FY 2012 Report to Congress on the Implementation of The E-Government Act of 2002

March 2013

Table of Contents

Introduction

This is the Office of Management and Budget's (OMB) tenth annual progress report on implementation of the E-Government Act of 2002 (Pub. L. No. 107-347; Dec. 17, 2002) (the "E-Government Act") as required by 44 USC 3606. This report describes information technology (IT) activities completed in fiscal year 2012 (FY12) that fulfill the requirements of the annual E-Government (E-Gov) Act report to Congress. All reports on the implementation of the E-Government Act from fiscal year (FY) 2003 through the present are posted on the Office of Management and Budget (OMB) website at http://www.whitehouse.gov/omb/e-gov/docs.

Since the passage of the E-Gov Act, Federal agencies have made significant progress in using the Internet and other technologies to improve citizen access to Government information and services, improve Government decision making, and enhance accountability and transparency. This year's report includes a status update on Federal agency activities under Title II, Section 202(f), and provides information required by Section 3604(f). Agency activites required under Title III can be found in the annual Report to Congress on the Implementation of The Federal Information Security Management Act of 2002. This year's report also includes reporting on implementation of the Federal Funding Transparency and Accountability Act of 2006 (Pub. L. 109-282; Sep. 26,2006).

This year's report has been restructured based on discussions with Federal agencies, evaluating best practices, and other recommendations OMB has received and primarily focuses on provisions and goals of the E-Gov Act. The report is structured as follows: Section I describes the use of the E-Government Fund, established by Section 3604 of the E-Government Act. Section II highlights the IT Dashboard, including the accuracy of its data, and complies with the E-Government Act's requirement to make Government information accessible. Section III describes activities the Government has implemented that improve the skills of the Federal workforce. Section IV describes how IT is used to support disaster management activities. Section V describes the use of standards and collaboration for geographic information within the Federal Government. Section VI illustrates Federal Government activities that implement E-Government Act provisions and goals, particularly those that support enhanced delivery of information and services to the public and highlights of agency work in capital planning and investment control, of all which support requirements under the E-Gov Act. Section VII provides an update on provisions required under Title II of the E-Gov Act. Additional information concerning other provisions of the E-Gov Act that are not discussed in this report can be found on the Office of E-Government and Information and Technology website at www.whitehouse.gov/omb/e-gov, the Office of Information and Regulatory Affairs website at www.whitehouse.gov/omb/inforeg, and the Chief Information Officer Council website at www.cio.gov.

Section I: E-Government Fund

The E-Government Act of 2002 improves the management and promotion of electronic Government services and processes by establishing a Federal Chief Information Officer within the Office of Management and Budget, and by establishing a framework of measures that require using Internet-based information technology to improve citizen access to Government information and services, and for other purposes. Section 3604 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. All projects supported by the E-Gov Fund must serve one of three purposes:

- 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.
- 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.

A summary of FY12 funding allocations for each investment area, activities, and accomplishments are summarized below.

Funding Allocation Summary

Investment Area	Allocation
Accelerate Cross-Government Innovation	
Cloud Computing and Security	$3.75M
Innovations in Technology	$2M
Promote Transparency and Accountability	
Federal Funding Accountability and Transparency Act (FFATA) Implementation	$2.2M
Performance Dashboards	$2.2M
Accessible and Transparent Government Information	$2.25M

Accelerate Cross-Government Innovation: Cloud Computing and Security

Cloud computing offers an opportunity to significantly improve the efficiency of the Federal Government's IT infrastructure by allowing agencies to reduce their spending in building and maintaining costly IT infrastructure, and focusing on paying for IT resources in response to fluctuating program demands. The Federal Risk and Authorization Management Program (FedRAMP) accelerates Government-wide adoption of secure cloud computing by establishing baseline security assessments and continuous monitoring requirements using National Institute of Standards and Technology (NIST) standards and guidance that must be adhered to by all cloud providers. FedRAMP puts in place a

consistent approach to independent, third party validation of compliance of cloud systems with these security requirements, and enables agencies to leverage security authorizations, avoiding expensive, duplicative security work. This investment also includes approaches that may be used to support the development of Government-wide solutions to improve utilization of IT resources.

Actions:

- Established a unified Government-wide process and baseline security requirements for assessing, authorizing, and continuously monitoring cloud computing services at low and moderate risk levels. The process and requirements create an efficient framework for agencies to leverage cloud computing security authorizations to save time, money, and staff resources.
- Launched the FedRAMP Initial Operating Capability in June 2012.
- Instituted a program to accredit third party assessment organizations (3PAOs) who provide independent verification and validation of cloud service provider security implementations in the FedRAMP process. Currently, there are 15 vendors accredited, 40% of which are small businesses. Over 50 applicants were reviewed.
- Created a program management office (PMO) to process applications and facilitate reviews by the FedRAMP Joint Authorization Board (JAB) comprised of the Chief Information Officers (CIOs) of the Department of Defense (DOD), the Department of Homeland Security (DHS), and the General Services Administration (GSA). The PMO works with the JAB and cloud service providers to grant provisional security authorizations of cloud services for Federal agencies to use. To facilitate efficiency, the PMO provides Federal agencies with templates on process requirements, contracting guidance to meet security requirements, and support in meeting FedRAMP requirements. Currently, there are 59 applicants.

Accelerate Cross-Government Innovation: Innovations in Technology

This investment area supports initiatives that enhance citizen engagement by simplifying and improving access to Government information through increased use of mobile and web technologies. This investment area supports initial funding for BusinessUSA, a new platform that consolidates information and services from across the Government into a single, integrated network for American business owners and entrepreneurs. BusinessUSA allows businesses to search through full range of Government information, programs, and services in a more streamlined manner.

Actions:

- Worked with the American Job Center team, the Department of Labor (Labor) and other agencies to support the development and launch of the American Job Center (http://jobcenter.usa.gov/) website; provided initial funds to host and design content, including a redirect plan for related pages on USA.gov.
- Launched BusinessUSA.gov in February 2012 working with Department of Commerce (Commerce), the Small Business Administration (SBA), and other agencies.
- Deployed web resources for the Digital Services Innovation Center in June 2012.
- Prepared web performance guidance (http://www.howto.gov/web-content/digital-metrics) and customer experience metrics (http://www.howto.gov/web-content/digital-metrics/digital-analytics-program) in support of the Digital Government Strategy[1].

[1] Digital Government, Building a 21st Century Platform to Better Serve the American People: www.whitehouse.gov/digitalgov/html5

Promote Transparency and Accountability: Federal Funding Accountability and Transparency Act (FFATA) Implementation

The USAspending.gov website was created to fulfill the Administration's commitment for an open and transparent Government, consistent with the requirements under the Federal Funding Accountability and Transparency Act (FFATA) and the charge under the Administration's Government Accountability and Transparency Board (GATB). USAspending.gov is a public-friendly system that provides easy access to information related to Government funded contracts, grants, loans, and forms of financial assistance. This information may be searched and sorted by recipient, locations, and other information selected by the user. Additionally, the FFATA Subaward Reporting System (FSRS) supports the capture and reporting of subaward and executive compensation data on first-tier subawards under grants and contracts subject to the FFATA reporting requirements and provides some visibility to Federal funds flow through state governments to cities and counties. USAspending.gov has been used by Congress and a variety of non-federal stakeholders including state governments, non-profit organizations, and organizations interested in federal spending trends and transparency. While stakeholders have acknowledged the unprecedented levels of transparency the site provides, they have identified areas of improvement both in the view and functionality of USAspending.gov and FSRS, the subaward reporting system. While stakeholders have raised important areas for improvement, continuing budgetary constraints impede opportunities to address continuing system challenges, some of which may have resulted in additional reporting burden. For financial assistance, it is currently estimated that over 1 million burden hours are associated with reporting under FFATA.

Actions:

- In June, 2012, GSA modified the application programming interface (API) algorithm used for matching contracts sent from IT Dashboard to increase the match rate.
- Consolidated and more fully integrated the USASpending site with the Federal Procurement Data System (FPDS) that provides the agency procurement data feeds. USASpending.gov and FPDS now share the same hosting platform. The result has been that data displayed is more consistent with FPDS.
- Provided agencies with the ability to submit additional financial assistance data directly using the USAspending.gov Data Submission and Validation Tool (DSVT).
- Data feeds into USAspending.gov, including key information on Federal awardees, formerly contained in the Central Contractor Registration System (CCR), have begun to be consolidated into one technology platform, the System for Award Management (SAM).

Promote Transparency and Accountability: Performance Dashboards

A key component of performance management is transparency of the key activities and related metrics of operations in agencies. Performance.gov was created to publiscly share information in support of the Government Performance and Results Act Modernization Act of 2010 (GPRAMA) and the Federal Infrastructure Permitting Dashboard have increased transparency and information availability to the public. Among recent performance areas highlighted are Federal infrastructure projects, which show Federally funded projects, descriptions, costs and progress. This investment enables continued operations and some enhancements to ensure improved usability and utility both by agencies and the public.

Actions:

- Updated the Performance Reporting Entry Tool (PREP) capability with guidance and workflow in July 2012.
- Worked with the Performance Improvement Council (PIC) to finalize Cross-Agency and Agency Priority Goal requirements for Performance.gov 2.0 design and platform architecture in June 2012 to meet the the first phase of GPRAMA requirements and serve as the foundation for substantial improvements in FY13.
- Agencies have identified and are expediting and tracking progress on 15 High Priority and 23 nationally or regionally significant projects on the Federal Infrastructure Projects Permitting Dashboard. Since August, the public was able to access to the application programming interface (API) features to allow automatic data feeds to other applications. These feeds are particularly useful for IT software developers.

Promote Transparency and Accountability: Accessible and Transparent Government Information

This investment area will support the on-going effort to make Government data and information open and easily accessible to citizens and businesses. Data.gov allows high value, machine readable, data sets that are generated and held by the Federal Government to easily be found, downloaded, and used by the public. Importantly, Data.gov serves as a vehicle to harmonize information dissemination across the Federal enterprise and significantly supports the Data Quality Act. Online communities have been established in such critical areas as health, energy, environment, and education to harness the power of the over 400,000 data sets to fuel innovation and develop new products and services. The system is a flagship initiative of an open and transparent Government globally, and it has been emulated by 35 other nations that have established government open data sites.

Actions:

- Held the second International Open Government Data Conference July 10-12 in Washington, DC, where open government data advocates and developers from around the world presented on topics such as Privacy and Security, Geospatial Innovations, Mobile Apps, E-Democracy, Semantic Web, and more. This event was held by the Data.gov team in collaboration with the World Bank.
- Listed 378,000 datasets from over 180 agencies and sub-agencies and over 1,200 data extraction tools in machine-readable catalogs in FY12.
- Offered over 150 interactive datasets in a cloud platform on Data.gov that allows easy creation of data visualizations, geo-coded maps, and application programming interface (API) support for mobile applications.
- Data.gov now has 15 Communities such as Education, Energy and Health communities, that enable the public to explore, discuss, meet others in the same field, and develop the data and apps in a field of interest.
- Announced the deployment of the Open Government Platform (OGPL) in June 2012 as part of the U.S. India Strategic Dialogue. This deployment was announced by the Data.gov team in coordination with the Executive Office of the President, the Department of State (State), the U.S. Agency for International Development (USAID) and the Government of India (GOI) National Informatics Centre. The effort makes the Data.gov software available in open source code to allow other countries to become more transparent and make their governmental data public.
- Thirty-five countries have emulated or applied Data.gov features to their own data websites.

Section II: IT Dashboard

This section highlights updates to the Federal IT Dashboard, is a web-accessible application that enables agencies, industry, the public, and other stakeholders to view details of Federal information technology investments at http://itdashboard.gov. The purpose of the IT Dashboard is to provide information on the effectiveness of Government IT programs and to support decisions regarding the investment and management of resources. The IT Dashboard continues to be a valuable tool in driving accountability and transparency in Federal IT spending and management. Using IT Dashboard data, OMB and agencies have strengthened the TechStat process, routine IT investment performance oversight, and budget analysis. Highlights in FY12 included improvements to the data schema and the development of a user-accessible interactive log of every update to the investment's data.

Improving trend analysis

The IT Dashboard now includes an interactive log of all updates or changes to an investment over time, allowing users to see the complete history of an investment at a glance. IT Dashboard users can now select any historical update and see a comparison of the before-and-after view of the investment at that time. This helps analysts understand the full picture of an investment's transition over time rather than just a current snapshot.

Section III: IT Workforce

The E-Government Act requires improvement of the skills utilized by the IT workforce in using information technology to deliver Government information and services. The activities described below are highlights from FY12.

In July 2011, OMB issued guidance to agencies on developing specialized IT acquisition cadres: http://www.whitehouse.gov/sites/default/files/omb/procurement/memo/guidance-for-specialized-acquisition-cadres.pdf. OMB's Office of Federal Procurement Policy and Office of E-Government and Information and Technology worked very closely to develop this guidance and utilized best practices from several agencies utilizing these cadres successfully. This guidance described how agencies could design, organize, and develop a cadre of contracting professionals, program managers and contracting officer's representatives to ensure these functions work closely throughout the acquisition process to create better program outcomes. Many agencies have utilized the guidance in FY12 to implement these cadres.

The Office of Personnel Management (OPM) has developed the IT Program Management Career Path Guide and recommended training curriculum for the newly-established Information Technology (IT) Program Management job title. OPM worked closely with the Chief Information Officers (CIO) Council and the U.S. Office of Management and Budget (OMB) on this project, initiated in May 2011, and included subject matter expert participation in various focus group meetings to develop the content for this product. The resulting resource builds upon the IT Program Management Competency Model released by OPM in July 2011 and provides guidance to Federal agencies on the creation and improvement of the IT Program Management career path at each agency. In November 2011, OPM published the IT Program Management Career Path Guide (http://www.chcoc.gov/transmittals/TransmittalDetails.aspx?TransmittalID=4413).

In August 2012, the White House launched the Presidential Innovation Fellows Program (http://whitehouse.gov/innovationfellows), which pairs entrepreneurs from the private sector, non-

profits, and academia with the Federal Government in a collaborative setting to address high-impact challenges that will produce significant results in approximately six months. These projects are primarily targeted to reduce costs, increase job growth, support agency mission goals, and provide tangible benefits to the public.

Section IV: Disaster Preparedness

The Office of Management and Budget (OMB) in consultation with the Department of Homeland Security (DHS), and Federal Emergency Management Agency (FEMA) are required to report to Congress on activities that further the goal of maximizing IT use in disaster management. Three of the E-Government initiatives that are managed by the Department of Homeland Security (DHS) support disaster preparedness, response and recovery: Disaster Assistance Improvement Program (DAIP), SAFECOM, and Disaster Management (DM). Each initiative uses IT in a different way when coordinating and facilitating information. Below is a brief description of IT use in each initiative.

DAIP maintains a Government-wide, single portal for disaster survivors to submit electronic applications for assistance. The mission of DAIP 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. DisasterAssistance.gov provides disaster survivors with a single source for potential assistance programs, easy access to the application, application updates and disaster related information.

In FY12, DAIP focused on increasing disaster survivors access to needed assistance, regardless of where the survivors are located. In the days immediately following a disaster, survivors are often displaced, without access to their residence, traditional landline telephones and desktop computers. Providing access to critical recovery mechanisms via web-enabled mobile devices allows survivors to begin the recovery process sooner. DAIP launched mobile optimized versions of DisasterAssistance.gov's questionnaire and application status inquiry in August 2012 to complement mobile registration capabilities developed in FY10.

Following a presidentially declared disaster for individual assistance, survivors in need of assistance can register online at DisasterAssistance.gov. Each year approximately 50 presidentially declared disasters cause injury and death, destroy homes and businesses, and disrupt the lives of hundreds of thousands of people across the nation. DisasterAssistance.gov brings together all Federal agencies that offer forms of disaster assistance to simplify the process for survivors. Users can apply for DHS/FEMA individual assistance and Small Business Administration (SBA) loans through online applications and can also receive referral information on forms of assistance that do not currently offer online applications. The DisasterAssistance.gov web portal eases the burden on disaster survivors and increases their access to disaster relief by creating a continually updated information clearinghouse that provides information on the assistance most valuable to a disaster survivor, such as housing, food and employment aid in both English and Spanish. DisasterAssistance.gov reduces the time needed to apply for aid and to check the status of claims while decreasing redundancy in application forms and processes. The portal ensures that disaster survivors, who may be displaced or otherwise out of contact, continue to receive benefits from non-disaster related assistance programs. Application information is shared only with those agencies that the user selects.

The E-Government (E-Gov) Act of 2002 mandates that the Government pursue opportunities to leverage Information Technology (IT) in a cost effective way to enable the Federal Enterprise to be more citizen-centered and market-driven. The DM program is dedicated to leveraging innovative IT solutions to

modernize and web-enable Government services, increase responsiveness to citizens and to business, and enhance Government-wide efficiency and cost effectiveness. The DM program's mission is to improve accessibility and availability of timely, accurate disaster-related information to the public, those affected by disaster, first responders, emergency managers, and others. The program is essential to the overall FEMA mission to enable first responders to communicate and collaborate with local resources, while providing the capability to coordinate upward and outward with supporting resources. The services of the DM program are designed to minimize loss of life and property by enabling emergency response personnel to broadly share real-time situational awareness information.

The integration of the website with FEMA Call Centers provides a greater degree of self-service and answers to Frequently Asked Questions (FAQs). All program activities work to ensure ease of access to services, as well as to assist those seeking services the ability to obtain support more quickly and effectively.

DM facilitates the development and adoption of emergency data exchange language standards for incident management, thus enabling the emergency response community to seamlessly and securely share data across disparate information systems. The Emergency Notification System consolidates multiple smaller notification and alert systems and results in a single resilient program to provide cost effective capability to provide notifications and alerts as an enterprise level service to all of DHS.

DM has implemented a disaster assistance knowledge base as part of a call center/website integration effort, which has streamlined and improved the availability of consistent, timely disaster-related information to citizens. The DM Initiative also leads and supports efforts within FEMA to consolidate portals and other public facing web properties in an effort to improve access to disaster related information for all stakeholders. Ownership of both DM-Framework and DM-OPEN have been transitioned from the DM program to the FEMA National Continuity Programs (NCP) Integrated Public Alerts and Warning System (IPAWS). This effort was completed in September 2011.

