DCOI cost-savings, closures, and optimization figures are all available on the IT Dashboard.

Cybersecurity Efforts

In accordance with the Federal Information Security Modernization Act of 2014 (FISMA), OMB is responsible for overseeing Federal agencies' information security practices and developing and implementing related policies and guidelines. The Federal Chief Information Security Officer (CISO) leads the OMB Cyber and National Security Unit

(OMB Cyber), which serves as the dedicated team within OFCIO that works with Federal agency leadership to address information security priorities. OMB Cyber collaborates with partners across the Government to develop cybersecurity policies, conduct data-driven oversight of agency cybersecurity programs, and coordinate the Federal response to cyber incidents.

During FY 2016, Federal agencies made considerable progress in strengthening their defenses and enhancing their workforces to combat cyber threats. In particular, agencies worked to enforce the use of multi-factor Personal Identity Verification (PIV) cards, with 81% of Government users now using this credential to access Federal networks. Additionally, over 70% of Federal agencies have employed strong anti-phishing and malware capabilities to help safeguard their networks from malicious activity. Agencies have also made significant progress toward safeguarding their high value IT assets and employing capabilities to identify, detect, and protect hardware and software assets on their networks.

OMB worked with agencies to develop policies aimed at strengthening cybersecurity across the Government, including a revision to OMB Circular A-130, Managing Information as a Strategic Resource, which sets the overarching framework for managing Federal IT resources. OMB also collaborated with the Office of Personnel Management to publish the first-ever Federal Cybersecurity Workforce Strategy to help agencies recruit and retain top cyber talent. OMB and its interagency partners look to build on these policies and continue driving cybersecurity performance in the coming years.

Additional information about these efforts can be found in the FY 2016 Annual FISMA Report, which OMB released in March 2017.

Open Government

- Launched in FY 2013 Project Open Data provides agencies with tools and best practices to make their data publicly available, and the Project Open Data Dashboard provides publicly accessible evaluations of agency progress in implementation of the Open Data Policy. OMB updates the agency evaluations on a quarterly basis and enhances its features regularly.

- The Interagency Open Data Working Group continues to responsibly unleash the power of data for the benefit of the American public and to maximize the nation's return on its investment in data. Led by OMB, the Office of Science and Technology Policy (OSTP), and the Data.gov team at General Services Administration (GSA), this community of practice hosts biweekly implementation meetings on Project Open Data for Federal employees and contractors. It connects over 800 Federal data professionals, who develop open data tools, share best practices, and ensure the adoption of best practices related to data governance, data policy, and the hiring and training of data science professionals. These biweekly U.S. Government Open Data meetings are open to public stakeholders on a quarterly basis.

- In 2016, OFCIO in OMB prioritized public feedback tools to facilitate the release of open data. OMB's M-13-13, Open Data Policy and the third U.S. Open Government

National Action Plan directed Federal agencies to engage with data users to prioritize release of open Government data, and agencies have approached this requirement in a variety of ways. OMB, OSTP, and GSA data.gov teams worked with Federal agencies to promote consistent, customer-friendly feedback mechanisms on opening new datasets and improving existing datasets.

- Between March and June 2016, OMB, OSTP, and the Center for Open Data Enterprise co-hosted a four-part Open Data Roundtable series to improve understanding of how Government data is used, with participation from approximately 300 leaders from Government, the private sector, and academia. The Roundtables identified case studies, lessons learned, and best practices to initiate rapid advancements in delivery of public services.

- In summer 2016, OMB hosted an Open Data User Engagement series to foster a community of Federal data stewards in Government. The five-session series met on a bi-weekly basis to improve user engagement skills and public engagement strategies to better engage the public with Government data sets. Participants learned how to identify data users, create personas, solicit user feedback, and launch hackathons to advance Federal agency missions in collaboration with public stakeholders.

- The first-ever White House Open Data Innovation Summit convened more than 1,200 Government trailblazers, entrepreneurs, advocates, and civic innovators at the Washington Convention Center on September 28, 2016. The Summit was co-hosted by OMB, the Office of the Vice President (OVP), GSA, the U.S. Small Business Administration (SBA), and the Data Foundation as a civil society partner. An additional 8,500 watched the Summit Livestream online. As part of the Summit, The White House published an Open Data Fact Sheet to highlight key open data accomplishments, impact, and value: "Data by the People, for the People — Eight Years of Progress Opening Government Data to Spur Innovation, Opportunity, & Economic Growth". At the Summit, agencies announced new or enhanced open data initiatives including:
    - GSA – improved Data.gov and Project Open Data, and launched a new effort, the U.S. Data Federation portal, for Government-wide data common formats, specifications, and vocabulary standardization.
    - DOT – released the Fatality Analysis Reporting System Open Data set containing detailed, anonymized information about each tragic incident.
    - U.S. Department of Commerce, National Technical Information Service (NTIS) – announced a data innovation partnership to provide data services through joint venture partnerships helping to advance Federal data priorities.

SECTION II: GOVERNMENTWIDE IT WORKFORCE AND TRAINING POLICIES

Section 209 of the E-Gov Act (44 U.S.C. § 3501 note) requires the Office of Personnel Management (OPM), in coordination with OMB, the Chief Information Officers (CIO) Council and GSA, to analyze the personnel needs of the Federal Government related to IT and information resource management. The Act further states that OPM, in coordination with OMB, the CIO Council, and GSA must identify where current training does not satisfy current personnel needs, and issue policies to promote development of performance standards for training. In accordance with Section 209 of the E-Gov Act, this section provides a summary of FY 2016 activities related to IT workforce policies, evaluation, training, and competency assessments. Appendix H of this report provides examples of agency-specific training initiatives.

In November 2015, OMB issued a memorandum titled "Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government" which required OPM and OMB to publish a Federal Cybersecurity Workforce Strategy. In July 2016, the Federal Cybersecurity Workforce Strategy was jointly issued by OMB, OPM, and the Federal Chief Information Officer. In December 2015, the "Federal Cybersecurity Workforce Assessment Act of 2015" imposed various reporting requirements on Federal agencies, including assigning revised Cybersecurity Data Standard codes to positions with information technology, cybersecurity, and cyber-related functions.

For the past three years, OPM has worked with agencies to collect and analyze data on the Federal cybersecurity workforce to identify and address the skills needed by this group. This effort included identifying and coding Federal positions with cybersecurity functions, thus allowing the Federal Government to pinpoint these crucial functions and positions. The codes align to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework and bring standardization across the public, private, and academic sectors to define cybersecurity work. An updated version of the Framework was released on November 2, 2016. OPM is currently revising the Government-wide Cybersecurity Data Standard codes to align with the newly designed NICE Federal Coding Structure. Since November 2015, OPM and OMB have worked collaboratively with agencies in their efforts to fulfill the reporting requirements of the "Federal Cybersecurity Workforce Assessment Act." An intra-agency working group was established to solicit input to address each aspect of the Act, which includes coding as well as reporting of cyber certification data. In addition, an on-line resource portal was established to share information on how agencies are collecting data. In FY 2017, OPM expects to provide formal guidance to agencies on fulfilling the reporting requirements of the Act.

In the area of talent development, OPM is establishing a Cybersecurity Human Resource cadre. These efforts will leverage opportunities for Government-wide rotational assignments to provide individuals with opportunities to work on interesting and challenging projects within various agencies and share critical skills with other cybersecurity employees. Talent development tailored cybersecurity training for employees, senior managers, and executives who work in related career fields outside of cybersecurity to include finance and acquisitions to ensure budget planning, financial management, and contracting help improve agencies' cybersecurity posture. Efforts have also covered leveraging the existing certifications and credentialing to improve the skills of existing employees and qualify them for pay increases or promotions based on increased technical abilities, and explore a legislative proposal for a cybersecurity skills and education incentive, where employees receive additional compensation based on their skills and education. In addition, OPM is working to promote the use of existing retention incentives, including exceptions to incentive spending limits in accordance with OPM guidance.

SECTION III: DISASTER PREPAREDNESS

Consistent with Section 214 of the E-Gov Act (44 U.S.C. § 3501 note), this section was developed in consultation with DHS and the Federal Emergency Management Agency (FEMA) and provides a summary of activities that maximize the use of IT for disaster management, including how IT enhances and supports crisis preparedness and response.

The Disaster Assistance Improvement Program

The Disaster Assistance Improvement Program (DAIP) maintains a Government-wide, single portal for disaster survivors to submit electronic applications for assistance. DAIP's mission is to ease the burden on disaster survivors by providing them with a mechanism to access and apply for disaster assistance through the collaborative efforts of Federal, state, local, tribal, and nonprofit partners.

