FY 2014 ANNUAL REPORT TO CONGRESS:

E-GOVERNMENT ACT IMPLEMENTATION

OFFICE OF MANAGEMENT AND BUDGET
February 27, 2015

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

DEPUTY DIRECTOR
FOR MANAGEMENT

February 27, 2015

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

Dear Mr. Chairman:

On behalf of the Director, 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) to 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 twelfth 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,

Beth F. Cobert
Deputy Director for Management

Enclosure

Identical Letter Sent to:

The Honorable Jason Chaffetz
The Honorable Elijah Cummings
The Honorable Thomas R. Carper
The Honorable Ronald Johnson

TABLE OF CONTENTS

INTRODUCTION

Since the passage of the *E-Government Act of 2002* (P.L. 107-347) (E-Gov Act),[i] 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 Accounting 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 entire Federal Government.[ii] The E-Gov Act, under Section 3543(a)(8), also requires OMB to report on certain information security activities. This information can be found in the annual report to Congress on agency compliance with the Federal Information Security Management Act of 2002 (P.L. 107-347) (FISMA). Previous reports from OMB to Congress are 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 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), this section provides a description of projects receiving E-Gov funds in Fiscal Year (FY) 2014, including funding allocations and results achieved.

- **Section II - Governmentwide Information Technology (IT) Workforce and Training Policies**
  In accordance with 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 transactions within the Federal Government and/or with the public.

  - *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

Section 101 of the E-Gov Act established an E-Government Fund (E-Gov Fund) to provide financial support to the innovative use of technology in the Federal Government (44 U.S.C. § 3604). According to this Section, projects supported by the E-Gov Fund may include 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 information technology (IT) in sharing information and conducting transactions with each other and with state and local governments.

In accordance with Section 3604(e), the General Services Administration (GSA) is required to provide Congress with notification and a description of how E-Gov funds are to be allocated and how the expenditure will further the purposes of this chapter. The following table provides a summary of Fiscal Year (FY) 2014 funding allocations included in GSA's notification to Congress that was transmitted in February 2014:

Investment Area	FY 2014 Allocation*
Promote Transparency and Accountability – Open Government and Transparency	$7.30 million
Accelerate Cross-Government Innovation – Cloud Computing and Security	$6.16 million
Accelerate Cross-Government Innovation – Performance Dashboards	$2.00 million
Promote Transparency and Accountability – Federal Funding Accountability and Transparency Act (FFATA) Implementation	$0.54 million
TOTAL	**$16.00 million**

*Amounts reflect the FY 2014 enacted appropriations for the E-Gov Fund per *Consolidated Appropriations Act, 2014* (P.L. 113-76).

E-Gov 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 2015 that remain unobligated to the Federal Citizen Services Fund to be used for electronic government

activities.

The FY 2014 E-Gov Funds were allocated in the investment areas described below.

Accessible and Transparent Government

Description

This investment area supports the on-going effort to making government data open and easily accessible to citizens and businesses. This includes improving public access to high value, machine readable datasets generated by Federal agencies on *www.Data.gov*, which provides citizens with access to approximately 137,000 distinct datasets and 409 government application programming interfaces (APIs) from 400 publishers representing 88 Federal agencies and sub-agencies, as well as state, local, and academic sources. It is the centerpiece of the global open democracy movement and has been emulated by 39 U.S. states, 46 U.S. cities and counties, and 45 countries, seeking to increase transparency and accountability, while fostering innovation. The software powering *www.Data.gov* is open-source, allowing 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. 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. End users are provided with opportunities to provide information feedback and ratings.

Results

- By the close of calendar year 2014, *www.Data.gov* featured over 137,000 open, machine-readable datasets on topics such as health, education, energy, and public safety.

- The Challenge Platform 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 with tools and best practices to make their data publically 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 Project Open Data Dashboard has also been successful in publically crediting agencies for demonstrating best practices in various measurement indicator categories.