The DM FY11-FY12 plan focuses on supporting the President's Open Government initiative by providing transparency via the ability to provide timely, findable, accurate information in usable formats on FEMA websites, through participation and collaboration, development and utilization of tools, methods, and systems that allow data to be analyzed and accessed easier for decision-making, and web consolidation, website management and outreach, and integration of the Disaster Assistance Knowledgebase and Call Center/Website Integration. Priorities include:

- Continued rollout of the CMS across DHS components;
- Consolidation of Web content to more easily access information on cross-cutting national initiatives that FEMA manages for the benefit of Federal departments and agencies and the American people, such as the National Exercise Program, National Training Program, lessons learned and corrective action platforms, grant programs, and FEMA's role in coordinating the Federal response and recovery efforts during disasters;
- Update and enhancements to FEMA mobile site and the FEMA mobile application; and
- Research, design, and development of emerging technologies.

Through collaboration with emergency responders and policymakers across all levels of Government, SAFECOM works to improve multi-jurisdictional and intergovernmental communications interoperability. The SAFECOM Executive Committee (EC) and SAFECOM Emergency Response Council (ERC) work 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 FY12, SAFECOM updated and delivered the annual SAFECOM grant guidance document to help maximize the efficiency in which public safety communications-related funds are allocated and spent; developed and delivered the Public Safety Communications Evolution Brochure to help educate the public safety community and elected and appointed officials about the future of emergency communications; provided guidance and support to the Office of Emergency Communications as it conducts follow-up, state-wide planning evaluation activities; and provided guidance and support to the Office of Emergency Communications in its delivery of state-wide and tactical technical assistance to state, local, and tribal governments and first responder organizations.

The SAFECOM website (http://www.safecomprogram.gov/) provides members of the emergency response community and other constituents with information and resources to help them plan for effective interoperable emergency communications for disaster preparedness, response, and recovery. It offers comprehensive information on topics relevant to emergency response communications and features best practices that have evolved from real-world situations.

Section V: Geospatial

In an effort to reduce redundant data collection and information, the E-Government Act requires the promotion of collaboration and use of standards for Government geographic information. The effective and efficient development, provision, and interoperability of geospatial data and services serve in the best interest of both the Federal Government and the public. Cross-agency coordination of geospatial activities can identify, consolidate, and reduce or eliminate redundant geospatial investments. Through interagency collaboration, common business, content, and technology requirements are identified to enable the development and implementation of standards that improve data quality and utility, ultimately increasing access to geospatial data. Recently, the Geospatial Platform website (www.geoplatform.gov) was revised to improve site navigation and information management.

The Geospatial Line of Business (LoB) is a Government-wide initiative supporting effective delivery of geospatial data, services, investments, and better utility across the Federal Government investments. In 2012, Geospatial LoB activities centered on implementation of the Geospatial Platform as a mechanism for developing shared services. The Geospatial Platform demonstrates advancement in our collaborative effort to support geospatial activities across agencies and governments and helps to improve the efficiency of government by making geospatial data more accessible, reliable, and less expensive to acquire through enhanced data-sharing and more effective management of resources. The Geospatial Platform offers access to trusted geospatial data, services, and applications managed in the Federal Geospatial Portfolio to support Federal, State, local, and Tribal governments in meeting their mission objectives, and provide efficiencies and cost savings through shared infrastructure and enterprise solutions.

In FY12, the Geospatial LoB conducted a review of the Data Themes identified in the Supplemental Guidance under OMB Circular A-16 to assess validity and data stewardship responsibility. Data themes are electronic records and coordinates for a topic or subject, such as elevation or vegetation. This review yielded a reduction in the number of Data Themes and in some instances, a reassignment of the agency stewards to increase efficiency. This review further defined the processes, roles, and responsibilities for managing National Geospatial Data Assets datasets and themes, and provided a repeatable process for modifying OMB Circular A-16, Appendix E, which describes the geospatial data themes that will be used for portfolio management.

- The Geospatial Platform Value Proposition was completed to validate the needs for a platform including: supporting decision making, addressing issues of National importance, and meeting common business needs.
- The Geospatial Platform Business Plan was developed to serve as a "what and how" document, providing an overview of the operational elements and the organizational structure of the Geospatial Platform.

Federal geospatial assets across the Government were inventoried and evaluated for strengths and weaknesses. This inventory determined outdated requirements and resulted in reducing the number of data themes from 33 to17 in effort to more effectively manage data in support of national priorities. The sharing of data, services, and applications through the Geospatial Platform provided a reduced cost for data, hardware, and software, and increase information technology (IT) security and efficiency. The sharing of data, services, and applications through the Geospatial Platform allows Federal agencies the opportunity to invest in one cloud based "Platform" instead of maintaining numerous Partner Agency platforms, providing users a faster, more flexible, and more economical way to share information.

Geospatial Platform Version 1 has been developed and provided improvements in the areas of:

- Enhanced new user account and registration functionality,
- A new administration page for managing user accounts,
- Enhancements to search capabilities through implementation of an algorithm for incorporating spatial relevance into search results,
- Implementation of the Federal Geographic Data Committee (FGDC) Service Status capabilities with the Platform catalog (http://geo.data.gov/geoportal/catalog/main/home.page), and
- Tighter integration with the data.gov activities and approval workflows.

Section VI: Highlights of Agency E-Government Activities

The E-Government Act of 2002 was enacted to promote the use of the Internet and other technologies to improve citizen access to Government information and services, improve Government decision making, and enhance accountability and transparency. Section VI provides highlights of agency activities that enhance delivery of information and services to the public and agency capital planning and investment control procedures for IT.

A. Enhanced Delivery of Information and Services to the Public

Department of Agriculture

Drought Data, Code Sprint

During the 2012 crop year, The Department of Agriculture (USDA) has given Secretarial disaster designations to more than 2,300 counties due to drought, one of the worst droughts in decades. As individuals across the country are seeking support, USDA reached out to the software programmer/developer community to encourage their use of publicly available Government information to help farmers, ranchers, and others. Specifically, USDA promoted the development of quick and reliable "one-click" access to information on drought conditions and Federal drought relief programs and efforts. For citizens in desperate need, too much time can be consumed searching multiple web sites, and reaching out to different offices or contacts. Also, there is a risk of receiving outdated or incorrect information. By making USDA's information accessible in one place through a tool or app, farmers,

ranchers and others can trust its reliability and currency. USDA reached out to the agriculture community, web and app developers and other related industries to generate interest to help solve this problem and make Government information more accessible. For example, USDA the media and websites to helped promote the effort and conducted interviews in various outlets.

Department of Defense

Defense Manpower Data Center

The Defense Manpower Data Center (DMDC) is now making it easier for service members and their families to obtain and maintain identification (ID) cards. The center has launched its Real-time Automated Personnel Identification System (RAPIDS) self-service portal. RAPIDS allows anyone with a Department of Defense (DOD) common access card (CAC) to apply for family ID or retirement cards, or update dependents' statuses online.

This is part of a larger, overall effort to improve and transform the entire ID card application process so that customers are able to shift towards online services. Before RAPIDS, service members, retirees and families had to jointly visit a Defense Manpower Data Center in person to submit an application form, and then wait until the ID card was processed and printed. Now, CAC holders may access the RAPIDS site using their CAC instead of visiting the DMDC in person with the entire family. Using the CAC, service members may access RAPIDS to provide a list of dependents, complete and digitally sign the form No. 1172-2 in order for their family members to receive an ID card. After this step has been completed, family members may individually visit the closest DMDC to pick up the ID card. This new process for ID card issuance allows more flexibility for service members and their families as they no longer must visit a DMDC jointly for applying for ID cards.

RAPIDS also allows service members to register for a DOD self-service user name and password, known as a DS Logon. DS Logon allows access to several DOD and VA websites, rather than requiring a CAC for access. DS Logon, which is available only to CAC holders, also has a "premium account" feature that provides the highest level of access, allowing an authorized user to view their personal data in the DOD and VA systems, apply for benefits online, check the status of claims and update address records.

DMDC will continue to expand its self-service options to include changing email certificates and information about family members. The upgrades include an effort to put the fingerprints of new recruits into the system, so lost paperwork can easily be replaced.

Department of Education

Integrated Student Experience

The Integrated Student Experience program, composed of StudentAid.gov, new media, and mobile interfaces, was released in July 2012. This initiative improves the customer experience by leveraging technology more effectively to better meet the demands of customers and to improve efficiency, expand access to higher education, and support customer decision making. The program is the Department of Education's (ED's) signature initiative in response to Executive Order 13571 on improving and streamlining customer service.

StudentAid.gov is the first phase in a project to consolidate Federal Student Aid's web presence. This release allowed for the decommissioning of five websites, resulting in significant cost savings (over $1.5 million) and streamlined internal processes. Content from across FSA's student- and borrower-facing

web portals and publications was reviewed, streamlined and rewritten to ensure plain language. StudentAid.gov was developed on an open-source content management system and uses a responsive design for the site to be accessed on any device. Future phases will continue to consolidate functionality from other FSA websites to further reduce the access points for students/borrowers, eliminate confusion, and increase financial literacy. StudentAid.gov has received over 8 million unique visits in the three months since its launch and is expected to serve over 30 million annual visitors. Mobile visits account for 11% of traffic. Customer feedback is closely monitored, and enhancements are planned based on feedback and usability testing.

As part of the Integrated Student Experience, FSA released and updated digital properties to interact with its customers where they are, using new media. A social media page was launched, a micro blogging account was created, and online video sharing sites were used to reach customers with engaging content. FSA is also engaging users on micro blogging sites (@FAFSA); "#AskFAFSA Office Hours" is hosted once a month, where users can ask FSA employees or subject matter experts questions and receive live answers.

Department of Housing and Urban Development

Community Planning and Development (CPD): eCon Planning Suite

On May 7, 2012, HUD launched the eCon Planning Suite, comprised of an expanded planning database, CPD Maps and the Consolidated Plan (Con Plan) template. This suite is designed to make place-based, data-driven strategic investment decisions achievable by grantees with varying levels of capacity. Moreover, as a public-facing website, CPD Maps promotes more informed and constructive public participation in the Con Plan process by making the same planning data accessible to community members as well as grantees.

All Community Development Block Grant (CDBG), HOME Investment Partnerships (HOME), Emergency Solutions Grant (ESG) and Housing Opportunities for Persons with AIDS (HOPWA) recipients will use the e-Con Planning Suite to assess their affordable housing and community development needs and make strategic funding decisions in response to these needs.

CPD Maps is built on HUD's existing Enterprise Geospatial Platform, combining demographic and market data from Census and investment data from CPD, Public and Indian Housing (PIH) and Multifamily divisions at HUD. The electronic Con Plan submission template was built within the Integrated Disbursement and Information System (IDIS), CPD's grant management and reporting system. CPD Maps and the Con Plan template are connected to each other, allowing data and maps to be imported from CPD Maps into Con Plans in IDIS and IDIS data to be displayed on CPD Maps.

Since the eCon Planning Suite rollout, CPD has held national webinars, reaching thousands of attendees, to introduce these new tools, demonstrate their usefulness and answer grantee questions. Technical assistance providers are providing in-person trainings and developing a number of toolkits and other technical assistance products. As of November 15, 2012 all grantees will be required to use these tools to prepare and submit their Con Plans.

Department of Justice

Victims Compensations Fund Management System

The Victims Compensation Fund Management System (VCFMS) was launched in October 2011 for the purpose of assisting the Department and the Victim Compensation Fund (VCF) Special Master to meet

the statutory requirements of the Zadroga Act in a comprehensive and cost-effective manner. The VCFMS is a secure web based Claims Management System for use by the VCF Special Master and staff to process compensation claims under the Zadroga Act. Title II of the Zadroga Act reactivates the September 11th VCF of 2001 and requires the VCF Special Master to provide compensation to any individual (or a personal representative of a deceased individual) who suffered physical harm or was killed as a result of the terrorist-related aircraft crashes of September 11, 2001, or the debris removal efforts that took place in the immediate aftermath of those crashes.

The website was set up to support making the September 11th VCF as fair, transparent, and easy to navigate as possible. On it, the claimant is able to: file a claim with the VCF, obtain a list of the kinds of documents and information that are needed to process the claim, and review updated Frequently Asked Questions. In addition to facilitating the application process to members of the public who may qualify for this program, the website includes enhancements to improve Government interaction with the public and industry-proven security tools to prevent misuse of information. Current estimates are that as many as 70,000 claims may be filed with an estimated 40,000 awards through FY16.

Department of State

Passport Card Application Pilot

The Bureau of Consular Affairs (CA) developed a functional Passport Card Application Pilot that demonstrated the Passport Services Directorate's ability to accept, adjudicate and archive an online application for a passport card. The Passport Card Application Pilot enabled applicants who possess a current, fully valid U.S. passport book to upload an acceptable digital photograph to the Internet and make an online payment to apply for a U.S. passport card online. The Pilot was used by State to determine if accepting electronic signatures would be feasible for customers while also maintaining the integrity of the U.S. passport as evidence of U.S. citizenship. Accepting electronic signatures and payments reduced processing times, overall cost, and eased the application process for U.S. citizens traveling by land and sea to Mexico, Canada, the Caribbean, and Bermuda.

The scope of the Pilot size was set at 90 days duration or 70,000 applications, whichever came first. The Pilot was initiated on January 24, 2012 and closed on April 27, 2012. Once the Pilot was closed, the Project Manager analyzed the data collected during the project and made recommendations for changes to the Pilot to prepare it for full roll out to the public. The public response to the Pilot was generally favorable, and over 2,500 applications were processed. Successful applications were processed in an average of eight days. Based on this analysis and feedback, CA plans to implement an online system for the renewal of both Passports and Passport Cards when the new system framework is implemented in approximately two to three years that will better support this online process.

Department of Transportation

Project Yellow Light Anti-Distracted Driving Video Contest

Project Yellow Light Anti-Distracted Driving Video Contest is a web-based initiative DOT co-sponsors where the participants use a variety of web and social media based technologies to promote ideas on how to stop distracted driving by teens. To build greater awareness among teens on the dangers of distracted driving, DOT and industry partners are co-sponsoring a nationwide search for the best "viral" (highly viewed) video with a message against distracted driving. Now in its second year, the contest will expand to both high school and college students. The winning PSAs will be announced as part of Global Youth Traffic Safety Month in May 2013 and will be distributed nationally. Winners will receive prizes

that include college scholarships and One-Day Teen Survival Skills Classes at the Skip Barber Racing School. This project helps to deliver the message to a much broader group of kids around the country about the dangers of distracted driving; without National Highway Traffic Safety Administration's (NHTSA's) support and links to information, the program would be less impactful for consumers around the country.

Department of the Treasury

CADE 2

The Internal Revenue Service (IRS) modernization efforts focus on building and deploying advanced information technology systems, processes, and tools to improve efficiency and productivity. In 2012, the IRS delivered the most significant update to its core tax processing system in decades with the deployment of the Customer Account Data Engine 2 (CADE 2) modernization program. After more than 50 years of posting returns and transactions on a weekly batch cycle, on January 17, 2012, CADE 2 moved the IRS to a daily cycle for tax processing of individual taxpayer accounts. Also, for the first time, IRS processing systems accept all 1040 forms electronically through a modernized e-filing capability and will feed into a single consolidated taxpayer account database, which will reduce the handling and mailing of voluminous paper returns.

Prior releases of CADE could only provide daily processing of simple tax returns. CADE 2 Daily Processing enhances IRS tax administration and improves service to taxpayers by enabling faster refunds for more taxpayers, more timely account updates, and faster issuance of taxpayer notices. The CADE 2 Database will support IRS's data-centric vision by improving data quality and providing more data to make decisions in administering the tax system. The relational database is extremely complex, housing taxpayer account data for more than 270 million individual filers, with more than a billion tax modules.

Department of Veterans Affairs

eBenefits Portal

The Department of Veterans Affairs (VA) and the Department of Defense (DOD) collaborated to develop the eBenefits Portal in support of Executive Order 13426, which recommended the creation of a web portal to provide the wounded, injured, and ill service members and veterans, their family members, and care providers a single, transparent, central access point to online benefits.

The eBenefits Portal was designed to enhance the customer experience and reduce the total time to process a claim. The new self-service system is a custom designed interactive tool built to empower the veteran, service members, and their dependents to obtain benefit information on demand. It has the capability to submit claims electronically in a guided, secure, easy to use format. The features and benefits of this new portal have had an immediate and positive impact; claims maintained in electronic form allows processing to occur anytime and anywhere and increased efficiencies (e.g., reducing or eliminating the cost of paper and storage). Veterans and service members may check a previously submitted claim status online. If a claimant is already in the system, then the claimant's information is pre-populated in the forms, which reduces the time required to complete forms. The pre-population also increases the accuracy of a claimant's personal data. If there is incorrect claimant information on a form, a claimant is able to report this issue to VA "live" online. The past practice of a manual process conducted by a service representative or adjudicator when a claim is submitted in paper format has been replaced by online claims processing, which eliminates or significantly reduces errors. Moreover, these

claims are processed without requiring an agent's assistance, which has reduced labor costs. Veterans can check the status of their claims online, which reduces the amount of calls to the National Call Center.

Additionally, VA has used eBenefits as a driver for streamlining policies. VA eased the Post-9/11 GI Bill application process within the eBenefits portal, including transferability to spouses or children for service members with over six years of service. Service members can now apply on-line to transfer the benefits of their Post-9/11 GI Bill to eligible beneficiaries.

Launching self-service capabilities such as registration, eligibility, status checks, and outreach, has significantly reduced cycle time, which decreases claim development time, and ultimately reduces the actual time to process a claim from initiation to issuance. Over the last month, weekly visits to the eBenefits site averaged approximately 701,000 visits. Over the course of FY12, the eBenefits Portal gained over 900,000 users, raising the total number of unique users to over 1.9 million.