Following a presidentially declared disaster for individual assistance, survivors in need of assistance can register online at DAIP's DisasterAssistance.gov. The DisasterAssistance.gov portal provides disaster survivors with a single source for potential assistance programs, easy access to the application, application updates and disaster related information. The secure portal ensures that disaster survivors, who may be displaced or otherwise out of contact, have access all Federal agencies that offer forms of disaster assistance, and continue to receive benefits from non-disaster related assistance programs.

In FY 2016, DAIP provided Registration Intake (RI) for 16 presidentially declared Individual Assistance (IA) disasters. It hosted 4,095,723 DisasterAssistance.gov site visits. It also registered 360,745 registrations for disaster assistance via call center support and internet transactions (120,233 using Desktops, 48,935 using Mobile Devices, 191,577 using FEMA Call Centers). The program continues to receive high customer satisfaction scores from survivors using the site. The program achieved "green" ratings from the DHS Office of Accessible Systems and Technology and the DHS Office of the Chief Information Officer Program Health Assessment.

Through continued investment in DAIP, the program implemented improvements to DisasterAssistance.gov to reduce the burden on disaster survivors who apply for federal disaster assistance. These efforts include modernizing a configuration rules engine and improving software to ensure survivors receive the fast and efficient responses with minimal latency even during high-impact disaster surge events.

SECTION IV: GEOSPATIAL

In accordance with Section 216 of the E-Gov Act (44 U.S.C. § 3501 note) this section provides a summary of activities related to the development, acquisition, maintenance, distribution, and application of geographic information. This includes common protocols that improve the compatibility and accessibility of unclassified geographic information and promote the development of interoperable information systems technologies that allow widespread, low-cost use, and sharing of geographic data by Federal agencies, state, local, and tribal Governments, and the public.

The Department of the Interior (DOI), as the managing partner, plays an important role in helping to facilitate the Government's efforts for the Geospatial Platform Shared Services (Geospatial Platform) initiative, which is led by the Executive Secretariat for the Federal Geographic Data Committee.

Geospatial Platform

The Geospatial Platform initiative continued to grow and maintain a fast rate of progress in 2016 with the release of many new features and capabilities. Some examples of these advancements include establishing the Geospatial Interoperability Reference Architecture (GIRA) as an online collaboration Community within the GeoPlatform, in coordination with the Program Manager-Information Sharing to further enable the timely discovery, access, use, and collaboration for the enhancement and sustainment of the GIRA. The GIRA provides guidance and best practices for geospatial data and system interoperability across agencies, between federal and non-federal partners, and across operational domains.

In addition, DOI added functionality to its GeoPlatform that now permits users to publish data direct access to the ArcGIS Online community and provide the ability to save and publish maps to the AGOL community Map Gallery. DOI made significant upgrades to the Geospatial Platform to improve the user experience through agile development processes, and expanded GeoPlatform capabilities across the spectrum of content and services such as:

- Provisioning enhancements to the Map Viewer for 2131 disparate integrated map services;

- Implementing significant enhancements to the common map manager;

- Strengthening IT security;

- Creating a shared marketplace tool for posting planned elevation data projects;

- Developing a new Platform resource manager (Registry+) for managing and providing rapid access to geospatial data, service, layer and map assets;

- Improving the Content Management System capabilities for Community support; and

- Providing a new service dashboard to monitor web service availability and reliability.

National Spatial Data Infrastructure (NSDI) Strategic Plan

The Federal Geographic Committee is working with partners in the Federal and non-Federal geospatial communities to develop an updated strategic framework for the National Spatial Data Infrastructure (NSDI). Geospatial data is a critical national asset that has increased the value of America's data resources and underpins key parts of the economy. Dependence on spatial data and services span all business sectors, levels of Government, and public and private investments. The NSDI provides a process for the collaborative development of this critical digital infrastructure for the Nation. The NSDI strategic framework will provide a high-level plan for the continuing development and expansion of the NSDI.

The NSDI framework has been developed with inputs from multiple sources, including forums for leaders of key geospatial organizations, workshops for Federal leaders, sessions at geospatial professional conferences, and public meetings of FGDC committees and the National Geospatial Advisory Committee. The ideas and suggestions received from partners have been instrumental in shaping the document. Following completion of the high-level strategic framework, the FGDC will develop a final NSDI strategic plan and implementation approach in 2017.

Foundational components of the NSDI are the National Geospatial Data Assets (NGDA) geospatial datasets managed by lead Federal agencies for mission execution and on behalf of all the other federal and non-federal users. Managed as national capital investments, the NGDAs make-up the core of the nation's geospatial data portfolio that is managed by the FGDC. Many datasets are managed by State, local, Tribal and other local Government agencies and the FGDC works with representatives from these entities to identify and advance the nation's geospatial portfolio and improve its fitness-for-use for mission execution and to understand and address priorities and issues of the nation.

The FGDC approved the creation of a new NGDA address theme in 2016 to support a collaborative national approach to address data. This action was strongly encouraged by non-federal partners and State, local and Tribal Governmental entities. The Departments of Transportation and Commerce (Census Bureau) are the federal agency leads. The lead agencies implemented pilot projects working with the State, local, and Tribal data managers and professional organizations to develop the initial data model and process work flows to support this national data aggregation initiative. A new FGDC Address Theme Subcommittee will support and promote the development of a National Address Database and will engage stakeholders from multiple levels of Government as mechanisms to sustain this national partnership or further developed.

Geospatial Data and Technology Standards

FGDC sponsored two items this year within the Open Geospatial Consortium: The Arctic Spatial Data Pilot Activity demonstrates the diversity, richness and value of Spatial

Data Infrastructure (SDI) Web services to Arctic SDI stakeholders; and, the Interoperability Testbed 12, a fast-paced, multi-vendor collaborative effort to define, design, develop, and test candidate interface and encoding specifications. This work supports the FGDC strategic plan Objective 3.1: “[l]ead and participate in the development and coordination of national and international standards applicable to the geospatial community.” The Arctic Spatial Data Pilot provides for greater adoption and utilization of standards resulting in enhanced interoperability of geospatial data, services, and systems. The Pilot also enables collaboration with the Canadian SDI and the emerging Arctic SDI geospatial communities and strengthens our strategic partnerships with existing standards development organizations.

Additional standards endorsed in 2016 included:

- Part 2, Digital ortho-imagery (revised), of the Geographic Information Framework Data Standard - facilitates interchange and use of digital ortho-imagery data.

- The United States Thoroughfare, Landmark, and Postal Address Data Standard (“Address Data Standard”) supports the (newly established) NGDA Address Theme - develops content specifications for address information; provides classifications for different types of addresses; establish appropriate standards and measures for evaluation of address data quality; and supports exchange of address data.

- INCITS/ISO 19115-1:2014, Geographic information -- Metadata -- Part 1: Fundamentals - a foundational geospatial metadata standard that provides information about identification, extent, quality, spatial and temporal aspects, content, spatial reference, portrayal, distribution, and other properties of digital geographic data and services.

- INCITS/ISO 19157:2013[2014] - facilitates description of geospatial data quality and defines standardized components and structures of data quality measures.

CONCLUSION

In 2002, Congress passed the E-Gov Act in response to the growing use of computers and the internet by the public, rapidly transforming societal interactions and the relationships between citizens, private business, and all levels of Government. In an effort to provide effective leadership and streamline Federal initiatives, OMB was tasked to spearhead efforts to develop and promote electronic Government services across the Federal Government. One of the key initiatives of this legislation was to improve the ability of the Government to achieve agency missions and program performance goals by promoting the use of emerging technologies across the Federal agencies to provide citizen-centric services and increase public access to Government information and data. Building on the objectives of this legislation, the Office of the Federal Chief Information Officer (OFCIO) within OMB has undertaken three broad goals for IT in the Federal Government: (1) reduce waste and duplication, and ensure that IT investments stay within their budgets and deliver on time; (2) help agencies deliver IT investments that maximize the Government's productivity and customer satisfaction; and (3) expand the use of data and analytics to support agency IT portfolio management.

Since the passage of the E-Gov Act, Federal agencies have made significant progress in using the Internet and other technologies to enhance citizen access to Government information and services improving Government transparency and decision making. This report highlights many of these innovative activities that will improve Government efficiency and delivery of services to the public. From disaster preparedness to Government-wide training programs, the Federal Government continues to develop new initiatives and reforms to improve the use of the internet and technology as required by the E-Gov Act.

APPENDICES: COMPLIANCE WITH OTHER GOALS AND PROVISIONS OF THE E-GOV ACT

This section provides a description of highlights of Federal agency compliance with other goals and provisions of the E-Gov Act. The subsections below are listed in order according to the corresponding sections of the E-Gov Act. The information contains broad overviews of what agencies are doing to comply with the goals of the E-Gov Act, and also includes some agency-specific illustrations of approaches to complying with the provisions of the Act. To view full agency descriptions of compliance with each provision of the act, please visit the IT Dashboard FY 2016 E-Gov Act Page.