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. The Federal Risk and Authorization Management Program (FedRAMP) is a governmentwide 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 save cost, time, and staff required to conduct redundant agency security assessments. The Federal Cloud Credential Exchange (FCCX) program, which was renamed *Connect.gov*, launched a pilot in FY 2014 to enable Federal agencies to use interoperable, commercially generated identity credentials to allow users to access digital services and information across agency systems with a single sign-on.

GSA serves as the Program Management Office for *Connect.gov* and is providing oversight, strategic guidance and agency coordination, and is developing the business model for the program; the United States Postal Service (USPS) has acquired and is managing the technical solution, which provides a single point of connection between Federal agencies and Sign-In Partners.

Results

- The FedRAMP Project Management Office issued an updated security control baseline to bring it in line with the baseline laid out in National Institute of Standards and Technology (NIST) *Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations*, version 4.

- As part of FedRAMP's transition from initial operating capabilities, which agencies were required to report compliance with by June 2014, to full operations, the program continued to improve its development of repeatable processes and standards for assessment, authorization and continuous diagnostics.

- As part of the program's continued effort to expand the availability of secure cloud options, FedRAMP issued an additional four Joint Authorization Board (JAB) Provisional Authorizations, interim security authorizations of cloud solutions using a standardized baseline approach, in FY 2014, with another 19 Cloud Services in the JAB Provisional Authorization pipeline. Additionally, 15 cloud services were in process for agency authorization, which requires cloud service providers to work through a specific agency to meet FedRAMP security requirements, at the close of the fiscal year.

- 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. Seven additional 3PAOs were accredited in FY 2014 to ensure a consistent assessment process, bringing the total to 31 accredited 3PAOs. A current list of FedRAMP accredited 3PAOs is available at: *www.fedramp.gov*.

- The *Connect.gov* program was successfully launched, with the Department of Veterans Affairs, Department of Agriculture, and NIST allowing consumers to access one or more of their applications using a third-party credential they already have and trust.

Federal Funding Accountability and Transparency Act (FFATA) Implementation

Description

Passed in 2006, the Federal Funding Accountability and Transparency Act (FFATA) requires full public disclosure of entities that receive Federal Awards, including the name of the Entity, the amount of the Federal Award, and other details. In FY 2014, the FFATA initiative continued to include *www.USAspending.gov*, a public-facing website that provides easy access to information on Federal Award spending to include contracts, sub-awards, grants, loans, and other types of spending. Data is provided by agencies to the website using the Federal Assistance Awards Data System and the Federal Procurement Data format, which provides details regarding each Federal Award. The dashboards on *www.USAspending.gov* provide agencies and the public access to details of various Federal contracts, grants, loans, and other types of spending online. The website also allows users to track progress over time. Additionally, the FFATA Sub-award Reporting System (FSRS) reports data on first-tier sub-awards under grants and contracts subject to the FFATA reporting requirements. It also provides some visibility of Federal funds that flow through state governments to cities and counties. The website has proven valuable to both government and public users and has been utilized by Congress and a variety of non-Federal stakeholders including state governments, non-profit organizations, and organizations interested in Federal spending trends and transparency.

Results

USASpending.gov

- Built on the requirements of the Digital Accountability and Transparency Act of 2014 (DATA Act), OMB and the Department of the Treasury (Treasury) have sought to establish a governmentwide financial data standard as well as interim steps to improve the quality of data provided to *www.USAspending.gov*.[iii]

- As reflected in the President's FY 2014 Budget and consistent with funds provided in the Consolidated Appropriations Act, 2014 (P.L. 113-76), management of *www.USAspending.gov* was transferred to Treasury in February 2014.

- Treasury has announced plans to make changes to *www.USAspending.gov* in order to improve the search function of that website, which could potentially help to facilitate linking subcontractors to prime contracts.

FSRS

- In the Fall of 2014, funding for FSRS implementation was transferred to the GSA Federal Acquisition Service in order to better align this work and its funding source with the Integrated Award Environment, which uses innovative processes and technologies to improve systems and operations for those who award, administer, or receive federal financial assistance, contracts, and intergovernmental transactions.

- FSRS implementation will be fully funded by agency contributions in FY 2015 and no E-Government funds will be required.

