FY 2015 ANNUAL REPORT TO CONGRESS:
E-GOVERNMENT ACT IMPLEMENTATION

OFFICE OF MANAGEMENT AND BUDGET

June 17, 2016

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

June 17, 2016

The Honorable Jason E. Chaffetz
Chairman
Committee on Oversight
and Government Reform
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

The attached report is submitted pursuant to the E-Government Act of 2002 (P.L. 107-347), which requires the Office of Management and Budget (OMB) submit an E-Government status report to the Committee on Oversight and Government Reform of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate. This report provides a summary of information agencies are required to report under the E-Government Act and a description of compliance by the Federal Government with other goals and provisions of the Act. This is OMB's thirteenth annual report on the implementation of the E-Government Act. If you have any questions regarding this report, please call OMB's Office of Legislative Affairs at (202) 395-4790.

Sincerely,

Shaun Donovan
Director

Enclosure

The Identical Letter Sent to:

The Honorable Jason E. Chaffetz
The Honorable Elijah Cummings
The Honorable Ron Johnson
The Honorable Thomas R. Carper

TABLE OF CONTENTS

INTRODUCTION

Since the passage of the E-Government Act of 2002 (P.L. 107-347) (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 and improve 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. Additionally, consistent with previous E-Gov Act reports, this report includes information required under Section 2(g) of the Federal Funding Accountability and Transparency Act of 2006 (P.L. 109-282). 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] OMB's annual report to Congress on agency compliance with the Federal Information Security Modernization Act of 2014 (P.L. 113-283) (FISMA) is available online at: www.WhiteHouse.gov/omb/e-gov/docs.

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 the majority of agency implementation data. The information on the IT Dashboard reflects the information as it was provided by agencies to OMB.

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 A. This report is organized as follows:

- **Section I - E-Government Fund**
  In accordance with Section 101 of the E-Gov Act (44 U.S.C. §§ 3604 and 3606), this section provides a description of projects receiving E-Gov funds in Fiscal Year (FY) 2015, including funding allocations and results achieved.

- **Section II - Governmentwide Information Technology (IT) Workforce and Training Policies**

[1] P.L. 109-282, Sec. 2(g), codified at 31 U.S.C. § 6101 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. http://www.gpo.gov/fdsys/pkg/PLAW-109publ282/pdf/PLAW-109publ282.pdf.

This section provides a summary of activities pursuant to Section 209 of the E-Gov Act (44 U.S.C. § 3501 note), this section provides a summary of activities related to IT workforce policies, evaluation, training, and competency assessments.

- **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 each agency's privacy impact assessment and provides URL's for agency privacy policies and privacy impact assessments.

- *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: E-GOVERNMENT FUND

The E-Government Act of 2002 established an E-Government Fund (E-Gov Fund) to provide financial support for the innovative use of 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, the General Services Administration (GSA) was required to provide Congress with notification and a description of how E-Gov funds were to be allocated and how the expenditure would further the purposes of the Act. The following table provides a summary of the related fiscal year (FY) 2015 funding allocations included in GSA's notification to Congress that was transmitted in February 2015:

Investment Area	FY 2015 Allocation*
Promote Transparency and Accountability – Open Government and Transparency	$5.98 million
Accelerate Cross-Government Innovation – Cloud Computing and Security	$6.91 million
Accelerate Cross-Government Innovation – Performance Dashboards	$1.25 million
Promote Transparency and Accountability – Federal Funding Accountability and Transparency Act (FFATA) Implementation	$0.00
TOTAL	**$14.14 million**

*Amounts reflect the FY 2015 enacted appropriations for the E-Gov-related purpose of the Federal Citizen Services Fund per Consolidated and Further Continuing Appropriations Act, 2015 (P.L. 113-235).

Electronic government project areas will continue to drive innovation in government operations through IT, use IT to improve the transparency of Federal operations, and increase citizen participation in government; however, as specified in the Consolidated and Further Continuing Appropriations Act , 2015 (P.L.113-235), going forward GSA will transfer any appropriations provided to the E-Gov Fund from fiscal years prior to FY 2016 that remain unobligated to the Federal Citizen Services Fund to be used for electronic government activities.

Amounts in the Federal Citizen Services Fund for E-Gov-related purposes were allocated in FY 2015 the investment areas described below.