Furthermore, several of the requirements set forth in the E-Gov Act require the provision of web addresses to specific content on agency websites. Due to the nature of these requirements, summaries of the following submissions are not included in the appendices but are included on the IT Dashboard:

- Accessibility: In accordance with Section 202(d) of the E-Gov Act, this section provides URLs for agency websites describing the actions taken by agencies in accordance with section 508 of the Rehabilitation Act of 1973, as amended by the Workforce Investment Act of 1998, Pub. L. No. 105-220.

- Internet-Based Government Services: In accordance with Section 204 of the E-Gov Act, www.USA.gov serves as an integrated internet-based system for providing the public with access to Government information and services. In accordance with Section 207(f)(3), this section provides URLs for agency activities on www.USA.gov.

- Freedom of Information Act: In accordance with Section 207(f)(1)(A)(ii) of the E-Gov Act, this section provides the URLs for agencies' FOIA websites.

- Information Resources Management Strategic Plan: In accordance with Section 207(f)(1)(A)(iv) of the E-Gov Act, this section provides the URLs for agencies' Information Resources Management strategic plans.

- Public Access to Electronic Information: In accordance with Section 207(f)(1)(B) of the E-Gov Act, this section provides URLs that contain agency customer service goals and describe activities that assist public users in providing improved access to agency websites and information, aid in the speed of retrieval and relevance of search results, and use of innovative technologies to improve customer service at lower costs.

- Research and Development (R&D): In accordance with Section 207(g) of the E-Gov Act, this section provides URLs for publicly accessible information related to R&D activities and/ the results of Federal research.

- Privacy Policy and Privacy Impact Assessments: In accordance with Section 208(b) of the E-Gov Act, this appendix provides information regarding each agency's privacy impact assessment. The IT Dashboard provides URLs for agency privacy policies and privacy impact assessments within each agency's individual E-Gov Act

Implementation Report.

APPENDIX A: ENHANCED DELIVERY OF INFORMATION AND SERVICES TO THE PUBLIC

The E-Gov Act requires OMB to oversee the implementation of a number of programs relating to capital planning and investment control for information technology; the development of enterprise architectures; information security; privacy; access to, dissemination of, and preservation of Government information; accessibility of information technology for persons with disabilities; and other areas of electronic Government.[2] The Act requires OMB to sponsor ongoing dialogue to encourage collaboration and enhance understanding of best practices and innovative approaches in acquiring, managing, and using information resources to improve the delivery of Government information and services to the public.[3] This appendix describes agency activities that enhance delivery of information and services to the public, improve or enable more data-driven decision-making in Government operations, and enhance interoperability between different public and private sector entities.

Agencies are undertaking numerous initiatives to provide the public with increased transparency and availability to Government data. For example, the U.S. Energy Information Administration within the Department of Energy (DOE) launched its U.S. Electric System Operating Data tool, which provides nearly real-time demand data, plus analysis and visualizations of hourly, daily, and weekly electricity supply and demand on a national and regional level for all of the 66 electric system balancing authorities that make up the U.S. electric grid. In a similar effort with Government climate data, Former Secretary of State Kerry, and Former Environmental Protection Agency (EPA) Administrator McCarthy announced in February 2015 a joint State Department/EPA partnership on air quality monitoring efforts at U.S. embassies overseas. Now active in more than 20 global cities, State's centralized platform leverages the expertise of the EPA for setting up the monitors, collecting and analyzing the data, and providing training and scientific exchanges.

Agencies are furthermore addressing public needs through targeted services, like those that connect recipients and providers of services. For example, the Department of Agriculture (USDA) reinvented its website strategy for USDA.gov and is currently migrating web and blog platforms to an open source content management system and enterprise shared framework. Through this migration, USDA.gov implemented a new taxonomy, information architecture, and design, as well as performed a thorough content review and user experience strategy. The U.S. Citizenship and Immigration Services (USCIS) system at the Department of Homeland Security (DHS) also leveraged technology to create multi-channel tools that give customers faster and easier access to immigration information, when and where they need it. The centerpiece of the new suite of tools is myUSCIS, an online one-stop shop for immigration information, which saw nearly 3 million sessions in its first year after it launched in December 2014.

Another agency initiative is DOI's Recreation One Stop (R1S), an interagency partnership among federal agencies to provide reservation services, shareable data, and recreation trip-planning tools for federal lands and waters across the United States.

[2] See 44 U.S.C. § 3602(e).

[3] See 44 U.S.C. § 3602(f)(9).

Currently, Recreation.gov hosts more than 3,300 individual facilities, with more than 90,000 campsites, 12 ticketed tours or events, and 26 high-demand locations accessed by permit or lottery. In 2016, there were more than 31 million sessions, 16 million visitors, and 287 million page views to Recreation.gov, which represents a 40 percent increase in visitation over 2014. In addition, the Department of Justice (DOJ) launched the Tribal Access Program for National Crime Information (TAP) in August 2015 to provide federally recognized tribes the ability to access and exchange data with national crime information databases for both civil and criminal purposes. During the course of FY 2016, nine Tribal Nation law enforcement agencies implemented the TAP solution.

Government-wide, agencies are also diversifying their information resource capabilities, with some providing data in both navigator formats and in Application Program Interfaces, and working to improve the usability of data and websites by leveraging public feedback mechanisms. The Federal Student Aid (FSA) Feedback System at the Department of Education (Education) launched a week before its July 1, 2016 deadline, and was developed to implement a state-of-the-art feedback system for customers who want to submit a complaint, report suspicious activity, or provide positive feedback concerning the student financial aid life cycle. In a similar vein, the Social Security Administration (SSA) implemented "my Social Security" in May 2012 as an online portal providing the public the ability to access personalized services and perform online transactions via a secure account. As of September 2016, over 27 million customers have registered for "my Social Security," with customers conducting nearly 122 million online transactions in FY 2016. Customer satisfaction also remains high with a rating of 89 through the ForeSee E-Government Customer Satisfaction Index. In addition, Benefits.gov, the official comprehensive benefits website of the U.S. Government, which provides information for more than 1,200 Federal and state benefit programs across 17 Federal agencies, saw nearly 9.4 million site visits, and reached at an all-time high of nearly 1 million monthly site visits in August. This year, Benefits.gov pioneered 'personalization' technology on its site, launching three new premiere site features which allow users to quickly find more benefits relevant to their situation. In FY 2016, the USAGov platform connected people with Government information more than 700 million times using websites, social media, publications, email, and phone calls through the USA.gov Contact Center.

In December 2015, the Federal Aviation Administration (FAA) worked with industry to launch a simple online tool that enables operators to register their Unmanned Aircraft System (UAS) or drones before they fly in just a few easy steps. The registry is now providing a valuable opportunity to educate hobbyists on safe flying practices, and reached over 600,000 people registering their UAS in the first year of launch. FY 2016 also marked the start of a new approach to customer service for the National Archives and Records Administration (NARA) with the launch of History Hub. History Hub offers tools like discussions boards, blogs, and community pages to bring people together around historical topics of interest. In the months since launch, there has been significant public participation with over 1,700 registered users who have posted and responded to 400 questions. Over the next two years, NARA will expand the pilot to incorporate the platform into its workflow, market it to a wider audience, and collaborate with similar organizations, such as the Library of Congress, the Smithsonian, and state and local archives.

Recently, OMB has improved the openness of data collections and agency document submissions pursuant to the Federal IT Acquisition Reform Act (FITARA),[4] OMB Memorandum M-16-19, Data Center Optimization Initiative (DCOI), and OMB Memorandum M-15-14, Management and Oversight of Federal Information Technology. As required by OMB M-15-14, agencies' FITARA Self-Assessments and Implementation Plans were required and have been drafted with input from OMB. Within 30 days of formal approval, OMB has required that the final Implementation Plan be posted publicly on each agency's [agency].gov/digitalstrategy webpages. Furthermore, all data collected pursuant to FITARA and the DCOI are required to be posted publicly at the same [agency].gov/digitalstrategy pages in machine-readable JSON format, increasing the openness of Federal FITARA implementation efforts and ability for the public to engage with the agencies about these objectives.

[4] Title VIII Subtitle D of the National Defense Authorization Act (NDAA) for Fiscal Year 2015, Pub. L. No. 113-291.

APPENDIX B: PERFORMANCE INTEGRATION

In accordance with Section 202(b) of the E-Gov Act (44 U.S.C. § 3501 note), this appendix describes what performance metrics are used and tracked for IT investments, and how these metrics support agency strategic goals and statutory mandates. Agencies describe a variety of performance metrics, including those that focus on cost and schedule of projects, risk factors, customer service, and innovative technology adoption and best practices. Select efforts are described in further detail below. The full list of activities and many of the aforementioned OMB metrics can be found on the IT Dashboard**.**

Performance metrics are an essential tool for determining the health of agencies' projects, risks, and future needs. These metrics are a product of both the project teams and agency CIOs designing and tracking performance metrics that support the strategic goals and statutory mandates of the agency. To strengthen links to departmental priorities, major IT investments are mapped to specific elements of the agencies' strategic plans and performance measures are required elements of each Business Case.