Performance Dashboards

Description

A key component of performance management is transparency of the key activities and related metrics of operations within agencies. The *www.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, *www.Performance.gov* provides information on governmentwide initiatives related to procurement, financial management, human resources, technology, performance improvement, open government, and sustainability.

Results

- The website www.*Performance*.gov was used to provide both the status of and updates to the Administration's Cross-Agency Priority (CAP) goals, select objectives that require collaboration between multiple agencies in order to implement.

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

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 2014 activities related to IT workforce policies, evaluation, training, and competency assessments.

Center for Strategic Workforce Planning

In FY 2013, OPM created the Center for Strategic Workforce Planning within the OPM Employee Services group. The Center, created as part of a readjustment to help provide more technical assistance to the human resources community, is instrumental in coordinating the efforts of the Federal IT workforce to meet their missions, specifically with regards to cybersecurity. The cybersecurity workforce community is a key focal point for the Governmentwide Initiative to Close Skill Gaps, led by OPM's Director and its Center for Strategic Workforce Planning. In FY 2014, and continuing through FY 2015, the overall strategy for addressing the needs of the Federal cybersecurity workforce has been to build upon previous governmentwide collaborative efforts to obtain more accurate hard data on the current Federal cybersecurity workforce. To do this, OPM utilizes key ongoing partnerships such as the CIO and Chief Human Capital Officers (CHCO) Councils as well as the National Initiative for Cybersecurity Education (NICE), a National Institute of Standards and Technology (NIST) led effort building on the strengths of more than 20 Federal agencies, as well as representatives from the private sector, academia and state, local and tribal government organizations. In additional, OPM partners with the Office of Science and Technology Policy (OSTP) in the White as part of the broader FY 2013-2015 Governmentwide Initiative to Close Cybersecurity Skill Gaps.

In FY 2014, the primary strategy for these collaborations focused on developing more complete, evidence-based information about the Federal cybersecurity workforce in order to assist and inform Federal decision-makers in their efforts to improve and strategically target their employment and career development programs for this uniquely essential workforce community. With the issuance of *OPM Memorandum, Special Cybersecurity Workforce Project* in July 2013, OPM directed agencies to, in FY 2014, apply and report using new cybersecurity data codes for all of their positions in order to rapidly form a new statistical dataset for the Federal cybersecurity work function. This new data code system, found in OPM's Guide to Data Standards, defines cybersecurity work by 40 distinctly characterized work categories and specialty areas. Its collaborative use by each agency's CHCO, CIO, and Chief Information Security Officer (CISO) characterizes each Federal position with a data code descriptive of any cybersecurity work assignment. The Guide to Data Standards aligns with the revised lexicon in the NICE *National Cybersecurity Workforce Framework* report issued in 2013. The dataset, which resides in OPM's Enterprise for Human Resources Integration (EHRI) data warehouse, will become available after January 2015 and will serve as a key resource of information regarding the shape and

skills of the Federal cybersecurity workforce. As of the end of FY 2014, preliminary analysis affirms that Federal cybersecurity work is a multi-disciplinary work function existing as a significant work assignment in positions spanning more than 100 Federal occupation series.

SECTION III: DISASTER PREPAREDNESS

Section 214 of the E-Gov Act (44 U.S.C. § 3501 note) requires OMB, in consultation with the Department of Homeland Security (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.

Disaster Assistance Improvement Program

Each year, disasters destroy homes and businesses and disrupt the lives of hundreds of thousands of citizens across the nation. The Disaster Assistance Improvement Program (DAIP) maintains a single governmentwide single portal for disaster survivors to submit electronic applications for assistance following a declared disaster. The mission of the DAIP is to ease the burden on disaster survivors by simplifying the process of identifying and applying for disaster assistance.

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 and disaster related information. 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 as well as information on non-disaster related assistance programs.