Blue Button

The "Blue Button" capability allows Veterans to download their personal health information from their My HealtheVet account. VA developed the Blue Button in collaboration with the Centers for Medicare and Medicaid Services (CMS), and the Department of Defense, along with the Markle Foundation's Consumer Engagement Workgroup. VA's Blue Button became operational at the end of August and the initiative was made nationally available in October 2010.

Significant enhancements to the Blue Button initiative were deployed in 2012. These enhancements include the addition of several new types of information from the VA Electronic Health Record for authenticated My HealtheVet users and makes the full medical record available to them (except diagnostic images, which are coming soon). This includes:

- VA Demographics
- VA Problem List (active problems)
- VA Admissions and Discharges (including Discharge Summaries)
- VA Notes (Progress Notes)
- VA Laboratory Results: (adds Microbiology)
- VA Vitals and Readings
- VA Pathology Reports: (Surgical Pathology, Cytology, Electron Microscopy)
- VA Radiology Reports
- VA Electrocardiogram (EKG) Reports (list of studies)

In addition this expansion includes two My HealtheVet self-entered data classes for all Veterans now available in the VA Blue Button:

- Food and Activity Journal
- The VA Continuity of Care Document (VA CCD) (in xml file format)

Environmental Protection Agency

Apps for the Environment

EPA sponsored the Apps for the Environment Challenge, a contest to encourage software developers to create applications that use EPA data to further environmental decision-making. The challenge resulted

in 38 apps that are available for the public to use. EPA also created the Data Finder web site to make it easier for the general public to find and access EPA's data by topic.

The Agency dedicates a large amount of resources to developing and maintaining software applications and websites that make EPA data easier to find, understand, and use. However, the data needs of the general public are not necessarily the same as for software developers. Software developers prefer that data be of a certain quality, and be provided in formats that will facilitate application development. In order to meet the specific needs of developers who may be interested in using EPA data, EPA created the Developer Central website.

Developer Central is a "how-to" website for using EPA application programming interfaces (APIs) and Web services for application development. The website focuses on providing well-documented data that EPA has made available via machine-readable formats, such as APIs and Web services that output to XML, JSON, and other file formats. Providing detailed documentation to APIs and Web services in a central location makes it easier for developers to locate and access EPA data in machine-readable formats. The website also provides code samples for accessing featured EPA data using Web services, making it easier for developers to understand how they can use EPA data in their applications. Developer Central also provides code for open source applications that use EPA data, so software developers can learn from existing applications and use them to inform their own projects. Publishing APIs and Web Services for software developers is often more efficient and cost-effective than developing new applications internally. Developer Central provides a platform for EPA to engage developers and more fully utilize private sector innovation.

National Aeronautics and Space Administration

Mobile Device Applications and Electronic Books

National Aeronautics and Space Administration's (NASA) online presence is well known for providing an unparalleled wealth of information to the public, providing direct access to agency programs and information, allowing the public to participate in the excitement and results of research and exploration. Internally, NASA personnel use web sites and services to support NASA's core business, scientific, research, and computational activities.

Today, Nasa.gov, is the main touch point for millions of people around the world regarding the agency's space exploration and aeronautics mission and attracts 600,000 unique visitors per day with an average of 43 million hits per day and average network traffic of 1.29 terabytes (TB) per day. The NASA portal alone generates more than 140,000,000 visits a year. NASA.gov also currently serves as a hub for NASA's social media presence, which includes over 250+ accounts across social media sites.

NASA's delivery of information to citizens has been enhanced through the implementation of mobile device applications and electronic books. These new communication channels take advantage of the growing use of mobile devices and tablets by the public. Current examples of mobile applications include: Rocket Science 101, International Space Station Live, and 3D Sun. A list of available applications is found at: http://www.nasa.gov/connect/apps.html. Electronic Books, or e-Books, are also used to provide information to the public and are offered in three different file formats to accommodate as many electronic reading devices as possible. A listing of e-Books is found at: http://www.nasa.gov/connect/ebooks/index.html.

National Archives and Records Administration

The Citizen Archivist Initiative

The National Archives and Records Administration (NARA) is engaging the public through the Citizen Archivist Initiative to improve the online delivery of Government records. NARA has elevated the importance of public participation by creating a role for "citizen archivists" and encouraging substantive contributions from the public such astags, transcriptions, and digital images that increase public access to the records of the Federal Government.

The Citizen Archivist Initiative is a new way for NARA to work with the researchers, genealogists, and the public, so that Government records can be more easily found online. NARA has developed several web based tools to enable public contributions, including tagging in their online catalog and an online transcription tool. NARA launched the Citizen Archivist Dashboard (http://www.archives.gov/citizen-archivist/) to centralize these activities, including external activities in online communities like Wikipedia and Flickr. In January 2012, NARA launched the National Archives Transcription Pilot Project (http://transcribe.archives.gov/), which enabled the public to transcribe more than 1,000 pages of records online in less than 3 weeks.

The Citizen Archivist Initiative at NARA leverages digital tools and external online communities to put Government records where the people are already are spending their time – in places like Wikipedia. Through the work of the agency's Wikipedian in Residence, NARA contributed 90,000 digital copies of historical records to the Wikimedia Commons. From this work, the Wikipedian community incorporated images of historical Government records into thousands of articles on Wikipedia. These efforts have led to an estimated 750,000,000 views of Wikipedia articles with images of records from the National Archives in FY12.

National Science Foundation

Innovation Challenge

In 2012, NSF announced its collaboration with a non-profit organization that promotes openness, innovation and participation on the Internet to host an open innovation challenge (http://www.nsf.gov/news/news_summ.jsp?cntn_id=125515). This innovation challenge is part of the U.S. Ignite initiative, which aims to spur the development of next-generation applications and digital experiences specifically designed for advanced-technology networks.

The challenge invites members of the public, including designers, developers, university researchers, entrepreneurs and other visionaries across America, to brainstorm and build applications for the faster, smarter internet of the future. Phase one of the challenge, the Brainstorming Round, aimed to foster ideas for the creation of apps that can take advantage of next-generation networks, in areas that benefit the public such as education, healthcare, transportation, manufacturing, public safety and clean energy. The next phase of the challenge will focus on the deployment and experimentation of applications.

In total, the challenge received over 300 solicitations for next-generation apps and services. The proposed apps are aimed specifically at areas that create public benefit; categories range from education, healthcare, public safety and clean energy to transportation, workforce development and advanced manufacturing. Eight teams were awarded prizes for their submissions to the Brainstorming Round. In the second phase of the challenge, developers can submit proposals to help build one of the winning ideas, or submit their own completely new concept for development. The results of the Mozilla

Challenge will drive innovation to benefit people in their everyday lives, build a better web, and keep the internet open.

NSF and its partner used online tools extensively to promote the challenge. This was NSF's first major research challenge posted on www.challenge.gov, an online challenge platform administered by the GSA that provides the public with a means to weigh in on some of the Federal Government's most pressing problems. In addition to advertising the challenge on Challenge.gov, NSF and its partner used press releases, blog posts, webcasts, and other mechanisms to ensure broad communication of the activity.

Nuclear Regulatory Commission

Web-Based Licensing System

The Nuclear Regulatory Commission's (NRC's) Web-Based Licensing System will provide an online platform for individuals and organizations to apply for a new license, renew a license, or amend an existing license for the use of radioactive materials. It will also provide an opportunity for Agreement States (States that have signed agreements with the NRC authorizing them to regulate certain uses of radioactive materials) to use the same licensing platform. Additionally, the system will provide a current, nationwide repository for official radioactive materials licenses. Users of the system will include current and potential materials licensees, Agreement States, and other Federal agencies that need NRC and Agreement State data for license verification.

The NRC is working towards streamlining the current paper-based materials licensing process and making the new system easy for applicants and Agreement States to use. Best practices adopted to improve the customer experience include establishing a help desk to address technical issues, providing automated tools for data transfer, and providing a stakeholder communications program that will use the NRC website, conference calls, webinars, coordinated efforts with Agreement States and NRC regional offices to solicit feedback, and participation in the annual meetings for the Organization of Agreement States and the Conference of Radiation Control Program Directors where NRC staff meet with the agency's regulatory partners in the Agreement States. The impact and benefits from this program include establishing a nationwide license verification program to reduce the risk of radioactive materials diversion for malevolent purposes, making it easier for materials licensees to submit and track the status of their license applications, providing an opportunity for Agreement States to avoid the costs of developing their own licensing systems, and streamlining the licensing process for the NRC staff.

Electronic Information Exchange System's Criminal History Application

One way that the NRC ensures adequate protection of nuclear facilities is through regulations that require all individuals who require unescorted access to these facilities to first undergo a criminal history background review. This review involves Federal Bureau of Investigation (FBI) evaluation of the prospective employee's or contractor's fingerprints to identify and report on the individual's criminal background. To facilitate this check, the NRC's Electronic Information Exchange system's Criminal History application enables licensees to electronically submit fingerprint files to the NRC and the NRC to report back the results of the FBI evaluation. The NRC receives more than 50,000 background check requests annually from its licensees. Timely turnaround of the background check requests is essential to these licensees because delays can cause costly work interruptions.

The NRC is streamlining the way that it accepts and processes fingerprints through its Criminal History application to reduce costs to the agency and improve the process for its licensees. Best practices that are

being used to improve the customer experience include providing a completely web-based user interface, eliminating the requirement to download a file to the user's computer, providing an interactive, real-time payment option to enable the submission and payment functions in a single transaction, and providing a customer interface that will allow licensees to review, in real time, the status of pending submissions as well as the history of their submissions. Benefits achieved through streamlining agency processes and accelerating delivery include reduced costs of responding to background check requests that arrive by postal mail by modifying the system to provide an electronic response to customers, thus saving overnight postage costs (approximately $6,000 per month), and increasing the number of licensees using the Criminal History system. Currently, licensees can submit background check information electronically or via postal mail. The more users who submit electronically, the more savings will be realized by the Government in both time and money. The electronic process is also more efficient for the licensees.

Office of Personnel Management

OPM's Plan Comparison Tools

OPM's Plan Comparison Tools (http://www.opm.gov/insure/health/search/plansearch.aspx; http://www.opm.gov/insure/dental/search/fedvipsearch.aspx are designed to make finding and comparing health, dental or vision plans easier for those eligible for Federal Employees Health Benefits (FEHB) or Federal Employees Dental and Vision Insurance Program (FEDVIP). These applications contain information about insurance plans available through FEHB and FEDVIP. Each tool is searchable, allowing the user to look up plans based on their zip code, the plan code or the plan's name.

When used, this instrument allows a side by side comparison of up to four plans at a time, based on features such as the plan's brochures, changes for each plan from the previous year, co-pay amounts, information on plan patient safety programs and plan premiums.

Small Business Administration

Surety Bond Guarantee (SBG)

The Surety Bond Guarantee (SBG) application is designed for reporting the Surety and Preferred Bond Guarantee program and financial information. The system uses a centralized database to furnish timely and accurate reporting of contingent liabilities, fee receivables, claim payables, and various income and expenses in connection with the program. An initial phase of this project will be enabling the "OUTSTANDING LISTS" reporting feature on mobile devices to allow customers to obtain Surety Bond Application statuses. The benefit of the SBG mobile app will allow customers (agents) to access the status of their bond applications and the ability to communicate via email with the SBA representative from a mobile device. Agents have overwhelmingly indicated that this feature would be most helpful since many of them actually do not have a home office.

Social Security Administration

MySocialSecurity

SSA's MySocialSecurity is a personalized online experience designed to allow registered users the ability to perform a variety of services including accessing and updating their SSA related information and records. SSA released this portal to the public on May 1, 2012 providing the public with the ability to access their Social Security statement. Over 2 million individuals have already successfully registered for MySocialSecurity and the online statement.

MySocialSecurity will:

- Transform SSA's eService delivery to a customer-centric model,
- Conveniently allow individuals to update, view, print, and save specific information, and
- Improved online transaction capability for the public.

In the future, this self-service interface will provide a tailored customer experience based upon the each individual's status with the agency, and allow for the exchange of sensitive and personal information in an efficient and secure manner. It will also support our efforts to develop creative outreach strategies and reduce field office visits and 800 number calls. MySocialSecurity will, along with other online services, continue to improve the quality of service to the public. MySocialSecurity provides the public with the ability to conduct business at their convenience and at their own pace, without the need to take leave from work, travel to a field office, and wait to meet with an agency representative.

eAuthorization

SSA's implemented electronic authorization, permits individuals applying for disability benefits to electronically sign and submit an authorization (SSA-827 form) to disclose medical information in 2012. This process helps reduce the disability application processing time, which can result in applicants receiving much needed medical insurance coverage and cash benefits sooner. Applicants also benefit from a streamlined process that allows online submission of all parts of their disability application. Additionally, adults filing a disability appeal online on their behalf now have the opportunity to read the SSA-827 and electronically sign the form as part of the disability appeal.

U.S. Agency for International Development

Office of Innovation and Development Alliances (IDEA)

USAID's IDEA was created to pioneer, test, and mainstream models, approaches, and mechanisms that can lead to improvements in development outcomes while establishing and coordinating partnerships that can lead to more process and results-based enhancements for the public and Government operations. To this end, IDEA implements the Development Innovation Ventures (DIV) initiative. DIV emphasizes producing development outcomes more effectively and more cost efficiently while managing risks and obtaining leverage by focusing on scale, rigorous testing, and evidence. DIV is a mechanism for working with partners to identify and test potential development solutions, and helping to scale those that are proven to produce development impact. DIV provides funding at three stages or levels. Applicants can apply at any stage, and those who have received funding at a prior stage do not automatically advance to the next stage.

- Stage 1 focuses on proof of concept and projects must demonstrate that their innovative solution cost-effectively addresses core development challenges and has the potential for mainstream adoption.
- Stage 2 focuses on testing and rigorous evidence collection, and projects must demonstrate clear evidence of cost-effective development impact for thousands of people.
- Stage 3 focuses on transitioning solutions to scale once they've been proven successful. Projects must demonstrate cost-effectiveness, and be widely scalable to tens of millions of beneficiaries. The most competitive Stage 3 projects replicate solutions across multiple countries and leverage substantial resources from additional partners.

The following is an example of a USAID DIV program that improves Government operations internationally:

USAID launched a $5 million Mobile Money Innovation Grant Fund managed by the Financial Access for Investing in the Development of Afghanistan (FAIDA) program. Through this initiative, USAID hopes to convert more of the 400,000 Afghan civil servants and security personnel salaries currently being paid in cash onto the mobile phone, facilitate bill payment for the 750,000 electricity customers, and encourage USAID implementing partners to use mobile payments.

Separately, IDEA has also offered competitive funding opportunities and capacity building to U.S. private voluntary organizations (PVOs) registered with USAID and local non-governmental organizations (LNGOs) to partner with USAID in the delivery of development and humanitarian services around the world. Within this framework, organizational and technical capacity building is integrated as a critical component of these field programs to strengthen the effectiveness of partner organizations as development actors.

B. Capital Planning and Investment Control Procedures for IT

Department of Agriculture

The Food Safety Modernization initiative supports an effective food safety system that collects, assesses and responds to hazards and risks. The Public Health Information System (PHIS) investment is the focus of the Food Safety Modernization initiative which consists of 15 key applications and supporting software that directly affects Food Safety and Inspection Service (FSIS) ability to achieve improvements in mission performance, management decision-making, and operational efficiencies.

The PHIS and the other FSIS applications/systems are primarily used to support mission critical FSIS business functions such as inspection, import/export activities, surveillance, auditing and enforcement. The PHIS provides a Service Oriented Architecture (SOA) approach and provides a single source for mission critical data. It establishes a common service for authentication/authorization, and uses predictive models to analyze real time data from FSIS and other Federal, state, and local agencies. The PHIS provides the user community a consolidated web-based user interface.

A certified Project Manager oversees this investment to ensure that sound project management practices are used to manage and communicate the status of this investment. As a result, the PHIS investment aligns with the USDA Enterprise Roadmap (Architecture) and specifically shows how it is managed efficiently through the use of shared services and cloud computing. For example, FSIS goals for PHIS include: (1) leveraging technology to automate procedures throughout agency programs; (2) sharing information with other government agencies, with USDA agencies, and with international trading partners; and (3) eliminating duplicative efforts for various system functions, data, and integration points.

The PHIS and the other FSIS applications/systems help close agency performance gaps by providing more effective and cost efficient services that better detect and prevent food safety threats. The IPT has worked to identify meaningful operational performance measures and closely monitors the results to ensure the investment is successful. For example, PHIS and its support systems will: provide an analytical tool and data to improve the agency's ability to detect intentional/unintentional food borne threats; enable near real-time data collection for reporting and analysis; provide the ability to collect information that assists FSIS with trace back and trace forward investigations on the origins of hazards; and provide the ability to collaborate with DHS, the Food and Drug Administration (FDA), international trading partners and with other USDA agencies in improving mission critical performance with inspections, surveillance, tracking, auditing, enforcement and more.

Department of Energy

In July 2011, Energy conducted a TechStat review of its Public Key Infrastructure (PKI) program, as part of the Department's capital planning and investment control process. The TechStat session brought together internal stakeholders, as well current and potential customers, to discuss ways to improve the program. Opportunities for increased efficiencies were identified including the recommendation to migrate the PKI program to the cloud by 2012.

To ensure a successful migration, session attendees agreed on next steps, including the development of a detailed cost analysis, project plan and acquisition strategy, and implementation of refined governance processes. The TechStat analysis identified the following benefits by migrating the PKI services to a cloud-based, shared service provider.

The cloud service will reduce the number of PKI systems currently in use by at least 50%, and will also provide high availability. This will result in overall service cost savings for Energy headquarters projected at approximately $1 million per year.

Migration of Energy PKI to a cloud-based shared service provider will enable Energy to become part of the Federal PKI trust framework via the Federal Bridge Certification Authority (FBCA). Federated PKI trust mechanisms, such as the FBCA, will enable recognition, mutual trust, and acceptance of identity credentials (e.g., PKI certificates on HSPD-12 credentials). This, in turn, will facilitate interoperability between disparate systems that recognize the federated PKI trust mechanism. The FBCA provides the backbone for secure communications between government agencies and between those agencies and their business partners. Such a federated PKI is also a key component of the Federal Identity Credential Access Management framework.