Agencies develop unique performance measures for each project in the IT portfolio, focusing on mission and business results, customer service, and improvements to business processes and technical goals for operational IT systems. Investments must contain results-specific metrics to measure the effectiveness of investments in delivering the desired service or support level. The Small Business Administration (SBA) uses its Annual Performance Report and Summary of Performance and Financial Information to report the agency's performance with respect to its mission. The SBA has linked performance goals to key stakeholders, private sector, other agencies, and internal operations through strategic goals and objectives. The Department of Veterans Affairs' (VA) FY 2016 Agency Financial Report provides information enabling the Congress, the President, and the public to assess the VA's stewardship over the financial resources entrusted to the agency and its performance as an organization. The report provides results on VA's progress towards providing America's veterans with the best in benefits and health care; a high-level summary of the VA's accomplishments during the year; a discussion of the challenges faced by the VA going forward; and an analysis of the VA's financial position.

In FY 2016, the Department of Treasury (Treasury) developed a new investment risk rating process and algorithm to apply more rigors in its review of the IT investment portfolio toward agency objectives, strategic goals, and statutory mandates to complement existing operations and performance metrics. Appropriate metrics are selected for each investment to show how they facilitate customer service, agency productivity and the adoption of innovative approaches, best practices and how they support various stakeholder groups. To strengthen the link to Treasury's priorities, major IT investments are annually mapped to specific elements of the agency strategic plan. In addition to metrics and risks tied to individual investments, Treasury monitors progress against IT Cross Agency Performance measures and reviews these quarterly at the Deputy Secretary level.

To enable decision-making, accountability, and transparency surrounding IT portfolio performance, metrics are reported to agency management, OMB, and the IT Dashboard on a regular basis. Investment performance against established goals is a key consideration for agencies in both the Capital Planning and Investment Control (CPIC) processes and in system operational analysis. In FY 2016, the CPIC process was expanded to include information security business cases. Numerous metrics applicable to PortfolioStat and TechStat sessions are enumerated in OMB M-15-14, and each of these metrics leverages the information received at least quarterly from the Federal agencies. Attachment D of OMB M-15-14 identifies 14 core metrics for PortfolioStat sessions such as, Commodity IT Spending, Potential Mobile Savings, and FedRAMP Implementation.[5] Attachment E of OMB M-15-14 provides a framework for utilization in evaluation and oversight over investments, particularly during TechStat sessions. This framework identifies and prioritizes 20 areas of any IT investment and a framework for assessing their risk and performance. These include Acquisition Flexibility, Process Governance, and agency personnel customer-centric initiatives.

[5] The full list of metrics identified in OMB's M-15-14 can be found on page 24 of that memorandum, located at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2015/m-15-14.pdf.

APPENDIX C. GOVERNMENT-PUBLIC COLLABORATION

In accordance with Section 202(e) of the E-Gov Act (44 U.S.C. § 3501 note), this appendix describes how agencies utilize technology to initiate Government-public collaboration in the development and implementation of policies and programs. They do so through a variety of approaches, including using public meetings on agency websites, engaging with the public through website comments and email lists, and using online portals to facilitate public participation in regular agency processes. Select efforts are described in further detail below. The full list of activities can be found on the IT Dashboard.

To further the implementation of the Source Code Policy, OMB launched Code.gov in November 2016. Through Code.gov, agencies can identify whether their software needs can be satisfied via an existing solution and work together to avoid wasteful spending on duplicative software. In the spirit of open source development, agencies can benefit greatly from adopting each other's approaches to open source generally. Complex topics like security, communications, and even how to run a successful hackathon are ripe for collaboration between agencies to share lessons learned and pool limited resources. In addition, members of the public can observe which agencies are participating in this initiative.

The most familiar way that agencies use technology to engage with the public is through websites and online portals. As repositories of information regarding mission, structure, and activities, these can be a valuable starting point for interested individuals. Many agencies take this one step further, using online portals to facilitate public participation in regulatory processes and other department initiatives and current events. For example, the Office of Educational Technology (OET) at Education developed a more coordinated digital engagement strategy to better engage and connect the public with the development and implementation of policies and programs. As a result, the tech.ed.gov website experienced nearly a doubling in the number of unique page views over the past year, with over 578,000 for FY 2016. In FY 2016 OET published 21 blog posts on its Medium blog which have had a combined 5,297 reads and approximately 34,500 downloads of OET publications, an increase from 10,692 in FY 2015. The OET Twitter presence has continued to grow, with the @OfficeofEdTech handle totaling 119,000 followers. OET leveraged this coordinated strategy with the launch of the 2016 National Education Technology Plan (NETP), with over 18,776 downloads and over 129,000 unique views of the HTML NETP pages on tech.ed.gov since its launch in December 2015.

At DHS, the Science and Technology Directorate (S&T) uses Ideascale, a crowd-sourcing collaboration platform, to host the National Conversation on Homeland Security Technology. The National Conversation focuses on issues related to homeland security capabilities, striving to bring together entire stakeholder communities to address challenges, capability gaps, emerging threats and more. Over the past year, S&T hosted conversations on ways to transform airport borders, developing a trusted cyber future, improving mass transit security, the responder of the future, bio/agro security innovation, enabling the decision maker, improving resilience and screening at speed. More than 1,500 public safety, homeland security, and emergency management stakeholders representing Government, academia, and non-profit organizations participated in those conversations.

The Department of Transportation (DOT) continues to use web-based interactive technology to engage the public on important policy matters. During FY 2016, DOT leveraged online dialogues to discuss matters including best practices in transit procurement in April 2016, as well as preventing transit worker assault in June 2016. These dialogues engaged hundreds of people, resulting in roughly 270 ideas, 300 comments on those ideas and over 2,000 votes on those ideas. The results of these online dialogues inform policies and reforms at the Federal Transit Administration and other DOT operating administrations.

Collaboration with the public, however, extends beyond making resources available to determining how they can be utilized. Agencies have held “datapaloozas,” hackathons, data jams, grand challenges, and apps challenges as collaborative Government-public efforts in an effort to demonstrate the value that can be achieved by making agency program data available to and usable by the public.

On May 23, 2016, DOE announced the U.S.-Israel Integrated Energy and Desalination Design Challenge, developed jointly by U.S. and Israeli experts. Through this challenge, DOE and Israel's Ministry of National Infrastructure, Energy and Water Resources (MIEW) encouraged leading engineers in the U.S. and Israel to design a novel integrated energy and desalinization system that could be suitable for both countries. The challenge sought desalination systems that can flexibly balance their input and output flows of water, electricity, and wastes as required by water demand, electricity system services, and environmental goals. There was discussion for a joint U.S. and Israeli workshop in early 2017, where the U.S. and Israeli Challenge winners will be selected.

On June 30, 2016, DOJ organized a live Community Policing Town Hall with Former Attorney General Loretta E. Lynch on Facebook *Live* at Facebook's Playa Vista Campus. The town hall was live-streamed and moderated by actor Michael B. Jordan, with participation from actress Yara Shahidi. The town hall audience consisted of local high school juniors, seniors, college students and Los Angeles Policy Department (LAPD) “cadets” – young people who volunteer to work at the LAPD – and 15 officers from the Hollenbeck Police Activities League and Los Angeles Sheriff Department. This conversation style town hall marked the final stop on the Attorney General’s 12-city Community Policing Tour and highlighted the social media and technology pillar of former President Obama's Task Force on 21st Century Policing final report.

In an effort to combat workplace hearing loss, the Occupational Safety and Health Administration (OSHA) recently partnered with other agencies to offer a challenge to inventors and entrepreneurs: help develop a technological solution to workplace noise exposure and related hearing loss. Every year 22 million workers are at risk of losing their hearing from workplace noise hazards, resulting in hearing loss disability costs of an estimated $242 million annually in workers’ compensation. As a result, OSHA and the Mine Safety and Health Administration (MSHA), in partnership with the National Institute for Occupational Safety and Health (NIOSH), launched the "Hear and Now – Noise Safety Challenge." The competition was open to the general public. The ten finalists appeared in Washington, D.C., to pitch their ideas to a panel of judges that include investors and representatives of NIOSH and the U.S Patent and Trademark Office.

The National Aeronautics and Space Administration (NASA) also actively engaged the public, with initiatives like the International Space Apps Challenge, a two-day innovation incubator where teams of technologists, scientists, designers, artists, educators, entrepreneurs, developers, and students across the globe collaborate and engage with NASA's publicly available data, models, and tools to design innovative open source solutions to global challenges. In 2016, more than 15,000 citizens in 161 cities from 61 countries engaged with NASA's open data to create 1300 innovative projects. NASA's Data Bootcamp model, created as an outgrowth of our focus in engaging more women in data, was used in 54 locations with 5700 participants around the world. Data Bootcamp introduces entry-level content on coding, making, dataset retrieval and manipulation, problem solving, and storytelling through panel discussions and hands-on workshops.