In FY 2014, DAIP implemented usability enhancements aimed at simplifying the overall user experience. DAIP implemented enhancements to the application process to support pre-registration of survivors in advance of known large events such as Hurricane Sandy. It also implemented an innovative Federated Application (FedAPP) Framework to enable secure data sharing amongst agency partners. FedAPP includes configurable off the shelf (COTS)-based forms engine to support the collection and delivery of partner agency disaster data to further reduce costs. DAIP also implemented Google Analytics to support robust site usage metrics collection, in order to improve quality, cut costs, and implement a customer satisfaction survey.

SAFECOM

SAFECOM is an emergency communications program within DHS, established in 2001 in response to a lack of emergency response interoperability between government programs which were previously disconnected and fragmented. With over 60,000 distinct emergency response agencies across the country, SAFECOM, in order to inform nationwide planning efforts, provides a process by which to obtain stakeholder input and feedback on emergency response activities performed by local, state, and Federal Government practitioners. The result is the development of better technologies and processes for the coordination of existing communications systems and future networks which cross jurisdictions and disciplines.

In FY2014, SAFECOM worked with the Office of Emergency Communications, the National Council of Statewide Interoperability Coordinators, and other public safety

organizations to update the National Emergency Communications Plan (NECP). The 2014 NECP addresses various challenges related to governance, planning, training coordination, and research on emergency communication capabilities and services. SAFECOM also updated and delivered the annual *SAFECOM Guidance on Emergency Communications Grants* document providing the most current information on emergency communications policies, eligible costs, technical standards and best practices for state, territorial, tribal, and local grantees investing in Federal funds for emergency communications projects.

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.

Geospatial Platform

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 initiative. The activities of the Geospatial Platform focus on the implementation of *www.Geoplatform.gov* as a mechanism for developing and delivering geospatial shared services across government. The Geospatial Platform initiative continues to grow and maintained a fast rate of progress through 2014 with the release of many new features and capabilities. Some examples of these advancements include the expansion of the geospatial hosting services to allow more agencies to develop and publish shared geospatial data and applications within the Federal Government and to the public, and support for the President's Climate Data Initiative through the publication of new data and the establishment of a dedicated climate resource area on *www.Geoplatform.gov*. The Geospatial Platform was also integrated with *www.Data.gov*, a resource which increases public access to high value, machine readable datasets generated by the Executive Branch of the Federal Government.

- ***National Spatial Data Infrastructure (NSDI) Strategic Plan***

DOI and its partners from the Federal Geographic Data Committee (FGDC) led an effort to develop a new strategic plan for the National Spatial Data Infrastructure (NSDI). The 2014-2016 NSDI Strategic Plan sets priorities and describes the actions to be taken, in collaboration with partners, to develop and maintain a Federal 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 subject matter experts and advocates for each of the objectives in the Plan. Detailed implementation plans for each of the objectives in the NSDI Strategic Plan describes pending actions, including: tasks and timelines, responsible parties, dependencies, and performance indicators/measures.

- **Geospatial Data and Technology Standards**

The FGDC has endorsed five geospatial technology standards to be used by all federal agencies that leverage geospatial information. Throughout FY 2014, the FGDC continued its leadership and participation in development and coordination of national and international standards related to the geospatial community. Selected examples of standards the FGDC endorsed in FY 2014 are listed below:

- The Real Property Asset Data Standard (RPADS) is a standard that applies to data on Federal asset accountability. This data will provide the basis for better understanding of Federal real property management, high-performance green buildings management, and other Federal Government initiatives. The RPADS includes the minimal set of attributes needed to identify and locate related assets on a map.

- Open Geospatial Consortium (OGC) GeoPackage 1.0, which the OGC adopted as an official Standard in February 2014, enables customers to access data in a simple, open format tailored to handheld mobile devices, even in environments where there is limited or no connectivity.

- Geopolitical Entities, Names, and Codes (GENC) Standard Edition 2 expands on Edition 1 by specifying a U.S. Government profile of ISO 3166, codes for the representation of names of countries and their subdivisions.

- OGC Sensor Web Enablement (SWE) 2.0 suite of standards, which provide a set of interoperability interfaces and metadata encodings. Developers can use these specifications in creating applications, platforms, and products involving web-connected devices such as flood gauges, air pollution monitors, stress gauges on bridges, mobile heart monitors, webcams, and robots as well as space and airborne earth imaging devices.