Open Government and Transparency

Description

This investment area supports the ongoing effort to make government information accessible, discoverable, and usable to increase efficiency and effectiveness in government operations; fuel entrepreneurship, innovation, and scientific discovery; and contribute to a more transparent, participatory, and collaborative government. This includes improving public access to high value, open data generated by Federal agencies on www.Data.gov, which provides citizens with access to over 188,000 datasets and collections[2] and almost 10,000 government application programming interfaces (APIs)[3] from 78 Federal agencies and sub-agencies, as well as state, local, and academic sources.[4] It is the centerpiece of the global open democracy movement and has been emulated by 40 U.S. states, 46 U.S. cities and counties, and 52 countries,[5] seeking to increase transparency and accountability, while fostering innovation. The software powering www.Data.gov is open-source, allowing Federal agencies and governments around the world to implement their programs faster and with less cost, and the development process is also open to the public, allowing transparency and collaboration between government and the public.[6] It also provides descriptions of the Federal datasets, information on how to access the datasets, contact mechanisms, metadata information, and links to publicly accessible applications that leverage the datasets. Lastly, users are empowered with opportunities to provide information feedback and ratings.

Results

- By the close of calendar year 2015, www.Data.gov featured over 188,000 datasets on topics such as education, climate, and public safety.

- Challenge.gov supported by this investment provides a no-cost platform for agencies to launch challenges and contests to leverage expertise and knowledge outside of the government and the traditional contracts and grants process. Solutions to government's most pressing problems can be obtained easily from the public, industry, and academia without requiring significant Federal funding. Individual challenges have yielded extremely cost effective, creative solutions.

- Launched in FY 2014, Project Open Data provides agencies the 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.

[2] http://www.data.gov/metrics
[3] http://catalog.data.gov/dataset?q=-aapi+api+OR++res_format%3Aapi#topic=developers_navigation
[4] http://www.data.gov/metrics
[5] http://www.data.gov/open-gov/
[6] https://github.com/gsa/data.gov

- The Project Open Data Dashboard has also been successful in publicly crediting agencies for demonstrating best practices in various measurement indicator categories.

- Sites.usa.gov (Sites) is a hosted service designed to enable the rapid deployment of government websites for the purpose of providing public information in a security and readily accessible environment. This government-wide shared service provides Federal agencies with WordPress, an easy-to-use web content management tool that is currently offered to agencies at no cost. Sites offers 12 responsive design themes, enabling agencies to easily deliver content to citizens, independent of the device they are using. This is especially important given the rapid growth of mobile use of Federal websites. In FY 2015, Sites doubled the number of live sites it hosted and reached out to more agencies across government. Sites currently hosts sites for a wide variety of Federal agencies and government initiatives including the 2016 Presidential Transition Directory, the Department of Labor (DOL) blog, Feeback.USA.gov, the Small Business Administration (SBA) Office of Advocacy blog, the National Institutes of Health Office of Research Services' News2Use, the Veterans Access Commission on Care, Federal Risk and Authorization Management Program (FedRAMP), and DigitalGov.

Open Opportunities is an innovative, micro-tasking program that is building a network of Federal employees with digital government expertise and interest to work on government-wide tasks and projects. The program invites agencies to post digital government tasks and projects for participating experts from across the government to tackle, helping agencies find needed skills for specialized tasks, while giving employees the opportunity to build and share their expertise. In FY 2015, using its 18F[7] unit, GSA expanded and automated the Open Opportunities platform to enable the program to scale for broader government-wide use. GSA's 18F is a consultancy of innovative technologists, designers, developers, and product managers who help interested agencies to buy, build, and share technological tools. 18F works with other agencies on a reimbursable basis for the services, procurement vehicles or platforms that they provide. There are currently 21 government-wide tasks and projects available on the site, and 245 tasks have been completed in FY 2015. All GSA Office of Citizen Services and Innovative Technologies and 18F employees are being encouraged to create a profile on the platform.

Cloud Computing and Security

Description

In an effort to support the development of innovative solutions, the Federal Government needs to invest in technologies and policies that modernize government operations. FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a "do once, use many times" framework that will reduce staff required to conduct redundant agency security assessments.

[7] https://18f.gsa.gov/

Results

- As part of the FedRAMP process, cloud service providers must use a FedRAMP approved Third Party Assessment Organization (3PAO) to independently validate and verify that they meet the FedRAMP requirements. Eight additional 3PAOs were accredited in FY 2015 to ensure a consistent assessment process, bringing the total to 39 accredited 3PAOs. A current list of FedRAMP accredited 3PAOs is available at www.fedramp.gov.

- In FY 2015 agencies issued 68 FedRAMP compliant authorizations to operate (ATOs) to Cloud Service Providers (CSPs). Of these, 50 ATOs were sponsored or reused by agencies. These included 22 original agency authorizations for CSPs and 28 reused ATOs. In addition, in FY 2015 the Joint Authorization Board (JAB) issued provisional ATOs (P-ATOs) to five CSPs. In FY 2015, P-ATOs were reused by agencies to issue an agency ATO 13 times. Through these processes, in FY 2015, 30 new CSPs were approved as FedRAMP compliant.