The Department of Justice has a very strong web presence that helps foster Government-public collaboration in the Government's administration of the Freedom of Information Act (FOIA). The Department of Justice's Office of Information Policy is responsible for encouraging Government-wide compliance with the FOIA. Through its blog, *FOIA Post,* the Department's Office of Information Policy (OIP) keeps both the public and agencies informed of key developments in the FOIA, including issuance of new FOIA policy guidance and opportunities for public engagement such as its Best Practices Workshops. For example, on December 9, of 2016, OIP made a blog posting requesting public comment on a proposed policy that would institute a presumption for FOIA released records being posted online so that they are available to the general public as well as the individual requester. The Department utilized regulations.gov to receive comments from the public, and in addition to *FOIA Post*, utilized Twitter and targeted e-mails to socialize the request for comments.

To help with the development of its fourth Open Government in FY 2016, NARA created a robust dialog and consultation process with the public. Internal and external engagement efforts brought in more than 180 discrete ideas, suggestions, and proposals for strengthening open Government at NARA. During Sunshine Week in March 2016, NARA's external engagement kicked off with blog posts on the NARAtions Blog, NDC Blog, Records Express, the FOIA Ombudsman, and social media posts on Facebook and Twitter. The Open Government Team at NARA also monitored ideas and comments submitted on the Open Government space on the History Hub site. The Archivist and Senior Executives also held their first Open Government webinar with an overview and presentations, and feedback from the public. NARA published its plan in September 2016, utilizing Github and making the source code to the plan publicly available.

On September 28, 2016, the National Science Foundation (NSF) announced $10 million in awards to 10 "Big Data Spokes" projects to initiate research on specific topics identified by the Big Data Regional Innovation Hubs (BD Hubs). Project topics ranged from precision agriculture to personalized education. The data spokes reflect the unique priorities and capabilities of the four BD Hubs, which represent consortia from the Midwest, Northeast, South and West of the country. An example of the types of activities the awards will support includes an effort, led by a team from the Massachusetts Institute of Technology (MIT), Brown University, and Drexel University, to develop a data licensing approach and automated platform that will allow individuals and organizations to share data.

At the beginning of August 2016, the U.S. Agency for International Development's (USAID) Global Development Lab announced $10 million for 49 new research projects that will address evidence gaps and advance technical capacity in critical areas of development. Spanning 23 USAID partner countries, the 49 new projects are funded through the Partnerships for Enhanced Engagement in Research (PEER) program, an initiative designed to foster collaborative global research. Through the PEER program, USAID supports the public in developing countries working in partnership with U.S. Government-funded researchers. These new awards will allow public-private collaboration on a variety of crucial research areas, such as wildlife protection, biodiversity conservation, water resource sustainability, satellite monitoring of natural resources, fisheries management, food security, disaster mitigation, and other areas.

APPENDIX D. CREDENTIALING

Section 203 of the E-Gov Act (44 U.S.C. § 3501 note) requires the Federal Government to describe current activities agencies are undertaking to achieve the interoperable implementation of electronic credential authentication for transactions with the Federal Government. This appendix describes select agency approaches to improving credentialing. The full list of activities can be found on the IT Dashboard.

Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors (HSPD-12) is the Federal directive that requires the use of secure credentialing capabilities in order to gain logistical and physical access into agency networks and facilities. The goal of HSPD-12 is to ensure that only authorized personnel are accessing Federal systems and information, and the necessity of this capability was reaffirmed when strong authentication was designated by the Administration as an essential component of the Cybersecurity Cross Agency Priority (CAP) Goal. The Government has sought to implement HSPD-12 through the issuance of Personal Identity Verification (PIV) cards. The establishment of the PIV credential as part of a broader enterprise solution enables common service capabilities in secure and reliable transactions.

Many Federal agencies have made significant progress in implementing HSPD-12 and adopting the use of PIV cards. For example, USDA completed a successful pilot of Derived PIV credentials for mobile devices. This solution will ultimately enable secure the use of secure interoperable HSPD-12 compliant credentials for use on USDA's expanding mobile computing infrastructure and helps to eliminate technical barriers to full PIV adoption within USDA. HHS also made progress in PIV adoption, issuing 123,779 PIV cards to staff out of the total eligible population of 129,271 for an adoption rate of 96%. Currently 99% of non-privileged users are required to use their PIV card to login to HHS networks; 88% of the staff must use the PIV to gain access to the network remotely.

Several other agencies also achieved substantial progress in PIV card adoption. This year, NSF made significant progress towards meeting OMB's targets for smart card enforcement with 87% of the user community currently using their smart card to login to the laptop/desktop to get into the NSF network. SBA has also achieved two factor authentication through 100% PIV implementation and enforcement including 99% enforcement for unprivileged network users. In FY 2016 DHS sustained its forward momentum on strong electronic credentialing, and continued work to close the remaining gaps ahead of the 100% compliance goal for mandatory authentication to networks using PIV cards for both privileged and unprivileged users. As of September 28, 2016, DHS as a whole achieved 99% compliance for both user groups, an increase of 4% increase from FY 2015. Mandatory PIV authentication for remote access users also increased to 77% from 74% in FY 2015.

DOI's Identity, Credential, and Access Management (ICAM) program manages over 80,000 PIV credentials in the DOIAccess identity and credential management system, which interfaces with the GSA USAccess Shared Service to assure compliance with HSPD-12 goals and standards. This year, DOI implemented the capability to automatically disable accounts when the employment status in DOIAccess or FPPS is suspended or terminated, ensuring access to the DOI network and integrated applications is quickly and effectively disabled. In addition, the DOIAccess system produces a Separations Report that system owners can use to manage access lists. In 2016, DOI also enforced PIV authentication to its cloud-based, enterprise email system, BisonConnect. In addition, DOI issued a Strong Authentication Exception policy to ensure PIV exceptions are issued consistently across DOI, and for limited durations (24 hours to 7 days). DOI also set the goal to have the total number of PIV exceptions in place be less than 3% of the population.

DOT continued its implementation and integration of capabilities to fully support Federally-issued and approved credentials meeting the FIPS-201 standard. In FY 2017 DOT plans to expand use of existing strong authentication and federation services to "PIV enable" more DOT mission applications, to make mandatory PIV usage required for remote access to DOT networks, to begin integration of CDM-specified identity management capabilities, and to begin leveraging GSA's Login.gov service offering for authentication to public-facing sites and applications. The Department currently has more than 97% of its employees using their PIV cards on a required basis to access DOT networks, and 100% of privileged network account holders are required to use their PIV cards to access their privileged accounts.

Recognizing the business need for identity federation and also the potential gaps in current policy/process, NASA's Identity, Credential, and Access Management (ICAM) team completed the Active Directory Federation Services (ADFS) effort in 2016. In addition the Federation business case have been drafted to support Federal Government agencies, academia, commercial, and international partners. The first of three agreements to obtain an identity broker service will be complete in December 2016.

While the basic level of compliance sought by HSPD-12 is to require PIV card use for access to facilities and systems, PIV cards may also be used to facilitate electronic signature and electronic authorization by high-level agency officials. At the end of FY 2016, GSA IT funded the second year of effort to establish an Electronic Signatures standard and solution across respective GSA applications. This solution will offer differentiated levels of credentialing and authentication in order to achieve interoperability with the identified applications across the Government and the public. GSA IT has a phased approach to introduce digital signatures to user groups across the enterprise. Furthermore, GSA is working on publishing APIs that will enable GSA applications to incorporate digital signing as part of their business process, and are developing a seamless integration with our Enterprise Document Management System (EDMS). The Electronic Signatures application will also have significant impact on other agency operations, such as the Office of the Federal Register (OFR) at the Federal Register, which is a part of NARA. In FY 2016, OFR increased the number of agencies submitting documents electronically by 14 percent as a result of ongoing efforts to promote use of the PKI capability and the *Federal Register*'s redesigned web portal, which facilitates the authentication and verification of both documents and user credentials and provides new tools for both users and administrators to identify and correct problem submissions.

Lastly, the Cybersecurity Action Plan (CNAP) was launched in February 2016. Specifically, OMB, on the heels of its October 2015 release of OMB Memorandum M-16-04, Cybersecurity Strategy Implementation Plan (CSIP) for the Federal Civilian Government, has taken steps to ensure that agencies not only have access to, but are actively integrating into their standard operating procedures, the tools, techniques, and best practices that have been identified as those most effective for the strengthening of their respective cybersecurity postures.