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 *www.itdashboard.gov/egov_act_report*.

Furthermore, several of the requirements set forth in the E-Gov Act require the provision of URLs 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 URL's 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 URL's 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 URL's for agencies' Freedom of Information Act website.

- Information Resources Management Strategic Plan: In accordance with Section 207(f)(1)(A)(iv) of the E-Gov Act, this section provides the URL's 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 URL's 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 URL's for publically accessible information related to R&D activities and/or 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 URL's 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 areas (44 U.S.C . § 3602(e)). Section 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, or make improvements in government operations. Agencies are improving information management, removing barriers to making information accessible, and making information more usable by a variety of users, thus enhancing the delivery of information to the public.

Additionally, when agencies collect and create information in a way that supports downstream information processing and dissemination activities, it removes barriers to making this information accessible to and usable by the public, thus enhancing the delivery of information. Agency efforts to move in this direction include building or modernizing information systems in a way that maximizes interoperability and information accessibility, maintaining internal and external data asset inventories, and clarifying information management responsibilities. For example, agencies such as the Department of Defense (DOD), GSA, and U.S. Agency for International Development (USAID), have developed internal tools for inventorying data, assisting bureaus in managing their data, and producing related JavaScript Object Notation (JSON) files. As a result of these efforts, the Federal Government has made significant progress in improving its management of information resources to increase interoperability and openness to the public. In particular, GSA's *Data.gov*, the Federal Government's open data portal designed to increase access to Federal datasets, now features over 137,000 datasets from federal, state, local, and academic sources. Over 75,000 of these datasets are from federal agencies, providing access to federal data in open, machine-readable formats, and making it easy for citizens to find government data on important issues that cut across federal agencies.

Agencies are also diversifying their information resource capabilities, with some providing data in both navigator formats and in APIs, and working to improve the usability of data and websites by leveraging public feedback mechanisms. The Department of Health and Human Services (HHS), for example, provides mechanisms to allow researchers to extract knowledge and insights from large and complex collections of digital data in a secure and efficient manner. Other agencies are using APIs to disseminate information like the Department of State (State), which uses an API for global Travel Warnings and Travel Alerts.

Agencies are also making efforts to improve the usability of their most-trafficked public-facing websites in compliance with governmentwide standards set by OMB and GSA. For example, agencies are using the Digital Analytics Program (DAP), which features Google Analytics, to analyze trends and incorporate findings to improve the user experience of web sites. Agencies are also incorporating responsive design for mobile devices to make it easier to access and share content, leverage low cost social media channels to reach citizens, and incorporate additional customer-generated, crowd-sourced input on department websites. For example, the Department of Education (ED) is working with customers to identify and prioritize new features for improving provided resources, and the

Department of Energy (DOE) is streamlining public-facing web operations in order to improve how consumers and business access the information and resources they need.

Agencies are also striving to make particular functions more accessible and useful for relevant external stakeholders. DHS, for example, has developed trusted and secure networks for collaborating and sharing Sensitive but Unclassified Information, in order to ensure the right information gets to the right people at the right time, thus increasing the nation's security and responsiveness. Similarly, the Federal Bureau of Investigation's (FBI) Next Generation Identification System provides authorized entities notifications of criminal history, improving the effectiveness of information sharing among relevant parties who need to be advised in an efficient, timely manner of criminal activity by persons under investigation or supervision.

Other Agencies are putting critical transactional services online in web-based systems for submitting applications and related documents electronically. Numerous agencies have begun using electronic systems to allow users to submit of forms and data, providing them with the ability to view the information quickly and track their submission status online. The Department of Labor's (DOL) *Benefits.gov*, for example, provides citizens with information and eligibility prescreening services for more than 1,000 Federal and state benefit programs across 17 Federal agencies. The Department of Interior (DOI) and the National Archives and Records Administration (NARA) have reduced costs and streamlined programmatic functions by providing integrated electronic enterprise recordkeeping systems and putting forms online.