In June 2012, Energy issued its first PKI certificate via the Shared Service Provider and has started to realize the benefits mentioned above. Energy plans to migrate all existing PKI certificates to the shared service provider by the end of FY13 Q2.

Department of Health and Human Services

HHS developed and implemented Capital Planning and Investment Control (CPIC) and Enterprise Performance Life Cycle (EPLC) policies and processes to enable effective IT project, program, and portfolio management across its 11 Operating Divisions and the Office of the Secretary. In FY12, HHS and its operating divisions undertook more than 150 IT projects and conducted more than 250 gate reviews to ensure that the IT projects were meeting their planned budgets and schedule, and the projects were delivering the requirements established by the business owners.

One example of how the CPIC and EPLC policies and process help HHS effectively manage and govern IT is the HHS Program Support Center One Stop Service Solution (UII: 009-000281658) proposed to integrate and automate the channels through which customers interact with the Program Support Center to acquire services, driving customers to one source to enhance the accuracy of information collection and reduce the time taken to process applications or requests.

A stage gate review revealed that the project to develop the One Stop Service Solution had issues with project execution, governance, risk management, and cost management. The resolution of the issues identified in the gate review resulted in an improved governance structure, a clarification and reduction in the project scope, greatly improved project management, and yielded approximately $800,000 in cost savings. The One Stop Service Solution project was completed on time and on schedule as measured against the revised project baseline.

Department of Justice

The Justice Security Operations Center's (JSOC) mission is to prevent, detect and react to cyber-attacks and espionage against Justice and its components through the establishment of an enterprise JSOC, and is delivered through the JSOC's component teams of Detection, Response, Reporting and Communications, Engineering, and Cyber Threat Analysis. These key capabilities support Justice in the fulfillment of its mission objectives: law enforcement, litigation, prisons, and administration.

JSOC protects Justice and its component's information assets by centrally monitoring, tracking and facilitating response to daily cyber-attacks. JSOC established processes to effectively isolate, contain, and diffuse threats and has successfully defended Justice against Distributed Denial of Service Attacks, spread of malicious code, numerous web and email based attacks and continues to refine the processes as threats change. The centralized incident coordination has enabled JSOC to advise Components of current threats, allowing them to proactively address security vulnerabilities.

By employing a measured approach to JSOC enhancement, Justice has been able to minimize the annual capital investment resources required to establish and mature the JSOC, while reducing and/or eliminating the need for threat management services and capabilities within many of Justice's smaller components. The defense at the gateway has resulted in significant cost avoidance in responding to and recovering from cyber incidents. In addition, costly deployment errors were avoided by using a product that had a proven successful track record.

Justice has progressively enhanced the center's capabilities and coverage of enterprise assets from an initial core set of tools primarily focused on monitoring the network gateways and the status of software vulnerability patch management. During the recent PortfolioStat review performed in FY12, Justice's IT Security Staff and JSOC team, in partnership with Justice components, identified three additional security services that can be consolidated into Justice enterprise security services which are estimated to result in near-term enterprise-wide cost savings of approximately $5M, and annual cost avoidance of approximately $3.5 million per year. The security services are: security operations center consolidation, enterprise vulnerability scanning tool consolidation and enterprise anti-malware (A/V) consolidation. These savings will be reinvested in other security priorities across the enterprise.

A key factor in the success of the JSOC investment has been the partnership and collaboration between the Justice OCIO and component CIOs in the planning and prioritization of needed security capabilities which support the business case for new investment funding during the CPIC process. Further, the JSOC team's record of effective project management and delivery of new capability on schedule and on budget has placed Justice in the top tier of effective IT security organizations within the Federal Government.

The progressive enhancement of JSOC capabilities has enabled Justice to respond to and mitigate more than 32,000 cyber-attacks since JSOC's establishment in 2007.

Department of Labor

In September 2011, the Adjudicatory Boards, consisting of the Administrative Review Board (ARB), the Benefits Review Board (BRB), and the Employees' Compensation Appeals Board (ECAB), hereafter referred to collectively as the Boards, deployed the Appeals Management System (AMS). The system replaced the Boards' three, separate, outdated, legacy systems with a single, web-based, cloud-like hosted infrastructure.

The AMS is mapped to the missions of the Boards and Labor's strategic goals and has been a great success in significantly streamlining processes, consolidating data, and making data access more robust as compared to the former case management systems. The system meets the requirements of the Boards' business operations, Labor security, and the Federal Enterprise Architecture (EA) by ensuring collaboration and no redundancy of IT projects within the Department.

A pre-deployment AMS cost benefit analysis was completed and it was determined that approximately $530,000 in costs would be avoided by outsourcing the hosting of the AMS solution versus hosting the solution on the internal Labor infrastructure.

Department of State

State's Electronic Medical Record project is an IT investment that is an example of effective capital planning and investment control procedures to achieve increased effectiveness, efficiency, cost savings, and cost avoidance. State's Office of Medical Services' (MED) Electronic Medical Record investment is comprised of two projects, Electronic Health Records (EHR) and eMED. The EHR system will establish the essential medical record infrastructure that MED must have to provide quality health care services for employees and their dependents of U.S. Foreign Affairs and other Federal Government agencies worldwide under the Chief of Mission authority.

During FY 2012, MED conducted a Benefit Cost Analysis (BCA) on its eMED system. The key factors the BCA evaluated were net present value, benefits cost ratio, project objectives, qualitative benefits and risks. The BCA revealed that the existing eMED system had a negative net present value of -$13,744, a benefits cost ratio of 0.21, and high risk ratings. The need for replacing eMED was further supported by MED's requirement for global support and Executive Order 13410 mandating that all federal agencies must have an EHR that is interoperable with other agency systems.

During FY 2012, MED conducted an alternatives analysis, which assessed developing a new system, purchasing a commercial-off-the-shelf product, or partnering with the U.S Coast Guard (USCG), which had procured Epic Electronic Medical Records for its medical staff. MED's decision was to partner with the USCG. As of January 2013, MED estimates a total cost avoidance of $31.7M through FY15. In FY11, MED avoided $22.7M in sunk costs the US Coast Guard (USCG) incurred for Epic implementation costs ($5.8M) and licensing costs ($16.9M). In addition, MED estimated a 53% cost avoidance in Help Desk costs by partnering with USCG totaling $9M.

In May 2012, an estimated $35.9M total cost avoidance was reported. That amount included an estimated cost avoidance ($14M) for the shared Help Desk cost using a Government Cost Estimate (GCE) over a five year contract life cycle totaling $27M. Subsequently, the Help Desk contract was awarded in FY12 for $17M consisting of a base year and two option years, giving MED a $9M cost avoidance for the Help Desk contract. Specifically, MED is avoiding approximately $3.3M in the base year, $3.3M in option year one, and $2.4M in option year two.

MED's collaboration with the USCG allows it to leverage a common intergovernmental commercial-off-the-shelf, state of the art solution with access to DOD and VA beneficiaries' records, and without a lot of upfront costs. MED's decision also aligns with the Federal Government's Digital Government and Health Insurance Portability and Accountability Act. MED and Coast Guard are now looking to consolidate Help Desk functions.

National Aeronautics and Space Administration

The NASA Enterprise Application Competency Center (NEACC) provides operation and sustaining support for numerous Agency Business Applications supporting various stakeholder communities. The NEACC also implements new systems and transitions any Center-developed applications targeted to become integrated enterprise applications. This portfolio is managed via capital planning processes described below.

New requirements are coordinated by the NEACC Release & Deployment Management activities. Release content is approved and prioritized by the Agency Business Process Leads (ABPLs). New requirements are identified through Service Requests (SRs) and are coordinated with the affected Lines of Business (LoBs) prior to additional review. SRs shall be sent for review and prioritization by the respective Functional Control Board (FCB)/Change Control Board (CCB) after LOBs provide an impact assessment for new requirements. The FCB then prioritizes the SRs relevant to that FCB's functional area.

The NEACC Internal Governance Board (NIGB) convenes monthly to review application architecture management, infrastructure management, and system security initiatives necessary to provide a platform that ensures application stability and supports integration with other components. All decisions and recommendations are made in compliance with superior IT governance bodies including the Business Systems Management Board.

The NEACC Cross-Organizational Review (CORe) convenes monthly following the FCB/CCB and NIGB Meeting and prior to Sprint Planning Sessions to review cross-organizational business, technical and operational priorities (including strategic roadmap initiatives), identify where there are cross-LoB/Delivery Area capacity constraints/priority conflicts, and provide guidance/seek resolution of those conflicts and/or escalate, if necessary.

Major Development, Modernization, and Enhancement (DME) projects are individually managed and tracked and their implementation is executed via the Enterprise Applications Service Technologies contract. Each LOB operates under product/delivery managers who monitor SRs, points, priorities, and issues to ensure the product owners' needs are met and operations are smoothly executed.

New projects are executed in compliance with NASA's system development methodology. Formal phase reviews are conducted under the decision authority of the NASA OCIO and funding for these efforts is approved/overseen by the Business Systems Management Board (BSMB) or a superior board depending on the project's cost, risk and visibility levels. Project evaluation is also performed as described by the methodology.

National Archives and Records Administration

The project to replace NARA's current in-house email system, Novell GroupWise, with a cloud computing-based email system, is aimed at improving the availability of email services to employees, contractors and volunteers. This effort utilized the planning portion (Select Phase) of capital planning and investment control (CPIC) to efficiently highlight technical and business concerns while effectively outlining the appropriate requirements.

The business needs summary was discussed at Architecture Review Board (ARB) meetings. These discussions emphasized the need for the contract solicitation to clearly articulate the Service Level Agreements (SLAs), data conversion and reporting requirements. In addition, it prompted an assessment of current and planned bandwidth utilization and impact on NARA's network.

NARA business units then had an opportunity to review and comment on the draft business case, requirements and objectives. These comments and other feedback were discussed at various business and technical Integrated Project team (IPT) meetings. This review and feedback process ensured that functional, operational, records management, security and privacy requirements were clearly incorporated into the final business case and Statement of Objectives (SOO).

The cloud-based email service will modernize the NARA email system while reducing the Government's hardware and software expenses, data center footprint, power and cooling requirements and contract support personnel costs. The resulting system will provide increased uptime, improved backup and recovery, improved records management of email, calendaring, contacts, chat, and tasks within the email system, and improve redundancy capabilities. The cloud email solution will also improve the email support by using the cloud email provider's Tier 2 and Tier 3 support.

The contract was awarded in September 2012 and project implementation is underway. Monthly status reports (in the form of "quad" charts) tracking the scope, risks, schedule and cost will be completed by the project manager and reviewed at IT Projects meetings to monitor implementation.

The anticipated annual savings based on contract award is approximately $250,000[2] per year, or an estimated 19% savings over the current email and records management application expenses.

Small Business Administration

The Government Contracting and Business Development (GCBD) investment combines three legacy systems: HUBZone, Mentor-Protégé , and Business Development programs into a single portal. This provides a one stop shop for small disadvantaged businesses and for businesses that contribute to the economic development of a HUBZone. The SBA CPIC process required the completion of an alternative analysis, acquisition strategy, and development of a business case for the new Government Contracting and Business Development (GCBD) informational system to select the most cost effective solution. During the CPIC process it was also identified that this investment will reduce fraud, waste, and abuse, support additional business processes, and address the three new Mentor-Protg initiatives authorized through the Jobs Act.

To merge the three previous mentioned legacy systems into one, GCBD worked closely with the Office of the Chief Information Officer (OCIO) to plan the consolidation and complete the governance process. Together with the OCIO IT Project Management Office, GCBD prepared the necessary CPIC documents and presented them first to SBA's Chief Enterprise Architect. After initial review to ensure architectural alignment, the consolidation proposal was submitted to SBA's two IT Investment governing bodies: The Business Technology and Investment Advisory Council (BTI-AC) and the Business Technology Investment Council (BTIC). GCBD presented the alternatives analysis, acquisition strategy and initial business case for review in July 2011. By August of 2011, both governing bodies had reviewed and approved the concept to make changes to the IT Portfolio for both the Exhibit 300s for HUBZone and (Business Development Management Information System (BDMIS) for the BY13 portfolio submission to OMB in September 2011.

[2] The $250,000 per year is based on average annual maintenance cost of approximately $1.1 million for the new email system with records management capability compared to the estimated annual cost of the existing email ($850,000) and records management application ($500,000).

Social Security Administration

SSA's mature and disciplined Capital Planning and Investment Control processes and procedures ensure:

- Investment alignment with agency mission and strategies
- Integration with enterprise architecture
- Strict adherence to IT information security policy
- Coordination among related functions, processes and procedures
- Thorough and detailed planning during all process phases and for each initiative
- Sound management and control during all phases and for each initiative
- Low life cycle cost; high return on investment; carefully assessed risk
- Accurate enterprise and initiative reporting
- Complete retrospective analysis and adoption of lessons learned
- Timely delivery on IT development projects

An example of an SSA Major IT investment achieving increased effectiveness and a positive return on investment resulting from our effective capital planning and investment control procedures is the Disability Case Processing System (DCPS) program.

The DCPS initiative will modernize disability case processing by replacing the five COBOL-based Legacy systems currently used by the 54 Disability Determination Components (DD Components). DCPS will implement Service Oriented Architecture (SOA) principles and modern technology to streamline the disability determination process. Replacing the five Legacy systems with DCPS will allow us to implement software enhancements and modifications more efficiently and therefore, more cost-effectively. The five legacy systems would cost approximately $3.2 billion to maintain over a ten-year period. In contrast, the estimated cost for development, implementation, and operation of DCPS over the same ten-year period is approximately $524 million. DCPS will provide an estimated $586 million benefit and 11.85% ROI over a ten-year period.

Replacing the current DD component systems with DCPS will minimize the average processing time for initial disability claims, decrease case processing-related task time and provide increased system availability to improve the overall quality of the disability determination process.

Once operational in FY16, DCPS will deliver common functionality and consistent support to each DD Component, while providing accurate, current, consistent, and accessible data. No longer maintaining multiple systems, SSA will implement software enhancements and modifications required by laws, regulations, and business rules more efficiently and consistently, and at a reduced overall cost as compared to the current legacy system environment.

DCPS will benefit SSA's disability process functionally and technologically by providing full process integration, ease of sharing disability processing workload across DD Component sites, a common interface with other SSA offices and systems, and a dramatic reduction in the technological complexity of system support. DCPS will provide a single system that integrates the entire claims process from start to finish, including case processing, correspondence, fiscal, management information, and workload management. DCPS will use intelligent case processing to support disability examiners in making consistent decisions based on SSA Disability Policy, and leverage SSA's investment in Intelligent Disability.

Section VII: Compliance with Goals and Provisions of the Act

A. Performance Integration

The following section contains agency examples of how performance metrics are used and tracked for IT investments and how these metrics support agency objectives, strategic goals, and statutory mandates as indicated in the E-Gov Act. Examples also discuss performance metrics that focus on customer service, agency productivity, innovative and best practices technology adoption.

Department of Agriculture

The USDA Office of the Chief Information Officer (OCIO) capital planning staff and executive management work closely with IT investment owners to emphasize business results and citizen benefits in all departmental IT life-cycle decision making activities – from structured investment selection events, to executive capital plan reviews, to acquisition plan approvals, ending with ongoing operational asset analyses. USDA OCIO ensures that key IT investment stakeholder and partner interests are included at every step of the IT life-cycle by monitoring IT projects for the regular use of comprehensive and inclusive project charters that encourage stakeholder/customer involvement, and by emphasizing the use and management of key stakeholder and customer performance goals and measures in the ongoing execution of IT projects.

For example, of USDA's total discretionary IT funding ($2.03B) in each of FY11 and FY12 (Est.) more than half ($1.10B) is dedicated to Services to Citizens. Also, more than two-thirds ($1.36B) of the FY11 and FY12 (Est.) IT portfolios are managed as Major Investments. These Major Investments include nearly 1,400 individual Performance Measurement Areas; nearly half of which (46%) are focused on Mission and Business Results (357 measures) and Customer Results (284 measures). Three specific examples include: (1) Average Number of Days required to complete Direct Loan Processing (from application completed to final disposition); (2) Number of States with Average Direct Loan Processing Time greater than 35 days; and (3) Tier 3 Resolutions occur within 5 business days, or in some cases, within Agency agreed upon timeline.

Department of Commerce

Commerce utilizes several activities and processes to effectively monitor and track performance of IT investments. A primary initiative is the Department's Balanced Scorecard (BSC) system, which tracks and measures program/bureau performance in support of Departmental priority goals on a quarterly basis. Another evaluation method used is the Commerce Information Technology Review Board (CITRB) that holistically evaluates IT Project performance and progress.

For tracking IT Investment performance, Commerce utilizes two BSC metrics that measure the activities of the CITRB, which oversees Commerce's major IT Investments/projects and portfolios and approves funding requests and/or increases:

- TechStat reviews performed on "red" rated IT projects/programs (Sustained red for 2 or more months within a 12-month period.) TARGET: Review 100% of sustained "red" rated IT Projects within a 12 month period.
- Percent of major IT projects undergoing CITRB or TechStat reviews per fiscal year. TARGET: Review 50% of major IT projects per fiscal year (approximately 21 reviews).

The CITRB is a comprehensive tool used to review IT Project performance, effectiveness and status. All major IT projects brief the CITRB either annually or bi-annually depending on criticality, the OMB IT Dashboard rating, risk, and CIO concern. The CITRB evaluates status and overall performance in several key areas: (1) Program/Project Management, (2) Risk Management, (3) IT Approach/Cyber Security, (4) Subject Matter Elements (e.g., Acquisition Management), and (5) Overall Health and Wellness.

Department of Defense

DoDI 8115.02, "*Information Technology Portfolio Management*," provides the procedural foundation for the Analysis, Selection, Control, and Evaluation of IT investment portfolios that focus on improving DOD capabilities and mission outcomes. Evaluation includes the development and application of outcome-based performance measures that are used to guide portfolio development and evaluate performance. Governance forums are established to manage these portfolios. For example, the Defense Business Council, chaired by the DOD Deputy Chief Management Officer, serves as the principal governance body to the Deputy's Management Action Group (DMAG) as a mechanism for defense business operations and as the Department's Investment Review Board (IRB) for defense business systems. This forum oversees application of system outcome oriented performance measures and reviews performance results to track progress against strategic goals such as interoperability and reduction in duplication. Various metrics are used in the structured review process of systems by the IRB and other review governance forums in support of the review and certification of systems.