Noteworthy progress in FY 2016 included the development and continued implementation of OMB Memorandum M-16-15, Federal Cybersecurity Workforce Strategy, the revision of OMB Circular A-130, Managing Information as a Strategic Resource, and the creation of the Federal Chief Information Security Officer (CISO) position. In addition to these activities, OMB Cyber continued to work with agencies to increase their performance on the Cybersecurity Cross-Agency Priority (CAP) Goals and to provide support, guidance, and accountability Government-wide so that Federal agencies may be optimally positioned for a secure, connected future.

APPENDIX E. E-RULEMAKING

One of the goals of the E-Gov Act (44 U.S.C. § 3501 note) is to assist the public, including the regulatory community, in obtaining access and electronically submitting comments on rulemakings by Federal agencies. Specifically, Section 206 of the E-Gov Act lays out requirements designed to not only increase engagement with the public, but to increase collaboration between Government agencies. This appendix describes the general efforts being undertaken by the Federal Government to utilize online electronic regulatory docket capabilities, specifically the usage of www.Regulations.gov (Regulations.gov) and the Federal Docket Management System (FDMS) at www.FDMS.gov. The full list of activities can be found on the IT Dashboard.

The central eRulemaking tool for Federal agencies is Regulations.gov. Launched in 2003, the website provides agencies with a platform to post final rules, proposed rules, requests for information, and other public documents in order to give the public an opportunity to review and comment on regulatory actions. Use of the commenting feature on FederalRegister.gov more than quadrupled in FY 2016 from the previous year to a total of more than 74,000 comments submitted to agencies through FederalRegister.gov. This feature is also integrated with existing MyFR and social media capabilities on the website. The eRulemaking Program Management Office is hosted by the EPA. In FY 2016, there were more than 4,800,000 visits and over 880,000 comments received via Regulations.gov. The eRulemaking program offers an application programming interface (API) which connects outside applications to FDMS so interested individuals can both read regulatory information and write comments to be processed through FDMS. In FY 2016, there were over 85,000 comments received through the API. On the EPA user side, the EPA Docket Center processed over 1300 Federal Register documents and received nearly 3.5 million comments in FY 2016 by way of postal mail, e-mail, fax, Regulations.gov and other media. USAID annually transfers funds to EPA that reflect AID's service fee for the implementation, use, and the operation and management of FDMS. Access to and use of FDMS is granted to USAID, along with all other Federal agencies and the general public. In FY 2016, OPM posted 20 final rules, 15 proposed rules, and 92 notices on Regulations.gov. Overall, OPM has posted 416 rules and proposed rules and 885 Federal Register notices in Regulations.gov. OPM also uses the FDMS system to receive public comments on every rule that is published and open for comment.

Many Federal agencies have used the system to great effect, posting large amounts of content and receiving tremendous input from the public on proposed regulatory action. During FY 2016, DHS posted 72,795 documents to Regulations.gov including agency rules, notices, supporting documentation and public comments. In addition, DOI posted 304 final and proposed rules, 136 Federal Register notices, and 66,431 public comments in Regulations.gov. DOI has 654,171 documents stored in FDMS.gov that are available to the public via Regulations.gov. The Department of Labor (DOL) also posted 99 final and proposed rules, 418 Federal Register notices, and 8,698 documents in Regulations.gov in FY 2016. DOL had 170 staff using FDMS.gov and created 19 rulemaking dockets. DOL has received 6,888 public comments via Regulations.gov that are directly stored in FDMS. For nearly a decade, Treasury has been participating in Regulations.Gov, and has numerous proposed and interim rules and other materials posted for public comment and review on the eRulemaking site. In FY 2016, Treasury posted more than 42,000 public comments received in response to requests for comments on 100 notices of proposed rulemaking and other documents. In FY 2016, USDA posted 340 rules and proposed rules, 836 Federal Register notices, and 54,633 public submissions via Regulations.gov. NSF typically publishes only one to three proposed regulations per year, and in FY 2016 NSF published one final rule and one interim final rule.

While agency use of Regulations.gov has increased the public's access to the Federal regulatory processes and allowed for greater participation in agency rulemaking, some agencies have taken the extra step of integrating other online tools to facilitate public engagement. For example, HHS maintains a 'one-stop' web page to find the Department's regulations, HHS.gov/regulations, which directs visitors to more information about the Department's significant regulatory activities. Other divisions of the Department have followed the Department's lead including the Centers for Disease Control and Prevention (http://www.cdc.gov/regulations/), the National Institutes of Health (https://oma.od.nih.gov/DMS/Pages/Regulations.aspx), and the Food and Drug Administration (http://www.fda.gov/RegulatoryInformation/RulesRegulations/). The Department continues to explore innovative ways it can make finding, understanding, and commenting on regulations user friendly."

Social media can also be a useful tool to engage the public. For example, the Department of State announces all rulemakings published in the Federal Register, on Twitter at its department regulations account, @DOSRegs, and currently has over 650 followers.

While technology has been important in engaging the public in the Federal rulemaking process, it has also been fundamental in promoting back-end functionality to help Government units to manage their various regulatory actions. FDMS is a Government-wide system that provides agencies the ability to search, view, download, and review comments on rulemaking and non-rulemaking initiatives. FDMS also enables agency users to manage docket materials through the use of role-based access controls, workflow and collaboration processes, and comment management tools. Many departments and agencies have extensively used these tools to facilitate their regulatory activities. DOI had 159 staff using FDMS.gov and created 112 regulatory dockets for new regulatory actions published in FY 2016. Overall, USDA provides the public access to 428,719 documents in Regulations.gov. USDA had 250 staff using FDMS.gov and created 94 regulatory dockets in FDMS for regulatory actions published in FY 2016. Education continues its use of regulations.gov and FDMS to conduct its rule makings. In FY 16, 53 rules (proposed and final) were published using these websites. Education also takes comments through these websites, and in addition to the 53 proposed and final rules, took comments on 201 notices during this time period. In FY16, 40 unique FDMS users at DOE posted 157 rules and proposed rules, 376 Federal Register notices, and created 11 dockets. DOE received 998 public comments on these actions. In FY 2016, DOJ created 34 regulatory dockets in FDMS for new regulatory actions published. DOJ posted a total of 78 rules and proposed rules with associated documents agency and received 971 public comments via Regulations.gov that are directly stored in FDMS and are available to the public online. During FY 2016, SBA created 11 rulemaking dockets and one docket for a notice seeking comments through FDMS for inclusion on regulations.gov. Each of the rulemaking dockets generated an average of 46 comments per docket.

APPENDIX F. NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (NARA) RECORDKEEPING

Sections 207 (e) of the E-Gov Act (44 U.S.C. § 3501 note) requires agencies to adopt policies and procedures to ensure that chapters 21, 25, 27, 29, and 31 of title 44, United States Code, are applied effectively and comprehensively to Government information on the Internet and to other electronic records. Agencies describe to OMB their adherence to NARA recordkeeping policies and procedures for electronic information online and other electronic records. The full list of activities can be found on the IT Dashboard.

NARA's Corporate Records Management Program adheres to Federal laws and regulations when implementing internal policies and procedures for NARA's own electronic records and systems. The Corporate Records Management staff ensures records management requirements are incorporated into the planning, design, development, and implementation of new information systems, including the disposition of data. Of the 33 major NARA IT systems, 19 are scheduled, and 14 are currently unscheduled mainly due to the original retention schedule for the content only covering paper records. NARA will be addressing those unscheduled systems as part of a larger project to revise schedules based on function and not format or office. In addition, there are six administrative systems (such as procurement, personnel/payroll, accounting, timekeeping, and travel management) that are covered by NARA’s General Records Schedules (GRS), as well as email records being covered by GRS 6.1.

Some agencies have sought to comply with the recordkeeping requirement by utilizing NARA-developed tools and methods to facilitate compliance with the E-Gov Act. For example, many Department of Defense (DOD) components decided in 2016 to adopt the NARA Capstone approach for managing email records. In FY 2016, the DOJ continued to follow its ongoing practice of scheduling electronic records that contain Federal records. The Department does not yet have the full FY 2016 numbers as that information is developed as part of the NARA Records Management Self -Assessment Process, which has been delayed until winter 2017. HHS uses NARA’s GRS whenever feasible, communicating its records management policies and practices on its Agency Internet website. For records the GRS do not address, HHS submits unique records schedules for NARA approval. HHS is currently revising its Email Retention Policy to capture the new NARA retention guidance and recommendations (*i.e.*, Capstone Approach).

The State Department (State) continued to adhere to its NARA-approved plan for all IT systems, as well as expanded the inventory of electronic information systems to address compliance and records management requirements. State scheduled two new IT systems and had six schedules pending for IT systems in FY 2016. Likewise, DOT maintains its records inventory through regular review and close coordination with NARA. Currently, DOT has approximately 500 electronic records sets scheduled with NARA and nearly 135 for which schedules have been submitted but not yet approved. To improve management of email records across the agency, Treasury is implementing NARA's Capstone approach to meet Government-wide email management requirements, with anticipated completion by December 31, 2016. Treasury has provided public access to the information that identifies the disposition authorities for the 1,267 records control schedules. Additionally, during FY 2016 EPA received approval from NARA for one revised and one new records schedules for major electronic information systems. Sixteen transfers for data from permanent electronic information systems were sent to the National Archives. Five more of EPA's new 21 consolidated schedules submitted to NARA in 2012-2013 were approved, bringing the total approved to 20.