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 project cost and schedule, risk factors, customer service, and innovative technology adoption and best practices, many of which can be viewed on the Federal IT Dashboard. Select efforts are described in further detail below. The full list of activities can be found on the IT Dashboard.

Performance metrics are an essential tool in helping agencies determine the health and status of their IT portfolios by providing unique measurements on project status, content, 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 and assess performance at both the program and agency-wide levels. To strengthen links to departmental priorities, major IT investments are mapped to specific elements of the agencies' strategic plans. Agencies also require performance measures as elements of business cases for each major IT program. For example, State evaluates IT investments based on Department-identified performance standards and how they align to strategic mission, goals, and objectives such as data integration and interoperability, mobile accessibility, and utilizing existing enterprise license agreements. ED uses value and performance metrics to evaluate its IT investments with its Value Measurement Methodology (VMM), during which the Office of the Chief Information Officer and Line of Business (LOB) senior executives identify mission priorities to which all IT investments align.

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, 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*. The DOI tracks IT performance by ensuring all of its major investments have at least one metric measuring financial performance, one measuring strategic and business results, and three measuring customer satisfaction. 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, such as the Social Security Administration (SSA), also use activities and technology specific metrics to measure programs against defined process standards or technical service level agreements.

Agencies use a variety of governance tools and structures to carry out performance measurement. For example, the Department of Agriculture (USDA) Office of the Chief Information Officer ensures that the interests of key IT investment stakeholders and partners are included at every step of the IT investment life-cycle by monitoring IT projects for the regular use of comprehensive and inclusive project charters that encourage stakeholder and customer involvement. Some agencies, such as the Nuclear Regulatory

Commission (NRC), even 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. Agencies also use IT Review Boards to track project performance against established metrics. To enable decision-making, accountability, and transparency surrounding IT portfolio performance, metrics are reported to Agency management, OMB and the Federal IT Dashboard on a monthly, quarterly, and semi-annual basis. DOE, for example, reports performance metrics related to major IT investments monthly on OMB's IT Dashboard, and also performs internal quarterly control reviews, and a required annual operational analysis to assess the performance of these investments. Investment performance against established goals is a key consideration for agencies in both the Capital Planning and Investment Control (CPIC) processes and in steady state system operational analysis.

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, DOD, the Environmental Protection Agency (EPA), and Treasury use online portals to allow the public to locate, view, understand and comment on federal regulatory actions and rulemaking materials. Similarly, DHS uses web-based crowdsourcing tools to directly engage with the public on a range of issues and policies. Ideas can be submitted directly by the public and individuals may vote for or against an idea and add their comments to the discussion. The Department of Transportation (DOT) also utilizes web-based interactive technology to engage the public, leveraging online dialogues to discuss important topics such as Disadvantaged Business Enterprise training.

While agency websites and internet portals continue to be a mainstay of public-private engagement, many agencies have also begun to utilize social and digital media to pursue this end. The Department of Commerce (DOC) and DOE utilize social media to partner with private sector, state, local, tribal and international governments to develop and share best practices. Agencies such as USDA and the Department of Justice (DOJ) archive live streams of symposiums, town hall meetings, Google Hangouts, and other live events. They also provide links to radio and TV programming and Streaming Media Archives on their websites, in addition to providing access to informative webinars. NRC uses two web-based systems to share public meeting information with the public and to make it easier for the public to provide feedback on meetings. The agency's new Public Meeting Notice Systems (PMNS) uses Twitter to provide up-to-date information on the agency's public meetings. NARA, in developing its Open Government Plan, sought public feedback through blog posts on the NARAtions Blog, the National Declassification Center (NDC) Blog, and the FOIA Ombudsman, along with web page updates and emails to stakeholders seeking their feedback. NARA also conducted in-person consultations with civil society representatives.