Department of Education

The performance metrics for agency IT investments are developed in the Enterprise Architecture Segment Modernization Planning Process. The Department categorizes its IT investments into 13 lines of business (LoB). LoB performance goals and objectives are aligned to those of the agency and are focused on innovation, customer service, continuous process improvement and organizational performance management. The Planning and Investment Review Working Group periodically evaluates performance metrics.

ED uses value and performance metrics to evaluate its IT investments with its value measurement methodology (VMM); the results are used to make funding and management decisions. The VMM process contains five steps: establish mission priorities; define value drivers; prioritize and select; execute and deliver; and assess value and benefit. In conducting the VMM process, the Office of the Chief Information Officer (OCIO) and LoB Senior Executives develop and prioritize mission priorities to which all IT investments align. Education senior executives develop value drivers in specific performance areas: Strategic Plan alignment; cost reduction/avoidance; productivity and efficiency; and effectiveness and capacity. IT investments are then given a value score based on their alignment to the established mission priorities and value drivers.

IT Operational Performance Metrics are available at http://www.itdashboard.gov/portfolios/agency=018.

Department of Energy

The Annual Performance Report (APR) provides detailed performance information related to Energy's suite of performance metrics and a description of the annual result for each measure.

- http://www.energy.gov/about/budget.htm
- http://www.goals.performance.gov/agency/doe

The Energy performance goals are linked to key stakeholders, private sector, other agencies, and internal operations in the Energy Strategic Plan and Annual Performance Report. These documents are available for review by the public and posted to:

- http://www.cfo.doe.gov/strategicplan/strategicplan.htm
- http://www.energy.gov/about/budget.htm

Department of Health and Human Services

HHS requires annual Operational Analyses of its IT investments. One part of the Enterprise Performance Life Cycle (EPLC) Framework is the Annual Operational Analysis Practices Guide. An excerpt from the guide describes how to measure performance in four specific areas:

Customer Satisfaction. Measures performance in terms of the extent to which the investment supports customer processes as designed. The focus is on how well the investment delivers the services it was funded to deliver (i.e., effectiveness), and considers stakeholder perception on whether the costs associated with providing the service is as low, to the customer, as it could be. Customer satisfaction data is typically collected via surveys and measured via both quantitative and qualitative metrics.

Strategic and Business Results. Measures the investment's impact on the performance of the Operating Division and HHS. These results provide a measure of how well the investment is meeting business needs, whether it is contributing to the achievement of Operating Division or HHS strategic goals, and whether it continues to be aligned with the Operating Division and HHS strategic direction.

Financial Performance. Measures and compares current cost-related performance with the pre-established cost baseline. While financial performance is typically reported as quantitative measures, the investment should also be subjected to regular reviews for cost effectiveness and efficiency.

Innovation. Addressing innovation should demonstrate the extent to which the project team is tracking emerging technologies and performing ongoing analyses of alternatives for achieving the same or better customer results and strategic goals at better cost, performance, and risk levels than the current solution.

Department of Homeland Security

DHS uses performance metrics to track IT investment performance through the following: (1) OMB 300 submissions, (2) Operational Analyses, and (3) IT Program Health Assessments. The results of these reviews are used to support Federal mandates for increased accountability and performance in IT investments (IT projects or programs in development and/or operational systems in maintenance). Well performing, relevant IT investments may continue to get funding by DHS while poor performing IT investments may be paused for review and course correction or stopped and perhaps eliminated. DHS participates in required monthly reporting to the Federal IT Dashboard, www.itdashboard.gov.

The following are further descriptions of the how performance metrics are used in each of the reviews:

The OMB 300 has a section on performance measures for IT investments (Exhibit 300B) and requires agencies, including DHS, to update their performance information monthly. The 300 requires agencies to map to the Federal Enterprise Architecture (FEA) Performance Reference Model (PRM) measurement categories which are (1) Mission and Business Results (2) Customer Results (3) Process and Activities and (4) Technology. DHS complies with these reporting requirements. The OMB 300 also requires agencies to indicate how their IT investments support the agency's strategic goals, legislative mandates (if applicable), and/or response to audit findings (if applicable).

Operational Analyses (OAs) are required on an annual basis on operational IT systems. DHS mandates, via official CIO memorandum, that OAs be performed and provides an Instruction Manual for conducting the OAs. The Operational Analysis requires investments with Operational IT systems provide performance measures/results to justify continued investment in the asset. Specifically, the Program Manager must provide performance measurement results in areas of customer satisfaction and overall operational performance and innovation.

DHS also conducts IT assessments called Program Health Assessments using criteria to determine the health of IT programs. The results (scores) are reported to the Federal IT Dashboard. The scoring criteria contain performance targets that are assigned a point value (0-10) based on the level of achievement in a particular area. Scoring also covers the degree to which Performance Areas were covered in any Operational Analysis associated with the program.

Department of Housing and Urban Development

The Performance and Risk Management Division (PRMD) was established by the reorganization of the OCIO at HUD. The PRMD monitors the performance of IT service delivery to provide meaningful data that drives decision making and performance improvement. The PRMD aims to: (1) improve visibility and accountability; (2) review, assess and influence performance outcomes; (3) maximize the benefits of IT Service delivery; and (4) improve customer satisfaction. The PRMD will use a balanced score card approach to measure the overall health of the IT Service delivery. There are four specific areas of measurement: investment health, workforce development, internal processes, and customer satisfaction. (Within each of the quadrants key performance indicators can be drawn from a variety of industry standards including the Information Technology Infrastructure Library (ITIL), COBIT, etc.) The IT Service Delivery Framework shall provide the IT community with accurate, actionable, data that enables data-driven decisions, optimizes business value, aligns investment with the strategic goals of HUD, improves customer satisfaction, and facilitates performance-based management of IT resources. This initiative is directly related to Goal 5 of the HUD Strategic Plan FY 2010 – 2015.

Department of the Interior

One of the key fundamental processes implemented by Interior's OCIO officials to manage IT organizational change and the staff's embracement of new initiatives was the identification of new performance metrics. The FY12 performance goals directly align with the Secretary's ITT Strategic Plan, as well as our Administration's priorities. Interior recognized the importance of establishing targets and monitoring actual performance to effectively achieve ITT goals. FY12 requirements were heightened in our Information Resource Management (IRM) Organizational Assessment (OA) that was used to identify Bureau/Office IRM quarterly (Q) ratings. The Q4 2012 ratings were incorporated into the Departmental OA for use in the Senior Executive Service (SES), Senior-Level (SL), and Scientific/Professional (ST) performance review process.

The following OA components have been established to support Interior's ITT Strategic Plan which is accessible via: http://www.doi.gov/ocio/index.cfm.

Requirements:

- Open Government: Published one high-value dataset each quarter.
- Federal Data Center Consolidation: Achieved 100% or > of FY12 targeted number of consolidations.

- Accountability: IT major Investments: 95% or > Performance: within 10% of the planned schedule and cost baseline.
- Secretarial Order 3309: Completion/Alignment of IT Annual Spend Plans; Performance Elements into Assistant Director for Information Resources/IT Program Managers Performance Plans; and Revisions to Departmental Manual Chapter's organizational descriptions.
- Mobile Device Management (MDM): Adopted Interior Enterprise MDM system as standard and migrated 25% of its existing mobile device inventories.
- E-Mail: Migrations from on-premise email and collaboration services to the Cloud-based email and Collaboration Services solution by December 30, 2012.
- E-Forms: Enhanced focus on the completion of selected forms.
- Radio Site Assessment and Remediation Plan of Action: to address OIG Finding on Health and Safety (OCIO Directive 2010-008).

Department of Justice

At Justice, performance planning and reporting is companion to the budget process. Performance information is vital to making resource allocation decisions and should be an integral part of the budget. Justice provides detailed component-specific annual performance plans within individual budget submissions, which also serve Justice's annual performance plan. The Justice Performance Accountability Report (PAR) provides a summary discussion of the progress that Justice has made against its three strategic goals. It reports on the 20 key performance measures for these goals by detailing program objectives and FY11 targets and actual performance, as well as whether targets were or were not achieved. Each key performance measure also includes information related to data collection and storage, data validation and verification, and data limitations. These metrics represent just a portion of the workload and performance metrics that Components report to the budget office on a quarterly basis.

In addition to the PAR, Justice collects performance metrics on each of its major IT Investments as part of the Exhibit 300 process. Each major IT Investment must identify a set of performance metrics which measure the effectiveness of the investment in delivering the desired service or support level. Metrics cover a wide area of performance including customer results, technology, and mission and business results. A certain sub-set of these metrics are tracked and reported on throughout the year through the Federal IT Dashboard. Additionally, these metrics are tied back to the Justice Strategic Goals and Objectives.

Department of Labor

The Labor Performance Model represents the overall landscape for performance measurement at Labor. The model is hierarchical and begins with Labor's Strategic Plan including the Secretary's vision, strategic goals, outcome goals, and performance goals and measures for Labor. The Labor Strategic Plan is supported by Labor's Annual Performance Plan, which describes the performance goals associated with each Labor Agency including their programs and strategies. Labor Agencies produce annual Operating Plans that align to and support the Labor Strategic goals and describe their fiscal year priorities and the key program activities and strategies to be accomplished including the associated performance measures (i.e., outputs) and/or milestones. Agency performance measures and/or milestones include mission operations, productivity, service, and/or customer service oriented measures/milestones. Agency IT investment performance goals, measures, and/or milestones are aligned accordingly to that agency's annual operating plans and/or performance plans. This hierarchical performance model enables Labor to ensure that initiatives are planned and managed within the bounds

of Labor's Strategic Goals and Performance Outcomes. Labor tracks progress toward achieving its annual and strategic goals by using quantifiable performance measures.

Specific Labor IT investment operational performance metrics/goals can be viewed on the OMB IT Dashboard at the following link: http://www.itdashboard.gov/portfolios/agency=012

Department of State

As part of State's Capital Planning and Investment Control guidance, a Performance Measurement Guide and Performance Workbook are available to assist project managers in developing their investment's performance measures. The Workbook is designed to capture all key elements of the performance management lifecycle. When completing the Workbook, managers collaborate with business owners to ensure that strategic drivers are identified and define success for the investment. Key metrics include: Mission & Business, Customer, Process & Activities, and Technology. The Department is continuously working to improve the quality of the performance measures and is implementing an enterprise portfolio management tool that seeks to collect and analyze performance data to help target investment decision making. This capability will help State to evaluate enterprise portfolio data against strategic IT priorities to determine whether investments are achieving results or whether funds need to be redirected to more effective investments.

State provides information regarding information technology performance measures at http://technology.performance.gov/agency/state/technology and describes how State links performance goals with other agencies at http://goals.performance.gov/agency/dosusaid. From the first link, one can navigate to State's performance measures for IT investments on the IT Dashboard (http://it.usaspending.gov) and from the second to information on State's performance and its contributions to the Federal Government-wide initiatives. In addition, performance information is provided as part of State's annual Congressional Budget Justification (CBJ). More information on Planning, Performance, and Budget can be obtained on the state.gov website located at: http://www.state.gov/s/d/rm/c6113.htm.

Department of Transportation

DOT's Integrated Program Planning and Management (IPPM) framework suggests a risk-adjusted Net Present Value (NPV) approach for evaluating the value of agency IT investments. DOT recognizes that NPV is but one method for evaluating an investment's worth against its costs, and has reallocated contractor resources to develop a more robust IT investment valuation model. The model will build on the DOT EA Roadmap, which identifies a number of IT-related strategic themes. These include:

- Data accessibility and information sharing
- Data completeness and granularity
- Root cause analysis and risk-based resource targeting
- Transparency, participation, and collaboration
- Delivering operational efficiencies to increase transportation infrastructure capacity
- Improved forecasting and prioritization capabilities

Department of the Treasury

Treasury implemented a new oversight process within its existing governance in July 2011 to monitor investment execution through monthly variance reporting, and trigger TechStats on investments that are performing poorly. This oversight role transitions to the new Treasury Technology Investment Review

Board once that body is fully operational. The Board selected metrics and benchmarks will integrate with Treasury's CPIC process and Bureau CIO performance plans.

Monthly Reporting of project cost and schedule variances was deployed on the Treasury IT Dashboard in July 2011. Major investments report monthly on projected cost and schedule changes for OMB's IT Dashboard. Using this data, Treasury develops a variance report that aggregates to the comparable level of management review from the Bureau CIO/CTO, through the Treasury CIO to the ASM and Bureau Heads. Treasury has begun capturing similar data for non-major investments by Bureau.

Bureau level TechStats occur when an investment's monthly variance index becomes yellow as defined by a cumulative score of cost, schedule, operational metrics variances, and CIO rating. Additionally the CIO may direct a Bureau to conduct a TechStat. Department level TechStats are conducted when an investment becomes red. The Treasury CIO also conducts TechStats to investigate wasteful, duplicative, or low value IT investments.

Treasury is targeting to have IT Spending per Employee within 10% of Gartner's benchmark for the Financial Services Industry for FY13. Treasury has established portfolio management targets of a maximum of 30% of portfolio reports in Yellow status and less than 2% in Red status.

Department of Veterans Affairs

As Federal agencies are being asked to explore "doing more with less" during tight fiscal environments, VA examined how to effectively change existing business arrangements in IT, particularly software Enterprise License Agreements (ELAs), which can be a significant portion of an agency's budget. Due to the nature of each agency's maturity in varying software ELAs, CIOs often must use "right size" ELAs based on each agency's portfolio maturity, requirements, and other needs. In April 2012, an OMB-led TechStat examined VA's methodology and approach concerning ELAs. Specifically, it identified how VA established a dedicated IT software acquisition team, a technology roadmap, and a streamlined analysis approach for strategic software sourcing options to drive efficiencies. Given the benefits realized using this model, this approach and the lessons learned will be shared across the Federal Government to help other agencies effectively update their approaches to IT business arrangements. Through this approach, VA has projected $40 million in cost-savings for FY13 and subsequent years, which will be used to pursue investments that are more mission critical as well as pilot projects that will inform VA's comprehensive enterprise software asset management strategy.

OI&T also tracks a wide range of IT performance metrics on its IT Performance Dashboard. This dashboard is an intranet site that gives VA employees a look under the hood at reports on availability, throughput, response time, customer service, financial data, and service level agreements. It provides real time access to a broad range of performance metrics across VA or within individual Regions, Veterans Integrated Service Networks (VISNs), or local facilities.

The OI&T Annual Report lays out the strategic priorities for the Office of Information and Technology to support the development of services and capabilities for the Major Initiatives, as well as IT support to the VA corporate offices and employees in executing their missions.

The applicable URL for performance goals related to IT can be found at:
http://www.oit.va.gov/docs/OIT_CIO_Annual_Report_FY_2011_Final.pdf

The FY12 Annual Report is currently under review.

Environmental Protection Agency

EPA's performance metrics for IT investments were established for investments focused on achieving EPA's mission to protect human health and the environment. They were formulated following the framework of indicating:

- Customer Results;
- Mission and Business Results;
- Processes and Activities; and
- Technology (efficiency/improvement)

The periodic results are monitored by investment managers and reviewed by mission office leadership monthly prior to final review by senior IT leadership and submission to the public- facing Federal IT Dashboard.

Much of EPA's work involves sharing of environmental information with Federal, state and local stakeholders, which is reflected in performance metrics such as eRulemaking's measure of 'Federal regulatory entities using the Federal Docket Management System' and the Central Data Exchange's measure of the number of support services received by its customers.

General Services Administration

Performance measurement plays a critical role in ensuring GSA meets its IT Strategic Business Plan goals and objectives. By monitoring various levels of performance measures, the agency is able to identify whether the strategic plan is relevant and responsive to changing conditions. Agency-wide IT strategic goals are issued as part of the IT Strategic Business Plan.

Through the Select process of CPIC, proposed IT investments indicate whether the investment in whole or in part addresses a statutory mandate, GSA IT Strategic Plan goals, and GSA's Annual Plan to assess whether:

- Investments continue to be aligned with strategic direction
- Projects are prioritized, implemented, and managed efficiently
- Projects support achievement of the desired initiative outcomes
- Initiatives move the agency toward the achievement of the IT strategic goals

GSA Major IT Investments are required to demonstrate how the IT investment will move toward agency's strategic goals' achievement, using specific performance metrics appropriate to the business mission and link to program, and process management.

Through the Control process of CPIC, performance measures of projects are monitored monthly to ensure investments are updating their measures timely and identifying whether investments are meeting the stated targets. Review of the operational measures enables the agency to perform root cause analysis and identify opportunities for improvement.

GSA is consolidating its IT resources and developing a new IT services-focused strategy and is re-baselining its IT Portfolio, both of which will be articulated in the new IT Strategic Plan (FY13 – FY15).

National Aeronautics and Space Administration

As NASA's consolidation efforts matured over the past ten years, the need to incorporate an on-going analysis of mission needs to ensure systems, equipment, and services meet operational performance requirements has been addressed. One method has been through specific contract language. Within the Agency Consolidated End-User Services (ACES) contract, NASA requires its contractors to "propose an innovation approach to providing collaborative e-mail and calendaring services across NASA". These services are performed with an incentive clause emphasizing that the contractor is going to be evaluated on a Cost Control Factor.

OMB's IT Dashboard assists NASA in the monthly monitoring of strategic investments. Investment metrics are captured and reviewed at both the Center and Agency level and periodically reviewed with the NASA CIO. Performance metrics are included in this effort and are also published to the IT Dashboard. The majority of these metrics focus on customer service (i.e., response time to the customer) and productivity (i.e., uptime of a system). NASA IT infrastructure metrics can be found at: http://www.itdashboard.gov/investment?buscid=46. Other metrics are shown under the individual NASA IT investments listed in the "Investment" tab on the following page: http://www.itdashboard.gov/portfolios/agency=026.