NSF uses the Electronic Records Archives (ERA) to transfer eligible permanent electronic records to NARA. The Official Electronic Award Record Archival project, completed in February 2016, ensures NSF is compliant with NSF Bulletin 09-2. NSF did not transfer electronic records under the agency's NARA approved record schedule (N1-307-88-2) during FY16, but does have 476 Award Records pending approval for submission. NSF implemented Documentum, an Electronic Records Management System (ERMS). At the present time, there are 84 USAID electronic records that have been scheduled with NARA according to the National Archive Records as of the beginning of October 2016.

Other agencies have developed their own systems and processes to comply with NARA recordkeeping requirements. For example, DOI established the electronic eMail Enterprise Records and Document Management System (eERDMS) program to move the agency toward an integrated electronic enterprise recordkeeping system. The eERDMS program consists of the multiple sub-component systems which include: Enterprise Forms System (EFS), Enterprise eArchive System (EES), Enterprise Dashboard System (EDS) and Enterprise Content System (ECS). DOI has identified 282 electronic systems as of FY 2017 potentially eligible for an integrated enterprise management.

APPENDIX G. PRIVACY POLICY AND PRIVACY IMPACT ASSESSMENTS

Section 208(b) of the E-Gov Act (44 U.S.C. § 3501 note) requires agencies to conduct a privacy impact assessment before (1) developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public, or (2) initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for 10 or more persons. In addition, and if practicable the E-Gov Act requires that agencies make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means. This appendix provides a high-level summary of agencies' implementation of the privacy provisions of the E-Gov Act and information regarding select agencies' work in this area. The full list of activities can be found on the IT Dashboard.

In FY 2016, 24 CFO Act agencies and 51 non-CFO Act agencies reported to OMB performance measures implementing the privacy provisions of the E-Gov Act. The goal for the Federal Government is for 100 percent of applicable IT systems to be covered by up-to-date PIAs.[6] In FY 2016, 77 percent of applicable IT systems reported by CFO Act agencies and 85 percent of applicable IT systems reported by non-CFO Act agencies had up-to-date PIAs. The 77 percent figure reported by CFO Act agencies represents a decrease in the compliance rate compared to previous years. In contrast, the 85 percent figure reported by non-CFO Act agencies is the same as the compliance rate from FY 2015.

On November 8, 2016, OMB issued OMB M-17-06, Policies for Federal Agency Public Websites and Digital Services. Section 6 of the Memorandum, Protect Privacy, requires agencies to maintain a central resource page dedicated to its privacy program. In addition to various other requirements, each agency's privacy program page is required to list and provide links to the agency's privacy impact assessments. In its FY 2017 report, OMB plans to provide information regarding agencies' compliance with the new guidance and URL's for agency privacy program pages.

Table 1: **CFO Act Agencies' Section 208(b) Performance Measures**

Key Privacy Performance Measures – CFO Act Agencies	**FY 2014**	**FY 2015**	**FY 2016**
Number of systems containing information in identifiable form	4,406	4,601	4,356
Number of systems requiring a PIA	2,701	2,940	3,128
Number of systems with a PIA	2,564	2,428	2,409
Percentage of systems with a PIA	95%	83%	77%

Source: Data reported to DHS via CyberScope and provided to the Office of Information and Regulatory Affairs (OIRA) from October 1, 2015, to September 30, 2016.

[6] In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks. (See OMB M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002).

Table 2: **Non-CFO Act Agencies' Section 208(b) Performance Measures**

Key Privacy Performance Measures – Non-CFO Act Agencies	**FY 2014**	**FY 2015**	**FY 2016**
Number of systems containing information in identifiable form	758	745	621
Number of systems requiring a PIA	529	540	665
Number of systems with a PIA	436	457	563
Percentage of systems with a PIA	82%	85%	85%

Source: Data reported to DHS via CyberScope and provided to the Office of Information and Regulatory Affairs (OIRA) from October 1, 2015, to September 30, 2016.

Select Agency Highlights for FY 2016

In FY 2016, Treasury piloted the use of an updated Privacy and Civil Liberties Impact Assessments (PCLIA). Treasury is committed to protecting the privacy and civil liberties of individuals in all agency programs. Section 522 of the Consolidated Appropriations Act of 2005 requires Treasury to appoint a Chief Privacy Officer to assume primary responsibility for privacy and data protection policy. Similarly, Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007 requires the Treasury to appoint a senior officer to serve as its Privacy and Civil Liberties Officer. Consistent with these requirements, Treasury Directive 25-09, Privacy and Civil Liberties Activities Pursuant to Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (TD 25-09), assigns these responsibilities to the Treasury Chief Privacy and Civil Liberties Officer (CPCLO). Treasury has updated the PIA process to include an assessment of civil liberties risks associated with the collection and maintenance of personally identifiable information. The Department's current guidance for conducting PIAs is provided in Treasury Directive (TD) 25-07, Privacy Impact Assessment.

In FY 2016, OPM revised its internal policies on conducting PIAs. The relevant OPM policies are described in OPM's Information Security and Privacy Handbook, the PIA Guide, and the PIA template. These were issued by OPM's Office of the Chief Information Officer, which, until the beginning of FY 2017, was also the designated Senior Agency Official for Privacy (SAOP). OPM policies are intended to ensure consistent documentation of all IT systems and projects that collect, use, or maintain PII to support the activities of the agency. The PIA Guide requires system owners to complete a Privacy Threshold Analysis, which is used to determine whether a new or updated PIA is required for a particular IT system or project. For those IT systems and projects that require a PIA, the PIA template requires detailed documentation and analysis concerning all aspects of the IT system or project, including the purpose, the PII that is used, collected, disseminated, or maintained, and the associated privacy risks and the steps taken to mitigate those risks. All PIAs are reviewed and approved by the system owner, the CIO and, beginning in FY 2017, the Chief Privacy Officer.

APPENDIX H. AGENCY IT TRAINING PROGRAMS

Section 209(b)(2) of the E-Gov Act (44 U.S.C. § 3501 note) requires agencies to establish and operate IT training programs. The Act states that such programs shall have curricula covering a broad range of information technology disciplines corresponding to the specific information technology and information resource management needs of the agency involved; be developed and applied according to rigorous standards; and be designed to maximize efficiency, through the use of self-paced courses, online courses, on-the-job training, and the use of remote instructors, wherever such features can be applied without reducing the effectiveness of the training or negatively impacting academic standards. This appendix describes select agency training programs for IT workforce. The full list of activities can be found on the IT Dashboard.

USDA offers a large variety of self-paced courses focused on multiple IT disciplines available to all IT Federal employees 24/7 through USDA's learning management system, *AgLearn*. With the collaboration of representatives from USDA agencies and staff offices, the IT Workforce organization developed an USDA IT competency model that was accepted department-wide and launched in the AgLearn system, for department use. USDA also has its premier leadership development initiative, the IT Fellows Program, which is open to IT employees, GS levels 12 – 15, department-wide. Program components include classroom leadership training and assessments; benchmarks with successful organizations and senior Federal and private leaders; a 120 day rotational assignment; and at least one action learning project. USDA continues to offer a department-wide Federal Acquisition Certification (FAC) Program/Project Manager (P/PM) training program. The department has coordinated with selected vendors to offer four (4) in-person classroom courses and 15 online courses (covering Levels 1, 2, and 3), with 31 courses offered in total.

In FY 2016, the Office of Management at Education continued efforts to deliver training and development opportunities to a more mobile workforce. Employees were provided access to virtual books on a wide range of relevant topics: IT Security; project management; databases; operating systems; and networking. To enhance training efforts with remote staff, ED continued to use WebEx and remote presence software (video/audio broadcast). Also, the IT Security Role Base Training was modified to allow IT professionals to select courses more directly related to their duties. IT Security Role Based Training was assigned to 1,218 employees and 100% of the employees completed it. Cybersecurity and Privacy Awareness training was required of all ED employees and 100% of employees completed this training.

In FY 2016, DOD validated the DOD Cyber Workforce Framework (DCWF) and associated work roles, and coordinated integration of the DCWF into NIST Special Publication 800-181through collaboration with the DHS and NIST. Internally, DOD conducted a review of DCWF information technology (IT) and acquisition work roles to identify additional cybersecurity training requirements in support of the DOD Cybersecurity Culture and Compliance Initiative. Work also commenced on defining qualification standards that will be used to develop updated training and credentialing requirements for all IT, cybersecurity, cyberspace effects and cyber-related intelligence work roles. All of these efforts will be used to enhance current cyber training initiatives including technical schoolhouse offerings, online training, and graduate-level education programs. The DOD continues to offer a variety of Privacy Act (PA) training courses including a privacy general awareness course, 3-day PA Compliance & Management courses; System of Records Notice and Breach Management training workshops; and a PA Essentials course.