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 25,000 global volunteers in hundreds of countries to create thousands of web and mobile applications and hardware solutions to spark innovation in categories

representing the agency's mission priorities: space technology, Earth science, robotics, and human spaceflight, among others. The specific effort, known as the International Space Apps Challenge, was a clear demonstration of the value of leveraging government data and the talent and skill of passionate volunteers from around the planet. Another example of this type of work is the "National Day of Civic Hacking", hosted by the National Science Foundations (NSF), NASA, and others, in which eighty participants competed to "mash" together publicly available data to create a usable application for public use. This year's winning application, "The Ethics Project," uses Congressional data to provide government users with information about company lobbyists.

APPENDIX D. CREDENTIALING

Section 203 of the E-Gov Act (44 U.S.C. § 3501 note) requires that the Federal Government describe the 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. While the implementation of PIV-based two factor authentication varies among Federal agencies, agencies such as the Office of Personnel Management (OPM) continue to lead the way by requiring all privileged users to authenticate using PIV cards. Additionally, some agencies have taken steps to ensure secure log-in for external resources. NRC has issued Federal bridge cross-certified Public Key Infrastructure (PKI) credentials at various assurance levels in order to allow external partners to interact with the agency's authentication systems.

The basic level of compliance sought by HSPD-12 is to require PIV card use for access to facilities and systems, but also as a way to digitally sign emails and documents and select electronic transactions. In some cases, such as at the Small Business Administration (SBA), agencies have found that using PIV credentials reduces other existing investments for help desk operations and password management. Agencies use differentiated levels of credentialing and authentication to meet the varied business needs of their department in the most efficient and cost effective ways. To help spread awareness of such policies, some agencies, such as NSF, are executing comprehensive enforcement campaigns that include technical, communication, and enforcement strategies in order to achieve enforcement targets.

Some agencies have taken additional steps to further utilize PIV credentials. USAID, for instance, implemented control gates within the agency's System Development Life Cycle (SDLC) to ensure that not only are new applications PIV-enabled prior to deployment, but legacy systems implement required credentialing. Other specific agencies, such as OPM, have taken the step of requiring all privileged administrators at the user account level to authenticate via PIV card. Treasury has initiated a specific investment for identity, credential, and access management: the Treasury Enterprise Identity, Credential, and Access Management (TEICAM) investment, which provides a consolidated view of identity management activities across the department and a standard for secure and reliable forms of identification. It also facilitates secure and timely access to information systems and facilities. Additionally, in an effort to continue improving the protection of its information resources, Treasury has established an improvement plan with measurable goals to

continue the development and improvement of its credentialing capabilities.

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, the Administrative Procedures Act (APA) and Section 206 of the E-Gov Act lay out requirements designed to not only increase engagement with the public, but to increase collaboration between government agencies and divisions. 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* 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 *www.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. The DOI, for example, posted 109 rules, 178 proposed rules, and 67 Federal Register notices to *www.Regulations.gov* in FY 2014, providing public access to a total of 60,621 documents. In response, they received 59,221 submissions from the public submissions in *www.Regulations.gov*.

While agency use of *www.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 further integrating 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 the Department'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 the Department to access current information specific to that division. DOL has also developed a new 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. This new website also provides the public a live web experience where the Secretary of Labor and other DOL executive leadership staff answer questions about the DOL regulatory agenda submitted online from the public. State launched a Twitter account with the specific purpose of informing a broader public audience of State's rulemaking actions. When a rule is published, State tweets its subject information as well as a link to the full text of the document on *www.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 governmentwide system that provides agencies the ability to efficiently search, view, download, and review comments on rulemaking and non-rulemaking initiatives. FDMS also enables Department users to manage their 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 264 staff using *www.FDMS.gov* in FY 2014, and created 128 regulatory dockets in FDMS for regulatory actions published in FY14. DOC, another major user of the system, had 196 staff use the system in FY 2014, creating and posting 182 regulatory dockets.

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

Sections 207(d) and (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 were asked to describe 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.

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 (PTR), 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 electronic 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; 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 all systems and programs that involve the collection and storage of personally identifiable information (PII). Through this IPA process, which is incorporated into the Department's IT security framework, DOJ also reviews information technology systems that contain PII and/or 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 the IT system is modified during its operational life cycle, and the modifications impact the technology associated with privacy of information maintained in the system, DOJ requires that a subsequent IPA be conducted to determine whether additional privacy requirements and considerations must be applied to the modified system.