National Archives and Records Administration

NARA uses performance metrics to track progress towards achieving strategic goals and objectives. The same process is followed with an IT investment as with any mission or non-IT program. Currently, NARA monitors 30 IT investments, which are aligned with the enterprise technical and business architecture as well as specific business functions. Six of these are also tracked as major IT investments (Ex-300s), with multiple performance measures that are reviewed regularly and have aggressive annual targets. NARA performance based reporting is focused on public facing applications.

A variety of performance metrics are tracked and reported such as availability, number of users, and cost per visit for public facing applications. In addition, customer satisfaction with NARA's helpdesk services and the percent of help desk responses that are completed within four hours are also tracked.

All six of the major IT investments relate directly to NARA's ability to carry out major operational processes, which enable mission accomplishment. These investments support the processes and infrastructure required for NARA to preserve and protect its holdings, and provide access in an efficiently and timely manner. For investments that are in an operations and maintenance phase, performance metrics are designed to illustrate the outcomes and results of these investments.

National Science Foundation

NSF strives to continuously monitor IT performance and implement lessons learned whenever possible. To this end, NSF utilizes performance metrics to assess the effectiveness of its IT investments. One resource NSF uses to track and report on the performance of its IT investments is the Federal IT Dashboard. Individual operational performance metrics are established for each IT investment. Each month, NSF tracks and reports on project costs, schedules, and operational performance for each of its major IT investments. Any variances are identified, reported, and, if necessary, acted upon.

Additionally, NSF staff meets regularly to review performance metrics for major IT systems. For example, each weekday morning, NSF's IT division hosts a 15-30 minute "tag-up" session attended by top IT management for the purpose of reviewing key daily activities and performance measures for

NSF's IT systems. This daily meeting helps ensure that NSF's IT program is responsive to the changing needs of NSF's customers and that NSF's IT systems perform as intended.

As previously described, NSF is formalizing an IT Strategic Plan to ensure alignment of IT priorities with agency business priorities. The IT Strategic Plan, which will include standardized performance metrics as appropriate, will help ensure that IT planning decisions are made with agency strategic goals in mind.

Nuclear Regulatory Commission

The NRC requires each investment to include performance metrics which are tracked and monitored as part of the "control" and "evaluate" phases of the CPIC process. Additionally, a roll-up measure for each major system is included in the System Owners' performance plan and combined with other performance plan measures as an element in their SES performance plan. The majority of the existing measures focus on customer service, productivity, customer satisfaction, and operational effectiveness. The NRC has just obtained approval for the Value Model from the agency senior governance board. The Value Model will be used to prioritize new FY15 investments, and bi-annually to adjust the portfolio in the year of execution. The NRC Value Model uses a matrix of four Investment Principles on the vertical axis and six measures on the horizontal axis that are weighted. The principles the value model focus on are as follows:

- Strategic
- Operational Effectiveness
- Infrastructure and Compliance; and
- Innovation

The measures have multiple metrics that are aligned with the metrics from the Exhibit 300s and rolled-up into a composite measure that is tracked in the performance management plan. Those measures and their definition follow:

- Benefits (multiple metrics including cost benefit)
- Risks (business, functional, and security)
- Cost (life cycle, current year , and budget year impacts)
- Management & Resources (multiple metrics)
- Quality (multiple metrics including those in the Exhibit 300)
- Efficiency (multiple metrics including those in the Exhibit 300)

Each metric has pre-determined thresholds which identify it as "green or red". If any individual metric is "red" than the measure as a whole is reported as "red".

Office of Personnel Management

OPM analyzes and establishes performance metrics for its IT investments. OPM tracks the performance metrics to ensure excellent customer service, to maximize business value of IT, and to find ways to manage the programs more efficiently. Performance metrics are reported monthly, quarterly and semi-annually on the Federal IT Dashboard demonstrating the "business value" of the investments to the taxpayer beyond just successful project cost or schedule management. These metrics are analyzed and briefed to the CIO weekly, to the IRB, and in Chief of Staff meetings as to progress of whether the metrics are met or not and any corrective actions to follow if necessary. Multiple statutory mandates and OPM strategic goals drive the metrics. For instance, the OPM strategic goals "Ensure the Federal workforce and its leaders are fully accountable, fairly appraised, and have the tools, systems, and

resources to perform at the highest levels to achieve superior results" and "Help agencies recruit and hire the most talented and diverse Federal workforce possible to serve the American people" are evident in the following performance metric examples:

- Consolidated Business Information System: resolution of help desk tickets/incidents, percentage of time taken to resolve incidents by criticality. Number of incidents solved within the acceptable timeframe/total number of incidents*100 (monthly).
- EHRI eOPF: web-based customer satisfaction survey to HR Specialists and employees using eOPF. Percentage of respondents that are satisfied or extremely satisfied (quarterly).
- USA Staffing: customer satisfaction and organizational effectiveness, i.e., percentage of customers confirming USA Staffing services contribute to improved organizational effectiveness (semi-annually).

Office of the Director of National Intelligence

The third strategic goal in the August 2009 National Intelligence Strategy (NIS), "Deliver Balanced and Improving Capabilities", necessitates IT Service Management (ITSM) service providers continuously reassess and adjust to prepare for tomorrow's challenges while ensuring the user community can meet today's missions. Enterprise Objective 4 (E04), Improve Information Integration and Sharing, supports the NIS third strategic goal.

The main ODNI ITSM Service Provider, the Infrastructure Services Group (ISG), a forward deployed Central Intelligence Agency (CIA) service provider, adopts several best practices in the delivery of IT service. A comprehensive view of IT health is provided through the monthly DNI Dashboard and ISG Scoreboard, and the Weekly DNI IT Status Report. These reports provide a series of Key Performance Indicators (KPIs) that track volume and trends of IT service delivery. Service Level Targets (SLTs) are tracked as an indication of how well ISG and other service providers meet mission requirements. Network availability, time to grant accesses, capability, volume of email, customer satisfaction, help desk activity, requirements and projects created and closed, incidents and service requests created and closed, and video teleconference service are examples of metrics regularly viewed. Additional weekly reports are shared with service providers such as missed SLTs and new requirements. Ad hoc reports, such as root-cause analysis of SLTs missed and process variation, are produced.

Small Business Administration

SBA assesses performance at both the program and agency-wide levels. SBA uses the Annual Performance Report to report the agency's performance with respect to each of its particular missions.

SBA's Summary of Performance and Financial Information FY11 can be found at: http://www.sba.gov/sites/default/files/files/FY%202011%20Summary%20of%20Performance%20and%20Financial%20Information.pdf

SBA has linked performance goals to key stakeholders, private sector, other agencies, and internal operations through strategic goals being set with positive outcomes and achievements. The SBA Strategic Plan 2011-2016, Strategic Objective 1.4, "Ensure that SBA's disaster assistance resources for businesses, non-profit organizations, homeowners, and renters can be deployed quickly, effectively and efficiently in order to preserve jobs and help return small businesses to operation." SBA's Summary of Performance and Financial Information FY11 shows that the Strategic Objective 1.4 for Disaster Assistance was met. There are significant percentage increases shown within the Actuals for each of the Fiscal Years.

The FY12 Summary of Performance and Financial report is available on www.sba.gov/performance.

Social Security Administration

The SSA Deputy Commissioner for Systems (DCS)/CIO ensures IT investments align with strategic business needs by following the performance management framework set forth in the SSA Agency Strategic Plan (ASP). This framework provides appropriate oversight, monitoring, and assessment of our efforts toward achieving short and long-term outcomes supporting our strategic goals. An important ASP component is leveraging technology to enable the agency to meet goals and achieve desired business outcomes. The ASP drives lower level planning, including objectives, priorities and constraints used in constructing detailed support plans. It reflects the goals and supporting objectives, strategies and performance targets over a multi-year period, normally four to five years. Each of these goals is dependent upon IT.

The agency's Annual Performance Plan (APP) shows how the goals and objectives in the ASP will be achieved, focusing on performance targets and the means and strategies for achieving them. Performance targets or output/outcome measures help assess our success in meeting a performance goal or initiative. Many of the expected business improvements or outcomes rely upon the enterprise availability of our IT services. Shortly after the close of the fiscal year, the Performance and Accountability Report (PAR) is published. The PAR outlines actual performance achievements during the past year and compares them with the performance goals and objectives set forth in the APP. It also includes explanations of any corrective action the agency takes for unachieved goals.

Goals, objectives, measures, and targets are explained in detail at http://www.socialsecurity.gov/budget/2012APP.pdf.

U.S. Agency for International Development

USAID's Office of the Chief Information Officer Project Management Office (USAID/CIO/PMO) assists project teams with developing and tracking performance metrics that support Agency strategic goals, statutory mandates, and other governmental goals and requirements.

Unique performance measures are developed for each project in the IT portfolio. These measures focus on:

- Mission and business results that projects deliver in support of agency strategic goals;
- Customer service;
- Improvements to business processes and activities;
- Deployed technology performance; and
- Project execution.

These performance measures incorporate the following “Performance Indicators” as some of the metrics of effective project performance: Customer Benefit, Service Coverage, Timeliness and Responsiveness, Management and Innovation, Productivity, Technology Costs, and Effectiveness.

All performance measures developed for the projects are mapped to USAID’s strategic goals and objectives, thus tying project goals and performance with Agency strategic goals and statutory requirements. The performance measures are tracked through the project’s development, modernization and enhancement phase into the operations and maintenance phase. The Office of the Chief Information Officer is currently forming a new office (the Portfolio and Contract Management Branch) to more

directly support performance measure tracking and ensure existing systems are in line with the latest best practices technology and remain cost effective.

B. Accessibility

The E-Gov Act mandates that all actions taken by Federal departments and agencies under this Act shall be in compliance with section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d). In September 2012, the Department of Justice issued its "Section 508 report to the President and Congress: "Accessibility of Federal Electronic and Information Technology." The report, authorized under Section 508, provides findings based on a survey of federal agencies on the accessibility of their electronic and information technology (EIT) and the procedures used to implement to requirements of Section 508. The Justice Department's report and additional information is available on the department's website at www.ada.gov/508. The following section contains the URL(s) for agencies' accessibility and 508 compliance program websites.

Department of Agriculture

Section 508 information can be found at http://www.ocio.usda.gov/policy-directives-records-forms/section-508.

Department of Commerce

Section 508 information can be found at http://ocio.os.doc.gov/ITPolicyandPrograms/IT_Accessibility/index.htm.

Department of Defense

Section 508 information can be found at http://dodcio.defense.gov/DoDSection508.aspx.

Department of Education

Section 508 information can be found at http://www.ed.gov/internal/accessibility-requirements.html and http://www2.ed.gov/internal/technical-standards-implementing-section-508.html.

Department of Energy

Section 508 information can be found at http://energy.gov/cio/department-energy-doe-and-section-508.

Department of Health and Human Services

Section 508 information can be found at:

- http://www.hhs.gov/web/508/index.html
- http://www.hhs.gov/ocio/policy/508_policy.html
- http://www.hhs.gov/web/508/Standards/index.html

Department of Homeland Security

Section 508 information can be found at http://www.dhs.gov/accessibility.

Department of Housing and Urban Development

Section 508 information can be found at http://portal.hud.gov/hudportal/documents/huddoc?id=s508-ins.pdf.

Department of the Interior

Section 508 information can be found at http://www.doi.gov/ocio/information_management/section-508.cfm.

Department of Justice

Section 508 information can be found at http://www.justice.gov/accessibility/accessibility_info.htm.

Department of Labor

Section 508 information can be found at:

- http://www.dol.gov/oasam/ocio/ocio-508.htm
- http://www.dol.gov/oasam/foia/dlms-chapters/dlms9-0600.htm.

Department of State

Section 508 information can be found at http://www.doi.gov/ocio/information_management/section-508.cfm.

Department of Transportation

Section 508 information can be found at:

- http://www.fta.dot.gov/about/13056.html
- http://www.faa.gov/about/office_org/headquarters_offices/aio/programs/ites/sec_508/
- http://www.nhi.fhwa.dot.gov/resources/section508.aspx
- http://www.fra.dot.gov/Page/P0165
- http://www.marad.dot.gov/about_us_landing_page/accessibility_certification/accessibility_certification.htm
- http://www.nhtsa.gov/About/Accessibility
- http://phmsa.dot.gov/about/accessibility
- http://www.dot.gov/drc/section-508.

Department of the Treasury

Section 508 information can be found at http://www.treasury.gov/about/role-of-treasury/orders-directives/Pages/td87-06.aspx.

Department of Veterans Affairs

Section 508 information can be found at http://www.section508.va.gov.

Environmental Protection Agency

Section 508 information can be found at http://www.epa.gov/epahome/accessibility.htm.

General Services Administration

Section 508 information can be found at http://www.gsa.gov/portal/content/105254.

National Aeronautics and Space Administration

Section 508 information can be found at http://www.nasa.gov/accessibility/section508/sec508_overview.html.

National Archives and Records Administration

Section 508 information can be found at http://www.archives.gov/global-pages/accessibility.html.

National Science Foundation

Section 508 information can be found at http://www.nsf.gov/policies/access.jsp.

Nuclear Regulatory Commission

Section 508 information can be found at http://www.nrc.gov/site-help/access.html.

Office of Personnel Management

Section 508 information can be found at http://www.opm.gov/html/access.asp.

Office of the Director of National Intelligence

Section 508 information can be found at www.dni.gov.

Small Business Administration

Section 508 information can be found at http://www.sba.gov/about-sba-info/accessibility.

Social Security Administration

Section 508 information can be found at http://www.socialsecurity.gov/accessibility/508_overview.html.

U.S. Agency for International Development

Section 508 information can be found at http://transition.usaid.gov/policy/ads/300/302mak.pdf.

C. Government-public Collaboration

The E-Gov Act requires agencies to sponsor activities that use information technology to engage the public in the development and implementation of policies and programs.. The following section contains agency examples of how agencies have utilized technology to initiate Government-public collaboration in the development and implementation of policies and programs.

Department of Agriculture

As USDA's chief scientific research agency, the Agricultural Research Service (ARS) works towards a better future through agricultural research and information. ARS is seeking public input in planning its

human nutrition research program for the next five years through an ideation platform. This input will help guide ARS in setting its human nutrition research priorities for the future. ARS research helps solve problems that affect Americans' lives every day. The public is invited to help ARS decide which problems should be its priorities. This research provides unique and important scientific information that serve as the foundation for many diet and health policy decisions in the United States. Scientists, medical doctors, the food industry, regulatory agencies, policy makers, and others use ARS' nutrition research data, including its nutrient database and food composition data, to identify ways to improve human health through food. The effort ran from September 4 through October 15, 2012.

As a result of its efforts, USDA-ARS received about 200 written comments which were taken into account in developing a five-year Action Plan for its Human Nutrition program. The Plan can be viewed on the ARS website. ARS human nutrition National Program leaders are now in the process of developing objectives for the research projects to address the problems identified in the Action Plan; this is followed by writing of ARS research project plans, and review by extramural experts. Research under this plan is implemented and conducted from 2014 to 2019.

USDA-ARS obtained written comments from many of our traditional stakeholders (targeted weekly e-mail blasts were sent to more than 150 human nutrition stakeholders, as well as other targeted communications with other stakeholders and customers) including other Federal agencies, agricultural commodity groups, and large food companies. We also got feedback from a large number of academics and private citizens, although comments from the latter were usually not relevant to the mission of ARS. USDA also used social media tools to promote the site.

Since we did not have an in-person stakeholder meeting, the agency saved approximately $100,000 in meeting and travel costs, and our stakeholders saved about $50,000 collectively.

Traditionally, ARS planned and held face-to-face workshops across the country with stakeholders and customers to gather input on setting research priorities. As resources are limited for the agency and many of its stakeholders, this information technology tool provides an opportunity to gather information from a wider range of customers, stakeholders and the public without requiring budget for travel or other meeting logistics. Without the use of the ideation platform, ARS may not have been able to solicit input on upcoming human nutrition research priorities.

Department of Commerce

The National Strategy for Trusted Identities in Cyberspace (NSTIC) is a White House initiative to work collaboratively with the private sector, advocacy groups, public sector agencies, and other organizations to improve the privacy, security, and convenience of sensitive online transactions. Commerce established a National Program Office, led by the NIST and NTIA, to coordinate the federal activities needed to implement NSTIC. Establishment of an Identity Ecosystem would allow individuals to validate their identities securely when they are performing sensitive transactions (e.g. online banking) and let them stay anonymous when they are not (e.g. surfing the web). The Identity Ecosystem would protect the privacy of individuals by reducing the need to share personally identifiable information (PII) in order to identify themselves at multiple web sites and by establishing consistent policies about how organizations use and manage PII in this Identity Ecosystem.

Throughout FY12, workshops were organized at NIST, Commerce, and the White House via live webcast to review the recommendations for establishing an Identity Ecosystem Governance structure, and to address specific issues surrounding the establishment of such a structure. Based on this input, NIST recommended the creation of a privately-led Identity Ecosystem Steering Group (IDESG) and

awarded a grant to spur its creation. A key tenet of the IDESG is to enable virtual participation through webcasts and other online tools, so that members can participate equally at meetings whether in person or online.

NIST also awarded grants to five organizations to pilot identity solutions that increase confidence in online transactions, prevent identify theft, and provide individuals with more control over how PII is shared. The pilots span multiple sectors and will test models and frameworks which are new to the existing marketplace.

Department of Defense

The Federal eRulemaking initiative facilitates public participation in the Federal regulatory process by improving the public's ability to find, view, understand and comment on federal regulatory actions and rulemaking materials. It is Departmental policy to make regulatory dockets electronically accessible and searchable, and to allow for electronic submission of comments using Regulations.gov, as part of our implementation of the E-Government Act of 2002. Department-related notices, draft rules open for public comment and other materials may be viewed at Regulations.gov. Additionally, websites like govpulse and OpenRegs allow the public to subscribe to alerts and provide additional search options.

eRulemaking has enabled DOD to harness the power of advanced digital technologies to make its rulemaking process more manageable, as well as expand and enhance the public's involvement in its rulemaking process. Through the use of information technology, the Department can increase the public understanding of rulemaking, improve policy decisions by making it easier for regulatory officials to analyze large volumes of data drawn from multiple sources, reduce administrative costs by allowing agency managers to coordinate rulemaking staff and other resources more efficiently, and increase regulatory compliance by increasing the public's understanding of what regulations require. eRulemaking will help the Department create higher quality rules, induce higher compliance rates, and foster greater public participation.