Performance Dashboards

Description

A key component of performance management is transparency of the key activities and related metrics of operations within agencies. The Performance.gov website was created to publicly share this type of information in support of the Government Performance and Results Modernization Act of 2010 (P.L. 111-352). The performance dashboards on the website enable the public, Congress, Federal employees, and others to monitor progress being made in cutting waste, streamlining government, and improving performance. Specifically, Performance.gov provides information on government-wide initiatives related to procurement, financial management, human resources, technology, performance improvement, open government, and sustainability.

Performance.gov is a window to the Administration's efforts to deliver a more effective, smarter, and leaner government, and it advances the President's commitment to communicate candidly and concisely what the Federal Government is working to accomplish, how it seeks to accomplish its objectives, and why these efforts are important. All cabinet departments and nine other major agencies (as listed by the site) have agency pages on Performance.gov. Each agency's page describes the agency's mission and lists the agency's strategic goals, objectives, and priority goals. Each agency's home page also provides links to the agency's strategic plan, annual performance plan, and annual performance report; reports agency progress on governmentwide management initiatives; and shows agency contributions to Cross-Agency Priority (CAP) goals.

Results

- Performance.gov was used to provide the current status of and progress updates to the Administration's efforts to achieve CAP goals, Agency Priority Goals (APGs), and Strategic Objectives contained within agency strategic plans.

- In order to allow users to see the evolution of CAP goals and better understand the context of agency activities, functionality was added to Performance.gov to allow users to download and review past assessments of progress toward CAP goal completion.

Federal Funding Accountability and Transparency Act Implementation

Description

The Federal Funding and Accountability Act (FFATA) program was transferred to GSA's Federal Acquisition Service in the fall of 2014. The $540,000 originally allocated to FFATA was reallocated to support the Digital Analytics Program (DAP).

DAP offers advanced web analytics to Federal agencies, allows the government to determine what content is effective and assists in user experience considerations on over 4,500 websites. In FY 2015, DAP saw 10 new agencies join the program, totaling participation from 45 agencies. In March of 2015, the DAP team released analytics.usa.gov, the public window into the Federal Government's web traffic data. The site is an ongoing effort to continue to expand data available to the public.

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 and the Chief Information Officers (CIO) Council, 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 and the CIO Council, must identify where current training does not satisfy current personnel needs, and then 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 2015 activities related to IT workforce policies, evaluation, training, and competency assessments.

Over the past three years, OPM has collaborated and coordinated with relevant stakeholders to get more accurate data on the current Federal cybersecurity workforce. OPM now has a government-wide cybersecurity data standard that aligns to the National Initiative for Cybersecurity Education (NICE) Framework. OPM requires agencies to code their workforces with the new data standard to identify those positions with significant cybersecurity work functions and to report the codes into the Enterprise Human Resource Information (EHRI) system. Retooling of the EHRI shared service providers' systems allowed for collection of the agencies' reported cybersecurity data. This significantly increased OPM's awareness and education outreach efforts to ensure the Chief Human Capital Officer (CHCO) agencies were coding the positions as mandated by OPM. OPM continues to collaborate with stakeholders to ensure that the dataset is accurate before advancing to the phase of utilizing the data to inform workforce planning decisions.

In 2015, OPM began supporting the Comprehensive National Cybersecurity Initiative to provide cybersecurity training through its USALearning website. USALearning implemented the Cybersecurity Virtual Training Environment training delivery and reporting site on behalf of the Department of Homeland Security (DHS) for all of Department of Defense (DOD), civilian Federal employees, key universities, contractors, Indian tribes, and state and local governments. The program is delivering online training in key areas, including cybersecurity risk management, cybersecurity, network monitoring, Internet Protocol version 6 (IPv6) security, and ethical hacking.

As part of OPM's continued efforts to close skill gaps and increase Federal employees' access to high quality training and educational resources, OPM and Champlain College entered into an educational alliance in April 2015. The agreement provides discounted tuition to Federal employees. While employees can benefit from a range of educational areas, Champlain College is recognized as a Cybersecurity Center of Academic Excellence, and therefore provides exceptional educational opportunities in cybersecurity for the Federal workforce.

SECTION III: DISASTER PREPAREDNESS

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

The Disaster Assistance Improvement Program

The Disaster Assistance Improvement Program (DAIP) maintains a single government-wide portal for disaster survivors to submit electronic applications for assistance following a declared disaster. 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, 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, disaster related information, easy access to the application for assistance, and application updates. The secure portal ensures that disaster survivors, who may be displaced or otherwise out of contact, have access to all Federal agencies that offer forms of disaster assistance, and continue to receive benefits from non-disaster related assistance programs.

In Fiscal Year 2015, DAIP provided Registration Intake (RI) for nine presidentially declared Individual Assistance (IA) disasters. DisasterAssistance.gov registered 59,135 online registrations for disaster assistance (11,214 from mobile devices and 47,921 from desktops). The portal also had 1,472,988 site visits (538,291 new visitors and 934,697 returning visitors).