In FY 2016, DOI conducted an initial analysis of the IT workforce that identified the major duties of IT positions throughout DOI and a comprehensive view of the IT work performed across the Department. Under the Department's implementation of the Federal IT Reform Act (FITARA), every bureau completed an assessment of their IT workforce. DOI is working across its bureaus to standardize position descriptions for IT job series and implement them consistently across the agency. This work will contribute to an overarching DOI IT workforce plan that will include more targeted training and development opportunities for employees based on skills gaps we see in the IT workforce.

DOJ's IT workforce training program in FY 2016 continued its efforts to bring together stakeholders from across organizational lines, to coordinate and scale training initiatives. Efforts to train the IT workforce have fostered a learning community, to share ideas and insights that benefit the entire department. A notable new initiative in 2016 was the DOJ IT Flash Mentoring event series, which brought IT professionals from across DOJ together with DOJ's IT leaders for roundtable discussions and advice on IT-related issues. A new agency training course on IT leadership and management was created this year and is scheduled to run in January 2017. DOJ’s enterprise Learning Management System (LearnDOJ) was upgraded and successfully deployed, enhancing user experience and providing employees with better access to training information and materials.

State’s Foreign Service Institute (FSI) School of Applied Information Technology (SAIT) provides IT, cybersecurity, knowledge management, records management and data privacy training to all systems administrators, IT Specialists, and domestic and overseas technology users to State and 47 other customer agencies. In FY16 SAIT implemented an ISO 9001 certified Quality Management System to ensure that IT curriculum is continuously reviewed and improved. SAIT’s Training Advisory Committee holds monthly meetings with stakeholders to ensure competencies for the IT workforce are covered. SAIT uses both classroom and blended virtual training platforms to bring training to the Department’s 110,000 employees in 260 locations around the world. IT professional tradecraft courses utilize seminars, work group discussions, and real-world experiences, allowing students to gain an overview of what is required of entry, mid and senior levels of IT responsibility and give IT professionals the skills to excel with today’s and tomorrow’s technology. In FY 2016, there were over 60,000 classroom courses were taken totaling about 3.2 million hours of training. Additionally, FSI has produced over 280 distance learning courses for U.S. foreign affairs professionals which were completed over 150,000 times in FY 2016, plus over 18,500 commercial course completions.

In 2011, EPA launched an agency-wide IT training program to provide employees with the necessary training to do their jobs successfully. EPA expanded the eLearning (SkillPort) Learning Management System from 5,000 licenses to over 17,000 for implementation as an enterprise tool. The EPA also developed an on-line training module for key privacy personnel, which was launched in Q2 FY 2016 on the eLearning site. The annual mandatory security awareness training taken by all employees and others with access to EPA systems also includes a privacy component. In FY 2016, the EPA also introduced an improved security role-based training which includes a credentialing program for employees with significant security responsibilities. Current and newly hired Information Security Officers have a time limit to complete the program. In addition, as part of EPA's FITARA implementation plan, the agency introduced an Innovation Fellowship program to bring an influx of high technology expertise to the agency.

GSA's IT Training Program is an enterprise-wide training curriculum provided by the CIO's team to help GSA's 17,000+ staff learn how to use hardware and software, complete mandatory courses, and improve their technical skills in various ways. In FY 2016, 84 instructor-led IT training events were created and delivered. Additional IT training is available through videos, user guides, presentations, and other instructional materials provided on the IT self-help internal website. GSA also developed customized technology training, created specific course materials to meet employee needs, and updated mandatory agency-wide IT training within our online training system.

In FY 2016, NARA revamped its Tier I Computer Based Training to better address emerging threats. The agency continued the development of a multi-level Tier II training program for users with elevated security responsibilities and other staff involved in risk management activities. Classroom instructions, along with on-site delivery of awareness training, have been scheduled and will be offered in the FY 2017 training cycle.

OPM offers wide range of IT courses via the OPM Learning Connection, which makes available over 300 IT-related courses, with 264 courses throughout FY 2016. The total number of completed courses in the IT-related area for FY 2016 was 1079 – a 234% increase over FY 2015. Among these training instances were 279 involving the Microsoft Office Suite, while Security, malicious code prevention, and privacy learning instances totaled 176. All OPM employees completed required IT Security Awareness Training. The Office of CIO acquired training classes in FY 2016 for OPM staff on the Information Technology Infrastructure Library (ITIL) Foundation framework. The ITIL framework is designed to standardize the selection, planning, delivery and support of IT services within OPM thus aligning the IT services with agency needs. Class attendees were required to take and pass an ITIL Foundation certification test in order demonstrate that they understood the ITIL Foundation concepts. The Office of CIO acquired the following Agile training classes in FY 2016 for OPM staff: "Agile and Scrum in a Day" and "Certified Scrum Product Owner." These Scrum classes provide the foundation for OPM staff in understanding and putting into practice the Agile Scrum process from the perspective of the OPM Program Office organization responsibilities.

APPENDIX I. CROSSWALK OF E-GOV ACT REPORTING REQUIREMENTS

E-Government Act of 2002 Requirement	Location in E-Government Act Report to Congress
Sec. 101 (44 U.S.C. § 3606) – Provide a description of projects receiving E-Gov Funds in FY 2016, including funding allocations and results achieved.	Section I – E-Government Fund
Sec. 209 (44 U.S.C. § 3501 note) – Provide a summary of activities related to IT workforce policies, evaluation, training, and competency assessments.	Section II – Government-wide IT Workforce and Training Policies
Sec. 214 (44 U.S.C. § 3501 note) – Provide a summary of how IT is used to further the goal of maximizing the utility of IT in disaster management.	Section III – Disaster Preparedness
Sec. 216 (44 U.S.C. § 3501 note) – Provide a summary of activities on geographic information systems and initiatives, and an overview of the Geospatial Platform.	Section IV – Geospatial
Sec. 101 (44 U.S.C. § 3602(f)(9)) – Sponsor ongoing dialogue to encourage collaboration and enhance understanding of best practices and innovative approaches in acquiring, managing, and using information resources to improve the delivery of Government information and services to the public.	Appendix A - Enhanced Delivery of Information and Services to the Public
Sec. 202(b) (44 U.S.C. § 3501 note) – Develop performance measures.	Appendix B – Performance Integration
Sec. 202(d) (44 U.S.C. § 3501 note) – Ensure comparable accessibility to people with disabilities.	IT Dashboard
Sec. 202(e) (44 U.S.C. § 3501 note) – Engage the public in development and implementation of policies.	Appendix C – Government-Public Collaboration

E-Government Act of 2002 Requirement	Location in E-Government Act Report to Congress
Sec. 203 (44 U.S.C. § 3501 note) – Implement electronic signatures.	Appendix D – Credentialing
Sec. 204 (44 U.S.C. § 3501 note) – Oversee the development of a Federal Internet Portal.	IT Dashboard
Sec. 206 (44 U.S.C. § 3501 note) – Report to Congress agency compliance with electronic dockets for regulatory agencies. Ensure public websites contain electronic dockets for rulemaking.	Appendix E – E-Rulemaking
Sec. 207 (e) (44 U.S.C. § 3501 note) – Report on agency compliance with policies pertain to the organization and categorization of Government information, and agency compliance with establishing policies and procedures regarding recordkeeping.	Appendix F – National Archives Records Administration Recordkeeping
Sec. 207(f)(1)A(ii) (44 U.S.C. § 3501 note) – Report on agency compliance with requirements to make information available to the public under the Freedom of Information Act.	IT Dashboard
Sec. 207(f)(1)(A)(iv) (44 U.S.C. § 3501 note) – Report on agency compliance with requirements to provide an information resources strategic plan.	IT Dashboard
Sec. 207(f)(1)(B) (44 U.S.C. § 3501 note) – Report on agency compliance with developing goals to assist the public with navigating agency websites.	IT Dashboard
Sec. 207(g) (44 U.S.C. § 3501 note) – Develop a Government-wide repository and website for all Federally funded research and development.	IT Dashboard

E-Government Act of 2002 Requirement	Location in E-Government Act Report to Congress
Sec. 208(b) (44 U.S.C. § 3501 note) – Report on agency compliance with developing a privacy policy and conducting privacy impact assessments.	Appendix G – Privacy Policy and Privacy Impact Assessments
Sec. 209(b)(2) (44 U.S.C. § 3501 note) – Report on agency compliance with establishing information technology training programs.	Appendix H – Agency Information Technology Training Programs