Department of Education

The 2010 National Education Technology Plan demonstrates the importance of educators becoming more connected to resources, tools, colleagues, experts, and learning activities, both within and beyond schools.

In collaboration with a wide range of educational organizations, the Connected Online Communities of Practice project is increasing the quality, accessibility, and connectedness of existing and emerging online communities of practice through four types of activities:

- Launching and leading new online communities of practice that address pressing needs in education and help us learn more about how such communities work best,
- Conducting design experiments within "test beds," online communities of practice run by collaborating organizations in which project staff will develop, facilitate, and evaluate selected content and activities that help address pressing questions,
- Undertaking case studies of both interesting communities of practice and of individual educational professionals' use of online communities and other forms of social media to connect, and
- Developing ideas about new designs and infrastructure that could better support educators in making productive connections.

Department of Energy

In April 2012, Energy challenged the American developer community to build apps that help utility customers make the most of Green Button electricity usage data. The Apps for Energy competition had a few key goals. The first was to encourage open innovation around Green Button – an open standard for sharing electricity data that is available to millions of utility customers. With Apps for Energy, Energy challenged developers to leverage the enormous potential of Green Button data by building web and mobile applications that help homeowners and business understand their energy usage and take action, so they can save money by saving energy. As the number of utilities around the country offering Green Button data increases, the importance of these applications will continue to grow. Equally important was the effort to create a thriving, energy-focused developer community that is committed to using technology to address real-world challenges, like reducing energy waste. The most significant challenge Apps for Energy developers faced was building applications that help consumers easily comprehend their energy data.

Department of Health and Human Services

HHS has led the Federal Government in using information technology to disseminate information and enable the transformation of how governments, the private sector, and citizens use information. The work of the National Library of Medicine has transformed access to biomedical information for researchers, practitioners, and patients.

HHS has continued "liberating" health data through the Health Data Initiative, making more and more data from HHS' vaults (from CMS, Centers for Disease Control (CDC), FDA and the National Institutes of Health (NIH), to name a few sources) easily available and accessible to the public and to innovators across the country. This information includes clinical care provider quality information, nationwide health service provider directories, databases of the latest medical and scientific knowledge, consumer product data, community health performance information, Government spending data and much more. Both HealthData.gov and Healthindicators.gov are examples of technology solutions to the Health Data Initiative. Additionally, and as part of HHS' growing use of cloud computing, HHS expanded and rehosted HealthData.gov in 2012 to increase the number of available data sets and to improve the public's ability to find information.

The continuing momentum of the Health Data Initiative was recently highlighted at a Health Data Initiative Forum (a.k.a. "Health Datapalooza") hosted on June 5-6, 2012, by the Institute of Medicine and HHS. The event brought together a diverse group of more than 1,500 data experts, technology developers, entrepreneurs, policy makers, health care system leaders, and community advocates to support innovative applications of health and health care data. This forum, a continuation of what has become an annual event, showcased the best products and services developed by companies that have harnessed HHS data to help consumers get the information they need, help doctors deliver better care, help employers promote health and wellness, help local policymakers make better-informed decisions and much more.

Department of Homeland Security

The DHS Office of Public Affairs (OPA) initiated the use of a web-based idea management and feedback tool that enables the Department to directly engage with the public on a range of issues and policies. This tool creates participatory, self-moderated communities and allows agencies to interact directly with the community that is formed around an idea. Agency representatives can leave comments

and communicate the status of an idea while building strong relationships with citizens by confirming that their voices are heard.

The idea management and feedback solution is available for headquarters offices, directorates, and operational components for separate dialogues and stand-alone iterations of the tool, with prior approval from OPA.

Some recent idea dialogues include:

- Federal Emergency Management Agency (FEMA) Employee Collaboration Community (201 ideas, 556 members)
- FEMA (790 ideas, 2637 members)
- E-Verify Listens (35 ideas, 184 members)
- Department of Homeland Security Office of Emergency Communications (0 ideas, 6 members)
- DHS.gov beta review (109 ideas, 80 comment, 265 members)

Department of Housing and Urban Development

Public Housing Authorities (PHAs) have a direct impact on their local communities, from providing support to residents, to improving the quality and availability of housing. To monitor this impact and understand the continuing needs of the community, HUD requires regular recertification of the PHAs and the reporting of various metrics about the services offered. Policies and tools will continue to be implemented through this initiative to reduce the reporting burden and increase the resources available to focus on mission delivery. The primary resource for this initiative is Public and Indian Housing One Stop Tool (POST), which allows PHAs to more easily and intuitively access information on HUD's website. The development of POST was based on public feedback solicited by the Delivering Together team through a "card-sorting" exercise on-site at several PHAs. This helped determine how PHAs looked for information on HUD's website. Clarifications of income verification hierarchy and excluded income verifications, promotion of tools to streamline the development of utility allowances, and the POST were published in January 2012. In POST, the centralization of links enables quick access to the numerous systems, tools and supporting information, resulting in efficient navigation of services available to PHAs. The links are organized according to eight categories: Public Housing Program, Systems, Housing Choice Voucher Program, Tools, Grants, Laws and Policies, Other Programs, and Directories.

Department of the Interior

The U.S. Geological Survey (USGS) is investigating the use of volunteers from the general public to update information about the location and names of common buildings such as police stations, fire stations, schools, and hospitals. This information would become part of The National Map (http://nationalmap.gov), a set of national databases that contain basic map information for the United States. The USGS typically maintains information in The National Map through partnerships with other governmental agencies and contracts with private sector firms. While the USGS has had a volunteer program in the past to maintain map information, technological advancements have made it much more feasible for the public to provide accurate locational information and for the USGS to incorporate this information into The National Map. In 2011, the USGS conducted a pilot project in the Denver, CO metro area to test the technology using a small number of university student volunteers. In 2012, the investigation was broadened to the state of Colorado and began to include contributions of data from the general public. If the results of the 2012 state level project are positive, further expansion of the data

collection area will occur in 2013. More specific information about the volunteer program can be found at: http://nationalmap.gov/TheNationalMapCorps/index.html.

Department of Justice

Justice is soliciting the public to provide input in two areas of the Federal Digital Strategy released by the White House in May 2012. The Federal Digital Government Strategy provides agencies with a 12-month roadmap that focuses on several priority areas, and will ensure that agencies use emerging technologies to serve the public as effectively as possible. Specifically, the Department asked the public to weigh-in on which information and services they like us to prioritize and make more tech and mobile-friendly. The two areas where input was solicited are:

1. What Justice Department information would you like to be able to access on mobile devices?

2. What Justice Department information, data, or applications would you like to us make available via APIs (Applied Programming Interface)?

For the public's consideration, Justice offered a few possibilities for each area. These can be viewed on Justice's Digital Strategy web page, www.justice.gov/digitalstrategy. The public's input combined with other internal and external conversations, will guide our digital plan in the coming months and years. The public was asked to provide their feedback on these two areas via opengov@usdoj.gov.

Department of Labor

In 2011, Labor established a Developer Community website (http://developer.dol.gov/) to assist, support, and encourage public entities to develop user friendly software applications using Labor datasets. Labor has also initiated challenges to the public via the www.challenge.gov website to create useful smart phone applications using Labor datasets and other public information. For example, in October 2011, the Labor announced the winners of two contests, launched in July 2011, for third-party developers to showcase innovative uses of Labor's data. SymSoft Solutions in Sacramento, Calif., with its "Where are the jobs?" application, won the Occupational Employment Statistics challenge to help connect unemployed workers with promising careers. Labor Mobile Application Development Contest Winners can be viewed at: http://www.dol.gov/dol/apps/winners.htm.

On August 9, 2012, Labor's Bureau of Labor Statistics economic data was used in consolidation with economic data from the Census Bureau and the Bureau of Economic Analysis, to create the Census Bureau's first mobile application called "America's Economy." The mobile app provides updated statistics on the U.S. economy, including monthly economic indicators and economic trends. The app also supports the real-time capture of 16 key Government statistics that drive business hiring, sales, and production decisions. The app is useful for small businesses, the construction industry, the banking industry, journalists, economists, planners, policymakers, and others who want or need to access or monitor U.S. economic data.

Department of State

In response to President Obama's directive entitled *Building a 21st Century Digital Government* and its comprehensive Digital Government Strategy (PDF/html5) aimed at delivering better digital services to the American people, in August 2012 State posted an entry to its official blog DipNote and cross-amplified the story on http://www.state.gov and other platforms. This blog entry invited the public to share their suggestions on mobile and API candidates by using the blog's "Comments" feature. Additionally, custom questions were added to State.gov's online survey to request public input on

mobile and API candidates. State.gov receives over two million page views per month; over a dozen comments from the blog and approximately 100 comments from survey were received. These comments from the public will be considered for future development activities.

Department of Transportation

DOT has also leveraged an idea management and feedback platform, first deployed in support of Open Government Plan development. DOT leverages this platform to gather public and expert feedback early in the policy development lifecycle and has recently used the tool to explore issues such as: women in blue collar transportation careers, implementing the freight and performance measurement requirements of recent legislation, and other strategic planning exercises. In addition, DOT advises Labor's ePolicyWorks initiative, a Web-based approach to policymaking that engages citizens and stakeholders by allowing them to collaborate on key issues in real-time, and is exploring opportunities to pilot the platform.

In addition, DOT's signature Open Government Initiative, outlined in version 2.0 of its Open Government Plan is the safety community on data.gov, http://safety.data.gov/.

Safety.data.gov is an Open Government initiative that seeks to build a safety community on the data.gov Web site. While DOT and other Federal agencies collect important safety-related data, DOT recognizes that releasing data alone does not fully leverage the potential of those datasets for discovering new information, inventing new products, or identifying complex patterns to improve decisionmaking.

DOT believes a data.gov community focusing on safety will create momentum behind the productive use of safety-related datasets. Safety.data.gov will serve as a data clearinghouse, and host forums, blogs, and discussions.

This Open Government flagship initiative will enable the public to make better safety-related decisions using both current statistical descriptions and explanations of the environment that will affect our future. Safety.data.gov will tap into the innovation of application developers, the immediacy of the internet, and information that the Federal Government collects to enable informed decisions that will enhance public safety and improve public health in the United States.

DOT's safety.data.gov team hosted a National Transportation Stakeholders meeting in March 2012 that facilitated collaboration between the initiative, stakeholders and developers. The meeting included a preview of the Web site for evaluation by stakeholders. An idea management and feedback exercise will be completed to further expand the scope of the conversation and provide additional feedback.

Department of the Treasury

To augment the President's emphasis on openness and transparency in government, FOIA enables citizens to access governmental records and establishes a citizen-centered process to efficiently meet the public's demand for timely information. Treasury continued implementation of a three-pronged solution for improving FOIA processing and public access to information, resulting in increased efficiencies and greater transparency of information balanced with the protection of non-releasable information. Prong 1 focused on the public by allowing online submissions of FOIA requests which has resulted in the majority of FOIA requests being submitted on-line for records pertaining to Departmental Offices. Prong 2 was implementation of a cloud tracking solution to manage the requests and citizens' information, and Prong 3 is in progress for implementing process improvements and utilizing the Department's Enterprise Content Management platform for FOIA processing workflows to facilitate collaborative document management of the myriad of documents involved in responding to a FOIA

request. The tools were selected because they provided improvements for both the public and Treasury personnel that process requests, were cost effective, and allowed for quick implementation. Treasury demonstrated and discussed the on-line submission functionality with several frequent requesters to get feedback on whether the tool was user friendly and gather ideas for future enhancements. Together the selected tools are known as goFOIA. The public access, tracking, and reporting pieces are hosted in the cloud. Treasury is currently evaluating the option of moving the citizen web services from the cloud provider to a multi-agency shared services platform for further cost reductions.

Treasury's Enterprise Content Management (ECM) goFOIA initiative was released on April 30, 2011, for citizens to post online requests: https://www.onlinefoia.treasury.gov/.

Department of Veterans Affairs

VA is an active and successful participant in the Federal Government's Inter-Agency eRulemaking initiative. This E-Government initiative provides the public an opportunity to view and comment on all proposed VA regulations by visiting a single Government website that displays VA regulations that have been published in the Federal Register and are open for public comment.VA uses the Federal Docket Management System to review and post public comments on the website, including those received by mail or other means. As a result, the public can actively participate in VA's rulemaking process as regulations are being developed. VA's Office of Regulation Policy and Management in the Office of General Counsel has a website located at http://www.va.gov/orpm, which links readers to the Electronic Code of Federal Regulations (eCFR) where all current VA regulations can be found.

Environmental Protection Agency

EPA utilized interactive webinars to collaborate with stakeholders on issues related to cleanup activities at federal Superfund sites across the country. Through this initiative we increased community engagement, provided greater transparency and explored ways to expand the utility and accessibility of electronic information. The webinars enabled us to continue a dialogue with the public which began at earlier face-to-face meetings. Electronic communication allowed us to bring together more stakeholders and federal agencies to focus on enhanced information access and innovative outreach tools.

A webinar entitled "New Developments in Information Sharing Tools" showcased the latest in data sharing technology being used by EPA and other federal agencies. Seventy-five people participated in the session which demonstrated how cleanup data are currently made available to the public. The webinar also included a presentation on the Open Government platform. This cutting edge data sharing tool provides 24-hour access to cleanup information along with publicly available data on demographics, health impacts, economics and environmental justice. Participants asked questions and provided suggestions on information content and delivery.

EPA also led a community webinar to solicit input on innovative outreach tools developed in collaboration with our federal partners. The webinar showcased a community video and training module on the Superfund five-year review process, which evaluates whether cleanup remedies remain protective of human health and the environment. More than 60 community members nationwide provided real-time, constructive feedback on the outreach tools. Comments were incorporated into the final products, ensuring they will have the greatest utility for the public.

General Services Administration

OCSIT's Digital Service Innovation Center team has been working diligently with the Presidential Innovation Fellows, the U.S. Chief of Technology, the U.S. Chief Information Officer and the White House Director of Digital Strategy to rapidly prototype a "MyGov" functionality, a streamlined and intuitive system for presenting information and accepting feedback around the needs of citizens. The "MyGov" functionality will provide a more simplified and unified experience tailored for citizen interactions with government and improving information exchanges benefiting both the public and federal agencies as well. The MyGov team engaged with the public via seven channels to share project progress and elicit feedback on the project and concepts. Through these channels, the public can help expand documentation, answer questions and join discussions; users can download and test the latest development versions and submit feedback; international communities can contribute translations in other languages; and developers can identify any issues.

National Aeronautics and Space Administration

The International Space Apps Challenge was an international code-athon style event that took place over a 48 hour period in cities on all seven continents on the weekend of April 21-22, 2012. The Challenge strived to achieve the US commitment to the Open Government Partnership by utilizing openly available data, supplied through NASA missions and technology, and the talent and skill of passionate volunteers from around the world to advance space exploration and improve the quality of life on Earth. Space exploration was the ideal catalyst to foster this culture of innovation. NASA, nine government agencies, and 90 other organizations hosted inaugural Challenge events online, and in 25 cities representing 17 countries on all seven continents. The event brought together 2,083 registered participants (ages 16-70) together to address 71 challenges that were grouped into four broad categories including open source software, open hardware, citizen science platforms, and data visualization. More than 100 unique solutions were developed in less than 48 hours during the event. All solutions were developed in a completely open source environment, and each have their own unique potential to go even further to address world and space technology challenges.

National Archives and Records Administration

On November 28, 2011, the Obama Administration released a Presidential Memorandum http://www.whitehouse.gov/the-press-office/2011/11/28/presidential-memorandum-managing-government-records) on Managing Government Records. This Memorandum tasked NARA with, among other things, developing a Directive directing agency heads to reform and improve records management practices within their agencies. The Memorandum also required the Archivist to consult with "other affected agencies, interagency groups, and public stakeholders."

In February 2012, NARA launched the "Managing Government Records" online forum to solicit input for the Directive. Records and information professionals, vendors, and the general public used this site to provide their ideas for improving the management of Federal records. Ideas were generated in the six categories specified in the Memorandum:

- Creating a Government-wide framework,
- Promoting practices that enable agencies to fulfill their mission,
- Maintaining accountability through documentation of actions,
- Increasing open government and access,
- Supporting agency compliance, and
- Transitioning from paper to electronic recordkeeping when feasible.

For nearly two months, (February 16, 2012 – April 13, 2012) 180 registered users posted 88 comments and cast 273 votes on 30 specific ideas. All of this input was evaluated by the team for potential inclusion in the final Directive that was issued on August 28, 2012.

National Science Foundation

NSF recognizes the value of collaboration between government and the public and encourages its use when possible. One recent example of NSF's successful collaboration with the public includes NSF's efforts to engage the public on its implementation of the Digital Strategy initiative. NSF used an idea management and feedback platform to solicit input from the public and help the agency prioritize which information sets to make accessible through web APIs. NSF invited the public to vote or comment on proposed information sets to help ensure the identified candidates would be the most useful and dynamic to NSF's stakeholder community. NSF used input from the public collaboration period to help determine which information sets should be prioritized for further development.

Nuclear Regulatory Commission

The NRC's Open Government Advisory Group, composed of representatives from the agency's public affairs, internal communications, and information technology organizations, oversees the agency's Open Government program. On December 6, 2011, the advisory group hosted a Webinar to solicit stakeholder input about activities to include in the next revision of the NRC's Open Government Plan, to be published in April 2012. As indicated in the meeting notice and agenda, the goal of the Webinar was to obtain feedback on the agency's Open Government accomplishments in 2010–2011, the high-value datasets published so far, and the goals pursued in our flagship initiative to enhance stakeholder engagement. NRC also hoped to learn what new initiatives stakeholders would like us to pursue as we establish our Open Government roadmap for the next two years.