The program experienced high customer satisfaction scores from survivors using the site, and continues to achieve "green" ratings in DHS's Office of Accessible Systems and Technology and the DHS CIO program health assessments.

Furthermore, through continued investment, the DAIP program released a new website design, improved the survivor experience with the implementation of an enhanced survivor centric application and account creation processes, increased stakeholder engagement, increased the resiliency of its technical infrastructure, and continued to increase operational efficiencies.

SAFECOM

SAFECOM works to improve multi-jurisdictional and intergovernmental communications interoperability through collaboration with emergency responders and policymakers across all levels of government. SAFECOM works with existing Federal communications programs and key emergency response stakeholders to address the need to develop better technologies and processes for the multi-jurisdictional and cross-disciplinary coordination of existing communications systems and future networks.

In FY 2015 SAFECOM, in partnership with the National Council of Statewide Interoperability Coordinators, developed the "Emergency Communications Governance Guide for State, Local, Tribal, and Territorial Officials." This guide serves as a comprehensive tool that provides recommendations and best practices for public safety officials at all levels of government to establish, assess, and update governance structures that represent all emergency communications capabilities.

SAFECOM also updated and delivered the annual SAFECOM grant guidance document to provide the most current information on emergency communications policies, eligible costs, technical standards and best practices for state, territorial, tribal, and local grantees investing Federal funds in emergency communications projects. SAFECOM guidance provides members of the emergency response community and other constituents with comprehensive information on topics relevant to emergency response communications and features best practices that have evolved from real-world situations

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. In FY 2015, several activities and accomplishments are particularly noteworthy, including DOI's ongoing efforts to develop the Geospatial Platform; work towards meeting the requirements of the National Spatial Data Infrastructure Strategic Plan 2014-2016 (Strategic Plan); and continued efforts to develop, adopt and promote geospatial technology standards for the Federal Government.

Geospatial Platform

The Geospatial Platform initiative continued to grow and maintain a fast rate of progress in 2015 with the release of many new features and capabilities. Some examples of these advancements include:

- Expansion of the data catalog holdings to total over 100,000 discoverable datasets, maps and web services;
- Registration of all National Geospatial Data Assets to facilitate discovery of these data and services by all users of Geoplatform.gov, which is integrated with Data.gov;
- Release of the new advanced Web Map Viewer and map sharing capability on Geoplatform.gov;
- Release of the National Geospatial Data Asset lifecycle maturity dashboard;
- Deployment of a new "preview release" of the Geoplatform.gov website and supporting environment; and
- Release of tools for harvesting maps from ArcGIS Online commercial software as a service environment for viewing in the Geospatial Platform.

National Spatial Data Infrastructure (NSDI) Strategic Plan

The Strategic Plan was approved by the Federal Geographic Data Committee (FGDC) Steering Committee and endorsed by the National Geospatial Advisory Committee in December 2013. The 2014-2016 Strategic Plan sets priorities and describes the actions to be taken, in collaboration with partners, to develop and maintain the national critical geospatial infrastructure.

The FGDC Executive Committee has the lead responsibility for overseeing and monitoring the implementation of the Plan. Designated Federal officials, appointed from the FGDC Executive Committee, serve as champions for each of the objectives in the Strategic Plan. Detailed implementation plans for each of the objectives in the Strategic Plan describe the actions to be taken and include tasks and timelines, responsible parties, dependencies, and performance indicators/measures.

Geospatial Data and Technology Standards

The FGDC continued its leadership and participation in development and coordination of national and international standards applicable to the geospatial community. There are a total of six endorsements of standards and technologies in 2015:

- Aeronautical Information Exchange Model (AIXM) 5.1: AIXM 5.1 defines how to exchange information applicable to airports, heliports, routes, navigation aids, instrument approach procedures, instrument departures, standard terminal arrival routes, organizations, units, services, obstacles and airspace. It is based on International Civil Aviation Organization standards and was initially developed by the U.S. Federal Aviation Administration (FAA) and the European Organization for the Safety of Air Navigation, with international support.

- ISO/IEC 15444-1:2004 Technical Corrigenda 1:2007 and 2:2008 JPEG 2000: JPEG 2000 (JP2) is a method for compressing images to reduce their file sizes and make them easier to deliver or share through standard applications like email. These two technical corrections update a core JPEG 2000 standard previously endorsed by FGDC.

- Geopolitical Entities, Names, and Codes (GENC) Standard Edition 2: Geopolitical Entities, Names, and Codes (GENC) Standard Edition 2.0 specifies names and codes for countries and their subdivisions (for example, states) that have been approved by the U.S. Board on Geographic Names (BGN), as required by US Public Law 80-242 (1947).