At Treasury, conducting PIAs is an integral part of the process when a Department program is 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 (PTR) 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 PII. To facilitate the process and approval of PIAs, PTR 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 PTR 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 information technology 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.

In December 2013, DOD published the DOD Cyberspace Workforce Management Strategy, a comprehensive strategy to transform its legacy IT and information assurance (IA) personnel into a cohesive cyberspace workforce, with a strong cybersecurity component. DOD is leveraging established training/education venues both internally and externally to maximize development of this workforce. DOD also has technical schoolhouses run by the Military Services and Combat Support Agencies, and six institutions qualified as Centers of Academic Excellence in IA by the National Security Agency and DHS. Commercial training and certification programs provide baseline IA/cybersecurity knowledge for designated jobs. Further, DOD participates with DHS and the State Department to provide online, on-demand training through the Federal Virtual Training Environment (FedVTE). DOD meets Privacy Act (PA) training requirements of OMB Circular A-130, "Management of Federal Information Resources," and DOD 5400-11R, "Department of Defense Privacy Program" through a 4-day Defense Privacy Officer Professionalization Program; 3-day PA Compliance & Management course; System of Records Notice and Breach Management training workshops; Privacy Impact Assessment/systems owner training; and PA Essentials course. DOD Components also provide annual and refresher PA training courses.

At ED, the Information Assurance and Privacy Safeguards programs develop required cybersecurity and privacy awareness training for all government employees and contractor staff to include mandated, specialized privacy training for those dealing with Department data. In FY 2014, ED enhanced its 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) Decreasing the average completion time by 30 minutes; (5) Releasing training earlier to allow more time for completion; and, (6) Improving readability of training and testing as measured by the Flesch Reading Ease Scale. The Department achieved a 100% completion rate for both cybersecurity awareness and role-based training. Additionally, in support of the Department's move towards a hoteling concept, as well as teleworking, the ED Office of Management (OM) is in the process of identifying requirements to enhance the technological features of the training facility to expand its offerings to a more remote workforce. OM has also partnered with OPM's Human Resource University to take advantage of the many online courses they have developed and made available governmentwide.

The Department of Housing and Urban Development's (HUD) Security Awareness Program consists of several components designed to protect the confidentiality, integrity,

and availability of HUD's information systems and the information they contain. These components consist of mandatory annual security awareness training, weekly security awareness tips disseminated to all employees, and security alerts as circumstances warrant. HUD's Computer Self-Help Desk is a one-stop website providing tricks and tips on Microsoft Office applications such as Word, Excel, and PowerPoint to that is available to all employees. The Office of the Chief Information Officer's Virtual Training site also offers employees additional Microsoft training opportunities via LiveMeeting or classroom sessions. New classes are added monthly. The HUD Virtual University offers employees access to over 2,000 online courses from the Skill Soft courseware libraries as well as custom courses developed by HUD program organizations.

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. § 3604) – 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 – Governmentwide 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(d) and (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) (44 U.S.C. § 3501 note) – Report on agency compliance with establishing information technology training programs.	Appendix H – Agency Information Technology Training Programs

END NOTES

i P.L. 107-347, Sec. 101(a), codified at 44 U.S.C. §3606. E-Government report. (a) Not later than March 1 of each year, the Director shall submit an E-Government status report to the Committee on Governmental Affairs of the Senate and the Committee on Government Reform of the House of Representatives. (b) The report under subsection (a) shall contain— (1) a summary of the information reported by agencies under section 202(f) of the E-Government Act of 2002; (2) the information required to be reported by section 3604(f); and (3) a description of compliance by the Federal Government with other goals and provisions of the E-Government Act of 2002. *http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf*.

ii P.L. 109-282, Sec. 2(g), codified at 31 U.S.C. 6101REPORT.— (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*.

iii Treasury notes that this is owned by Treasury and funded through appropriation.