- GeoRSS-Simple and GeoRSS-GML: GeoRSS is a standardized way to encode location data in news feeds. It allows users to search for geographic information or map information found in news feeds. GeoRSS allows users to search using a variety of geographic criteria. GeoRSS-Simple is a very lightweight format of this GeoRSS capability that can be added simply to existing news feeds. GeoRSS-Simple supports only basic geometries (point, line, box, and polygon), while GeoRSS-GML supports a wider variety of features for more advanced applications.

- OGC GeoPackage 1.0: GeoPackage is an open, standards-based and platform-independent format for transferring geospatial information. GeoPackages are particularly useful on mobile devices like cell phones and tablets in communications, and this standard is useful in enabling those new technologies for mapping applications.

- Part 2, Digital Orthoimagery (revised) of the Geographic Information Framework Data Standard: Imagery captured by satellites or through aerial photography, often serves as a base map upon which both artificial features like roads, and natural features like rivers can be displayed. This imagery is useful in a number of applications, including environmental assessments and transportation planning, and this standard defines how to collect, register, and integrate digital orthoimagery data.

More detailed information about these standards and other activities of the FGDC can be found at http://www.fgdc.gov/standards.

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 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 15 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, mentioned above:

- 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 (P.L. 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 and provides URLs for agency privacy policies and privacy impact assessments.

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

The E-Gov Act requires OMB to oversee the implementation of the E-Gov Act in a number of 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. 44 U.S.C. § 3602(e). 44 U.S.C. § 3602(f)(9) 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. 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, enhance interoperability between different public and private sector entities, or enhance the delivery of information to the public.

The Homeland Security Information Network (HSIN) is a platform for sharing of "sensitive but unclassified" information. It is the primary centralized location through which private sector; DHS; small agencies; and other Federal, state, local, territorial, international and tribal government personnel can collaborate regarding threats to important infrastructure. Of particular note is HSIN's devoted suite of services for emergency service professionals and law enforcement officials, for whom HSIN enables multiple jurisdictions to coordinate during emergencies, determine the best use and distribution of multiple resources, and share information about ongoing events with partners across jurisdictional and geographic boundaries.[8]

In one unique example, HSIN was leveraged to manage impacts and civic infrastructure during the 2015 Road World Championship, a nine-day cycling competition held in Richmond, Virginia. This year the event welcomed 1,000 athletes and 645,000 spectators from around the world—almost 200,000 more attendees than anticipated. HSIN played an important role in management of critical infrastructure in the city and neighboring towns during the race and was used to coordinate and manage support efforts like road closures and utility outages most efficiently. In the past two years, HSIN utilization has more than doubled, reaching more than 47,000 emergency managers, law enforcement officers, intelligence analysts, and other public safety officials, all of whom coordinate simultaneous efforts and conduct critical information-sharing through HSIN.

Agencies are furthermore addressing public needs through targeted services, like those that connect recipients and providers of services. SBA's Leveraging Information and Networks to access Capital (LINC) connects applicants for loans with loan providers, enabling small and nascent business owners to find the right funding and financial support. If the applicant's information and need matches a loan product the lender offers, contact information can be extended instantly to the two parties.

Government-wide, agencies are also diversifying their information resource capabilities, with some providing data in both navigator formats and in Application

[8] More information can be found on http://www.dhs.gov/hsin.

Program Interfaces, and working to improve the usability of data and websites by leveraging public feedback mechanisms. For example, in FY 2015 the National Aeronautics and Space Administration (NASA) updated its data.NASA.gov data registry. The site allows users to view and interact with that data through APIs, gain insight and developer details on NASA API's, and create visualizations with NASA's data. The site is integrated with the open.NASA.gov web platform as well as NASA's API management System on API.NASA.gov.

Recently, OMB has improved the openness of data collections and agency document submissions pursuant to the Federal IT Acquisition Reform Act (FITARA)[9] and OMB memorandum Management and Oversight of Federal Information Technology (M-15-14). As required by 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 collection pursuant to FITARA has been 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.

[9] 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. The Department of Education (ED) uses value and performance metrics to evaluate its IT investments with its Value Measurement Methodology (VMM), in which the Office of the Chief Information Officer and Line of Business (LOB) senior executives identify mission priorities to which all IT investments align. In another example, U.S. Agency for International Development (USAID)'s IT Project Governance incorporates project, configuration, security, and portfolio management processes. These supplement their execution of required policies and procedures such as Capital Planning and Investment Control (CPIC), Enterprise Architecture (EA), and USAID's Automated Directives System's (ADS).

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. For example, the Department of Labor (DOL) develops and manages IT investment performance measures and metrics in accordance and compliance with the Performance Reference Model as described in the Common Approach to the Federal Enterprise Architecture. DHS uses IT Program Health Assessments to determine performance areas for corrective action. Scoring for performance targets are assigned point values based on the level of achievement in a particular area.

Agencies use a variety of governance tools and structures to carry out performance measurement. Some agencies, such as the Nuclear Regulatory Commission (NRC), include metrics in system owners' performance plans, combined with other performance plans as needed. Measures are developed with direct line-of-sight from goal to metric, and are included in the goal leads' performance plans for tracking and accountability. Other Agencies like the Department of Commerce (DOC) use IT Review Boards to track project performance against established metrics. The Office of the Director of National Intelligence (ODNI)'s different stages of performance review are produced in separate offices and are analyzed and reviewed monthly at Infrastructure Services Group Performance Measure Management Reviews. External infrastructure services groups are provided weekly reports evaluating their performance and delivery.

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 CPIC processes and in system operational analysis. Numerous metrics applicable to FY 2015 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 M-15-14 identifies 14 core metrics for PortfolioStat sessions such as, Commodity IT Spending, Potential Mobile Savings, and FedRAMP Implementation.[10] Attachment E of 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.

[10] 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/default/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.

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, in 2015 the Department of Justice (DOJ) unveiled numerous resources to help law enforcement agencies implement the use of body worn camera technology and the department policies that govern their use. Among these was the launch of a new online resource called the National Body-Worn Camera Toolkit, which seeks to enhance and share knowledge about best practices and the critical importance of stakeholder and community engagement required to support successful body-worn camera program implementation. It also aims to advance understanding of more complex program requirements that inform policy, training, and equipment procurement related to storing digital evidence and deployment of body-worn cameras in local communities. Furthermore, DHS uses web-based crowdsourcing tools to engage with the public directly on a range of issues and policies. Ideas can be submitted directly by the public, which can also vote for or against each idea and comment within the discussion.

DOC utilizes social media to partner with private sector, state, local, tribal and international governments to develop and share best practices. USDA posts the majority of its public meetings on USDA.gov/live and the agency's YouTube channel. These public meetings are also broadcast through various digital broadcast tools and the agency's own television and radio studios. These environments are also used for collecting public comments, on the USDA blog, Facebook page, Twitter, and other platforms.

Collaboration with the public, however, extends beyond making resources available to determining how they can be utilized. Responding to the President's call to encourage open innovation and leverage technology to support agency missions, agencies have held "datapaloozas," 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. The National Aeronautics and Space Administration (NASA) over the last three years has worked with more than 39,000 global citizens spanning technologists, scientists, designers, artists, educators, entrepreneurs, developers, and students, from hundreds of countries to design innovative open source solutions to global challenges: space technology, earth science, robotics, and human spaceflight, among others.

OMB has made additional strides toward open policymaking through the implementation of open data policies, such as through Project Open Data and the Project Open Data Dashboard. Furthermore, as outlined in the Second Open Government National Action Plan, the Administration is committed to the idea that "using and contributing back to open source software can fuel innovation, lower costs, and benefit the public."[11] In furtherance of these objectives, OMB OFCIO sought public comments on a draft Federal Source Code Policy to improve to the way custom-developed Government code is acquired and distributed moving forward.

The draft policy requires that, among other things: (1) new custom code whose development is paid for by the Federal Government be made available for reuse across Federal agencies; and (2) a portion of that new custom code be released to the public as Open Source Software. The first draft of the Federal Source Code Policy received approximately 2,500 comments and suggestions during its public comment period, and is currently being revised for final release, based in part upon that significant public feedback. A publicly-accessible source code discoverability portal and additional implementation guidance will be provided after the policy's release.

[11] "New Open Government Initiatives as part of the Second Open Government National Action Plan for the United States of America". September, 2014.
https://www.whitehouse.gov/sites/default/files/microsites/ostp/new_nap_commitments_report_092314.pdf

APPENDIX D. CREDENTIALING

In accordance with Section 203 of the E-Gov Act (44 U.S.C. § 3501 note), it 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 logical 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. In FY 2015, ED initiated procurement of an independent third party credential validation service to support approximately 40,000 external users of ED's grant management systems, to comply with HSPD-12. The Department of Health and Human Services (HHS) has issued 121,133 PIV cards out of 129,799 total eligible staff, an adoption rate of 93%. Additionally, some agencies have taken steps to ensure secure log-in for external resources.

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. In FY 2015, GSA's CIO developed a digital signature solution in order to further interoperability with the identified applications across the government and the public. Applications that generate standard Word, Excel, and PDF documents can incorporate the GSA CIO digital signature solution, enabling users to send documents for signatures between government entities and the public.

Lastly, OMB Cyber National Security Unit (OMB Cyber), through the 30-Day Cybersecurity Sprint (the Sprint) initiated by the Federal CIO in June 2015, directed agencies to take a number of steps immediately to protect Federal information and assets and improve the resilience of Federal networks. The Sprint resulted in dramatically improved utilization of PIV card implementation government-wide, from 42% to 72% of civilian agency users. Throughout FY 2015, civilian agencies increased their use of unique PIV cards for all users from 41% in FY 2014 to 81% of civilian users at the end of the FY 2015. When including DOD, this percentage increases to 82%. Most recently, OMB issued the Cybersecurity Strategy Implementation Plan (CSIP) for the Federal Civilian Government (M-16-04) to ensure agencies have the best practices, techniques, and tools at their disposal regarding Federal cybersecurity best-practices.

On February 9, 2016, the Administration announced the Cybersecurity National Action Plan (CNAP), a capstone of more than seven years of determined efforts – that takes near-term

actions and puts in place a long-term strategy to ensure the Federal Government, the private sector, and American citizens can take better control of our digital security. As part of the CNAP, the President issued an Executive Order establishing a Commission on Enhancing National Cybersecurity to bring together top leaders from outside the Government to make critical recommendations on developing new technical solutions and best practices to enhance cybersecurity awareness, protect privacy, ensure public safety and economic and national security, and empower Americans to take better control of their digital security. . The CNAP will also empower the American people to secure their online accounts by using additional security tools, which will work with leading companies to secure online accounts and financial transactions.

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 regulated 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 provide comments on regulatory actions. 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. For example, NRC has created dockets on Regulations.gov for all documents it has published in the Federal Register since FY 2008. In FY 2015, NRC posted 77 rules, proposed rules, and petitions for rulemaking documents; 622 Federal Register notices; and 1,580 public submissions on Regulations.gov.

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. HHS, for example, maintains a web page dedicated to regulations (www.hhs.gov/regulations) which is maintained by the HHS Public Participation Task force. The page serves as a "one-stop shop" on HHS's regulatory activity and features a daily update providing access to all HHS regulatory proposals currently open for comment. If they wish, visitors can select a certain division of HHS to access current information specific to that division. DOL also has a website (www.dol.gov/regulations/) that provides the public with a central point to learn more about the regulatory process and specific DOL regulatory activities as well as facilitate access to DOL regulatory material. Lastly, The Department of State (State) utilizes its @StateDept Twitter account to reach a broader audience. In FY 2015, this Twitter handle exceeded 1.2 million followers. When a rule is published, State tweets its subject information as well as a link to the full text of the document on Regulations.gov.

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. USDA, for example, had 228 staff using FDMS in FY 2015, and created 163 regulatory dockets in FDMS for regulatory actions. DOC, another major user of the system, had 194 staff use the system in

FY 2015, creating and posting 210 regulatory dockets.

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. Work initially described in 2014 still holds today. The full list of activities can be found on the IT Dashboard.

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. Treasury, for instance, is in the process of implementing the NARA Capstone approach, in accordance with NARA Bulletin 2013-02, Guidance on a New Approach to Managing Email Records. The Capstone approach was developed in recognition of the difficulty of practicing traditional records management approaches on the overwhelming volume of email that departments and agencies produce. This approach will provide Treasury with feasible solutions to email records management challenges, especially as it considers cloud-based solutions. Capstone allows for the capture of records that should be preserved as permanent from the email accounts of high-level Treasury officials. Using this approach, an office or bureau categorizes and schedules email records based on the duties and position of the email account owner. Moreover, the Capstone approach supports Treasury's effort to standardize business processes, and allows it to comply with the requirement in M-12-18, "Managing Government Records Directive," to "manage both permanent and temporary email records in an accessible electronic format." Treasury's Office of Privacy, Transparency, and Records (OPTR), in collaboration with the Office of the General Counsel and the Office of the Chief Information Officer, is developing new policies, training methodologies, and materials related to Capstone. Full implementation of the Capstone policy is anticipated by the December 31, 2016 deadline set forth in M-12-18.

Other agencies have developed their own systems and processes to comply with NARA recordkeeping requirements. DOI established the Email Enterprise Records and Document Management System (eERDMS) program to move the agency toward an integrated electronic enterprise recordkeeping system that provides support for messaging, records management, content management, case management, and early case assessment review. The eERDMS program consists of five systems: the Enterprise Forms System (EFS), the Enterprise eArchive System (EES), the Enterprise Dashboard System (EDS), the Enterprise Content System (ECS), and the Enterprise Fax System (EXS). These systems provide a Department-wide solution to increase cost savings and improve greater efficiencies for managing records in a records management environment compliant with DOD 5015.02-STD, "Electronic Records Management Software Applications Design Criteria Standard."

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, as required; ensure the review of the privacy impact assessment by the CIO, or equivalent official, as determined by the head of the agency; and if practicable, after completion of the review, make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means. This appendix provides information regarding select agencies' work in this area. The full list of activities can be found on the IT Dashboard.

DOJ's privacy compliance process begins with an Initial Privacy Assessment (IPA), which allows the Department's components to streamline the assessment of information privacy issues associated with (1) all systems or projects that collect, maintain, or disseminate information in identifiable form; or, (2) new electronic collections of information in identifiable form for ten or more persons (excluding agencies, instrumentalities, or employees of the Federal Government) (consistent with the Paperwork Reduction Act). Through this IPA process DOJ also reviews information technology systems that contain information in identifiable form to determine whether the privacy requirements under the E-Gov Act and OMB guidance apply. If the privacy requirements apply to the IT system, DOJ requires a full Privacy Impact Assessment (PIA) be conducted for the system to ensure that system developers and owners have made technological and operational policy choices that incorporate privacy protections into the underlying architecture and operational processes of the system. In addition, if significant changes to information collection authorities, business processes, or other factors affecting the collection and handling of information in identifiable form occur, components must update their affected PIAs. DOJ requires that a subsequent IPA be conducted to determine whether such changes would require a modification to an existing PIA, or would require a new PIA.

At Treasury, conducting PIAs is an integral part of Treasury's process for developing a new system, revising existing technology, or revising or instituting a new information collection. In coordination with Treasury's Office of the Chief Information Officer, the Office of Privacy, Transparency, and Records (OPTR) established a standard reporting framework for conducting PIAs tailored to the missions and functions of the Department. The program manager, system owner, and/or developer conduct PIAs for new systems and projects as well as enhancements or modifications of existing systems that collect, maintain, or share personally identifiable information (PII). To facilitate the process and approval of PIAs, OPTR developed the Privacy Clearance Tracker on SharePoint. This application gives Treasury the capability to upload PIAs in draft form, identify and engage the necessary reviewers to obtain comments, and expedite final clearance and approval in a paperless process. The Deputy Assistant Secretary for OPTR is the approving official for Treasury. All approved PIAs are then posted to the agency website, accessible to the public.

SBA conducts reviews of all FISMA systems to determine how information about the public is handled when the Agency uses IT systems to collect new information, or when agencies develop or buy new IT systems to handle collections of PII. The Privacy Threshold Analysis and PIAs are used to identify privacy information stored and processed within the environment and discusses the controls in place to prevent harm resulting from the loss, misuse, or unauthorized access to or modification of privacy information. SBA policy,

through Standard Operating Procedure 40, Number 04, Revision 3 (SOP 40 04 3), "Privacy Act Procedures," directs the Agency to conduct periodic reviews of how information is handled within SBA when IT is used to collect information. Compliance with SBA privacy guidance is considered whenever new systems are developed or acquired.

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.

At ED, the Information Assurance Cybersecurity Awareness and Privacy programs develop required cybersecurity and privacy awareness training for all employees and contractor staff. In FY 2015, ED enhanced this IT training program by: (1) Incorporating best practices to mitigate audit findings; (2) Adapting training to be responsive to identified threats (i.e. phishing); (3) Increasing the number of access points to training; (4) Enhancing the Role-Based training to follow the NIST National Initiative for Cybersecurity Education guidelines for staff with elevated privileges; and (5) Improving readability of training and testing. In FY 2015, ED met Federal guidelines for completion rates. Additionally, in support of ED's move toward hoteling and teleworking, ED's Office of Management has partnered with OPM's Human Resource University to ensure compatibility and access to those courses for all ED staff both in-office and by way of remote network connection.

OPM makes available over 300 IT-related courses and training in its "Learning Connection" learning management system. In FY 2015, the total number of completed courses related to information technology, all completed through this platform, was 461. 217 courses involving the Microsoft Office Suite; 189 courses involving networking, databases, and programming; and 55 courses involving security, malicious code prevention, and privacy were completed, increasing productivity and closing knowledge gaps throughout the agency's staff. Additionally, the "Learning Connection" provides OPM project managers several blended learning sessions using the Project Management Body of Knowledge (PMBoK) 5th edition. These sessions provide continuous learning credits for Project Management Professional (PMP) recertification, an encouraged certification most useful for IT project managers.

Lastly, OMB has also created training programs to teach contracting professionals best practices in agile development processes. In October 2015, a class of 30 students began the inaugural program, called the Digital Service Contracting Professional Training and Development Program. The six-month program is led by OMB's Office of Federal Procurement Policy and U.S. Digital Service and will train contracting professionals in the agile development contracting best practices necessary to implement modern, iterative software development projects. An additional training and skill development program, the first IT Solutions Challenge was conducted also in FY 2015. This annual, 6-month training opportunity involves several small working groups of rising stars within the IT and IT acquisition communities and challenging them to identify issues within the Federal Government and develop solutions to those problems.

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 2013, 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) – Avoid diminished access and ensuring 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 governmentwide 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