To guide this discussion, we worked with a meeting facilitator who used an approach that focused on soliciting participants' views of the strengths, weaknesses, opportunities, and threats (SWOT) or challenges a program faces. This approach is often referred to as a SWOT analysis. We asked for these views on each of the cornerstones of our Open Government program: transparency, public participation, and collaboration.

In addition to the December 6, 2011 Webinar, we collected stakeholder views from responses to various blog posts and from feedback received from the agency's 2011 stakeholder strategic planning meeting. All of this feedback was summarized in a worksheet published on our public web site.

Office of Personnel Management

The USAJOBS program relies heavily upon collaboration with the public to balance the needs of Government agencies and job seekers in the continuous development and improvement of the USAJOBS site. Public feedback on USAJOBS content and functionality as well as on the federal hiring process is continuously collected and monitored through an online survey, the USAJOBS Help Desk, and social media pages. An online survey is presented to seekers at the USAJOBS site to collect feedback on site functionality, effectiveness and proposed changes. Through help desk submissions, seekers are able to comment on current functionality and processes and to even recommend functional changes in utilizing USAJOBS to find federal employment. Finally, social media pages are utilized by USAJOBS for open two-way communications between the program and seekers. Here seekers are able to begin discussions on the Federal recruitment, application and hiring processes with the program and

other seekers. Together, these exchanges contribute to continuously improving the services provided by USAJOBS.

Office of the Director of National Intelligence

The Intelligence Advanced Research Projects Activity (IARPA) continues to utilize the www.FedBizOpps.gov portal as its primary vehicle to initiate collaboration with the public (academia and industry) for research. During FY12, IARPA posted almost a dozen announcements on FedBizOpps.com for new program Broad Agency Announcements (BAA), Request for Information (RFI) and Proposers' Day Conferences. All three announcements initiated direct collaboration with the public. Over 100 abstracts/proposals from were received in response to the BAAs, nearly 150 responses to the RFls and over 100 people attended the conferences.

Small Business Administration

SBA is actively using technology to support Government-public collaboration. Banks, savings and loans, credit unions, and other specialized lenders participate with SBA on a deferred basis to provide small business loans. SBA hosts the web site www.sba.gov/for-lenders that provides lenders with resources they need to issue SBA loans.

SBA's Lender Portal allows lenders to view their own quarterly performance data, including their most current composite risk rating, the "Lender Risk Rating". The Risk Rating System is an internal tool to assist SBA in assessing the risk of each active 7(a) Lender's and Certified Development Company's (CDC's) SBA loan operations and loan portfolio.

The Lender Portal data comes from the Office of Credit Risk Management (OCRM) Loan and Lender Monitoring System (L/LMS). L/LMS obtains data from the SBA's 'system of record', the Loan Accounting System (LAS), as well as the 504LAMP database and the Partner Information Management System (PIMS). L/LMS also receives third party credit quality and business data from contractor Dun & Bradstreet, including the Fair Isaac Small Business Predictive Solution (SBPS) credit scores. Lenders can also access data on peer group and portfolio averages.

In addition to the Lender Portal technology, that supports Government-public collaboration; SBA coordinates many town hall meetings throughout the year. As an example, the National Small Business Week forum was open to the public. This forum provided free networking, educational sessions, and open dialogue for the public to give suggestions and recommendations to SBA. SBA forums encourage small business owners and entrepreneurs to attend and voice their opinions, ideas and concerns.

Social Security Administration

To develop ideas for the content of our refreshed Open Government plan, SSA used an online engagement 'tool' to solicit ideas from both employees and the public. Seeking a widespread and diverse participant base, we publicized the engagement on our Open Government portal, sent an agency-wide request to all employees, and reached out to our advocate audience and those who already receive our electronic updates. Both employees and the public posted suggestions, shared comments on one another's ideas, and "voted" on posted ideas. Once our plan was revised and posted in April 2012, we launched a second engagement to solicit feedback on the revised plan. We used the input collected through both engagements to strengthen and refine our plans.

U.S. Agency for International Development

USAID pro-actively works to collaborate with civilian groups and organizations internationally in ways that advance defined U.S. foreign policy and core values. To meet these goals, USAID implements the Secretary of State's Quadrennial Diplomacy and Development Review (QDDR). Experts from USAID have participated in QDDR working groups, and the State Department officially documents these experiences, as well as the strategic vision of the senior leadership of both agencies in a formal report. Technologically, USAID's implementation of QDDR emphasizes the importance of investing in innovation – identifying, testing, and scaling development solutions that can drastically improve outcomes and at a lower cost. USAID achieves this through the previously mentioned Development Innovation Ventures (DIV) initiative. USAID implements DIV as a QDDR mechanism for working with civilian partners to identify and test potential development solutions.

The DIV model emphasizes testing potential solutions and rigorously evaluating impact – often through randomized control trials – in order to identify what works and what does not, and helping scale only those solutions proven to produce development outcomes. The following example illustrates how QDDR's DIV implementation has initiated technological innovations and enhancement for the public in a specific international case:

USAID partnered with the Bill & Melinda Gates Foundation to launch the Haiti Mobile Money Initiative (HMMI) to encourage the start-up and scaling of mobile money products in Haiti following the 2010 earthquake. If successful, this effort will result in 5 million transactions. In January 2011, one year after the earthquake, HMMI awarded Digicel Bank and its partner bank Scotiabank, its "First to Market" award of $2.5 million for "Tcho Tcho Mobile." By 2012, USAID and its partners reached 300,000 subscribers and Haitians had conducted nearly 1,000,000 transactions.

Overall through the QDDR initiative, USAID engages the growing number of civilian agencies that engage in international activity: energy diplomacy, disease prevention, police training, trade promotion, and other areas. USAID's implementation of QDDR is designed to spur economic growth abroad, secure international investments, and create jobs domestically.

D. Credentialing

The E-Gov Act seeks to achieve interoperable implementation of electronic signatures for appropriately secure electronic transactions with Government. The following section contains current activities that agencies are undertaking to achieve the interoperable implementation of electronic credential authentication for transactions within the Federal Government and/or with the public.

Department of Agriculture

USDA OCIO has taken major steps in the utilization, acceptance, and integration of digital signature in multiple business and technical processes thereby improving operational efficiencies. As of the end of FY12, 15 business processes are enabled for digital signing enterprise wide; with the list growing daily as USDA agencies continue to adopt. Some highlights of these processes include: performance plans, evaluations and appraisals, award forms, reimbursable agreements, probationary agreements, employee review files, and security, compliance, and accreditation documents. Currently, two enterprise technical processes are also enabled for digital signing, which include workflow design and mplementation functions as well as electronic fax desktop capabilities. Additional USDA Digital Signature Accomplishments in FY12 include: (1) one completed Digital Signature training course created and distribution USDA-wide, along with the development of a second course currently in process; (2) a

completed Agency Utilization "Outreach" roll-out (currently working with 12 of the 29 agencies); and (3) User Guides and Job Aids developed for all current Operating Systems.

The increased capabilities, cost savings, and ease of use associated with digital signature have been overwhelmingly positive; with outreach activities expanding at a very high rate. Current agency utilization of digital signature has met or exceeded the multiple benefits USDA originally expected from this technology.

Department of Commerce

Homeland Security Presidential Directive 12 (HSPD-12) mandates the development and adoption of a Federal Government standard for Personal Identity Verification (PIV) cards. The implementation of this standard will ensure that identification data for Government employees and contractors is reliable and secure, and access to Government resources and information systems are appropriately controlled. The PIV card system will also create a "minimum level of trust" across the Federal Government, based on the minimum background check required to receive an access card. This initiative is being managed as part of a larger Government-wide Identity Management initiative. In alignment with the HSPD-12 directive, Commerce operates dedicated USAccess identification verification and badge issuance stations and is issuing PIV credentials to all employees and associates. All Commerce agencies have already implemented, or have plans in place to implement, the infrastructure required to support PIV cards to deliver PIV multifactor logical access authentication to all Commerce users. Further, Commerce implemented Managed Trusted Internet Protocol Service (MTIPS) to support the operating units within the Herbert C. Hoover Building in accordance with OMB's Trusted Internet Connection (TIC) initiative. Twelve of the Department's 14 operating units will be in compliance with OMB's TIC initiative by the end of the calendar year 2012. Additionally, NIST is completing an update to the PIV standard, FIPS 201, that introduces the concept of PIV-derived credentials to support mobile devices.

Department of Defense

The DOD has a long history of supporting the use of externally issued, or Non-Federally Issued (NFI), identity credentials. As early as 2004, DOD established procedures to approve non- DOD issued Public Key Infrastructure (PKI) credentials for use in DOD. These procedures have been maintained and still exist today. They have been used to evaluate and approve Personal Identify Verification (PIV), PIV-Interoperable (PIV-I), other commercial, and even foreign military PKI credentials. The list of DOD approved NFI PKI credentials can be found at http://iase.disa.mil/pki-pke/interoperability/index.html. While historically, the approval of NFI credentials for use in DOD has been focused on PKI, approval is being expanded to include credentials at lower information assurance levels (IAL); IAL-2 and IAL-3. However, per DOD policy, IAL-1 credentials are not allowed for authentication to DOD information systems.

The DOD is preparing a DOD CIO Memo to promulgate guidance on acceptance and use of NFI credentials. The memo requires DOD components to enable their information systems to accept approved NFI credentials for authenticating PIV-ineligible personnel. An executive summary outlining the DoD process for adoption and use of identity credentials, titled "*DOD's Adoption and Use of Non-Federal Issuer Credentials*," will be attached to the memo. The memo and accompanying executive summary are expected to be signed and released in 2013.

Department of Education

In FY12, ED published an Identity, Credential, and Access Management (ICAM) Roadmap that aligns with the Federal ICAM initiative aimed at addressing the gap between technology concept, maturation, and adoption; driving the need for interoperability of solutions; allowing for the evolution of capabilities to accommodate future needs; and ensuring solutions are secure, resilient, cost effective, and easy to use.

ED has implemented Physical Access Control Systems (PACS) for systems hosted on the network and established a basis for implementing Logical Access Control Systems (LACS) for information technology systems. Current LACS implementations at the Department are not centrally managed and provisioned. ED's target state will use PIV credentials for PACS and LACS, and programs whose constituencies are primarily Federal employees will utilize capabilities of the PIV card for access control. The issuance process for PIV cards will leverage common services through automated interfaces to improve efficiency in PIV processes.

To support the transition to the target state, ED has drafted an identity management concept of operations and system security policy, as well as initiated implementation of enterprise identity management services, which provide the foundation for improved trust and interoperability among the Department, other federal agencies and other external communities.

Department of Energy

Energy has implemented the use of electronic signatures allowing Department officials to sign documents and carry out business transactions electronically. The use of electronic signatures provides assurance that the authors and signatories of e-mails and/or electronic files are who they claim to be and provides significant advantages, such as improved security and streamlining business activities.

Department of Health and Human Services

HHS developed a two-pronged approach to electronic credentialing. To meet the requirements of Homeland Security Presidential Directive 12 (HSPD-12), HHS undertook an IT program to provide secure logical and physical access using Personal Identify Verification (PIV) cards for HHS employees and contractors. The resulting systems now enable PIV card logical access to approximately 150 systems and provide PIV card physical access to more than 200 HHS facilities. In FY12, the HSPD-12 program integrated HHS PIV card logical access with the Department of Defense MyPay system, and worked toward enabling HHS PIV card access to the OMB MAX portal.

To meet the needs of credential authentication of the public, HHS also undertook an effort to validate and maintain credentials for external users. The resulting system, iTrust, was developed and is operated by NIH in collaboration with the InCommon Federation and the OpenID Foundation. The iTrust system provides secure access to NIH systems to external users without the need to establish new user accounts. iTrust supports Government-to-Government, Business-to-Government, and Citizen-to-Government applications.

Department of Homeland Security

Current activities include the following:

- Homeland Security Information Network (HSIN) has applied to join the National Information Exchange Federation (NIEF) as a Relying Party to accept NIEF member agency credentials.

- HSPD-12 PIV Interoperability implementation with Department of Defense (DOD) Intelink-Unclassified
- Security Assertion Markup Language (SAML) federations services to support Financial Disclosure Management Reporting System
- Identity, Credential and Access Management Program Management (ICAM PMO) Collaboration with Program Manager for Information Sharing Environment (PM-ISE)
    - Federal Identity, Credential and Access Management (FICAM) Trust Framework Provider (TFP) Certification for the National Information Exchange Federation (NIEF)
- ICAM PMO Collaboration with PM-ISE Controlled Unclassified Information (CUI) /Sensitive but Unclassified (SBU) on Identity and Access Management (IdAM) Federation
    - Development of the IdAM Reference Architecture
- Requirements for Accepting Externally-Issued Identity Credentials
    - October 6, 2011 memo from Federal CIO to CIOs of Executive Departments and Agencies
- § Activity - DHS Science & Technology Directorate (S&T) implementation of Google level 2 third party credential for First Responder Community of Practice (FRCoP)
- National Strategy for Trusted Identities in Cyberspace (NSTIC)
    - DHS participation in Identity Ecosystem Steering Group (ICAM PMO, Cyber Security and Communications, Privacy, S&T Cyber Security Division)

Department of Housing and Urban Development

HUD is evolving and maturing its use of electronic authentication tools to support secure access to systems and data both internally and externally. Internally, HUD has issued FIPS 201 compliant personal identity verification (PIV) credentials to virtually all of its employees and applicable contractors. HUD is beginning to integrate use of these two-factor authentication credentials with the access controls to HUD's systems as an upgrade to the more typical user name and password approach. Externally, HUD has been using electronic authentication tools to permit secure access to systems and data by customers for many years. HUD has initiated a new project to consolidate and standardize its access control tools using contemporary technologies. This project will permit HUD to fully utilize the electronic signature capability on the PIV cards used by employees and contractors and reduce the number of system specific user names and passwords used by customers. The project will also implement better management controls for providing and revoking access to specific systems and data.

Department of the Interior

In early FY12, Interior completed the implementation of a Interior-managed, federal external directory service project it began in FY11 that provides both authentication and authorization services to external partners and collaborators who use the agency's on-premise collaboration systems. Today, the authentication, authorization, and federation services components Interior designed and deployed to support this initiative also support Interior's move to cloud-based email, collaboration, and electronic records and document management systems. In addition to the issuance of Security Assertion Markup Language (SAML) 2.0 tokens this platform issues for Interior employees to use for cloud services today, the framework is engineered to support the consumption SAML tokens from external providers per the CIO Memorandum, "Requirements for Accepting Externally-Issued Credentials." Interior's FY12 activities in support of the Memorandum were focused primarily on:

- New engineering work to extend the capabilities of the Agency's in-development, external-facing credential issuance system to also accept externally issued credentials.

- Inventory and analysis of the Agency's Level 1 and Level 2 web systems that allow or require the public and our partners to register or log on to access Interior's information.

As web systems inventory and prioritization resulting from systems analysis draws to a close, Interior will select Trust Framework Providers. Interior's newly developed infrastructure platform will provide the basis for work the Agency will begin in FY13 to enable Level 1 and Level 2 web sites where appropriate with authentication using externally issued credentials. Interior expects full implementation within the next two years per the Memorandum.

Department of Justice

Beginning in FY12, Justice has begun piloting the use of "identify federation" and "claims-based" authentication technologies. These technologies will ultimately support a single sign-on (SSO) user experience for users as well as provide a pathway for PIVCard application authentication compliance. These same technologies will also allow Justice to interoperate with external identity providers. This interoperability will provide a means to accept 3rd party identity credentials issued by such providers for Justice externally facing systems which allow members of the public and business partners to register or log on. Based on a preliminary review, Justice has a limited number of Level 1 web sites that qualify under the federal requirement for accepting externally-issued identity credentials. Justice expects to have a plan in place by the end of Q2 FY13 to remediate these sites, and any others Justice identifies, to accept externally issued credentials.

Department of Labor

Labor is currently pursuing the implementation of an enterprise-wide Identity Life Cycle Management Program consisting of Identity Creation and Management, User Authentication and Access Management. This effort will afford the Department the full lifecycle management of identities/credentials for Labor employees and contractors and support identity management and security services within the Department. This includes electronic credentialing and authentication services in compliance with recommendations and guidance from the Federal CIO Council sponsored committee known as the Federal Identity Credentialing and Access Management (FICAM) Committee and in compliance to the Homeland Security Presidential Directive 12 (HSPD-12).

The first phase of HSPD-12 was PIV-II, which has been operational since 2008. In 2011, the second phase began expanding PIV-II usage via Identity Management (IdM) project by designing and developing a framework of people, processes, and technologies intended to standardize and enhance the Labor's capability of managing identity data across multiple systems. This phase has a short-term goal of simplifying the log-in process leveraging existing credentials and a long-term goal of implementing a full-scope Identity Life-cycle Management solution interoperable with other enterprise-wide solutions.

The IdM project is in the development stage with simplified log-in processes. Labor will continue to introduce more advanced consolidation and integration appliances throughout 2013 while establishing the full-scope Identity Life-cycle Management framework.

Department of State

State does not have an externally facing application that accepts externally issued credentials. The Department considered the current approved trust frame work credentials, only one of which met the requisite assurance level for eServices, but at a significant cost. State will continue to review our external facing applications for viable solutions for accepting externally issued credentials.

State is collaborating with DOD on a pilot that will allow personnel from each agency to use PIV credentials to access each other's facilities. This initiative is currently in the planning and technical exchange phases. Upon completion of the pilot, the intent is to transfer the knowledge and solution to overseas locations with priority going to areas in theaters of operations. On the logistics side, State is in the process of PIV enabling its eServices application. Initially, this application will allow personnel assigned overseas to request household services, such as maintenance requests, using their PIV credential for authentication. This application will serve not only State personnel, but also personnel from other agencies assigned to U.S. embassies and consulates. This initiative is nearing the end of the development phase and will shortly move into the certification and accreditation phase before going live.

Department of Transportation

DOT is continuing to refine and implement its Identity, Credential, and Access Management (ICAM) program to better secure the authentication and access to DOT systems and applications. Specifically, DOT's IT security will be improved by authenticating internal users with Personal Identification Verification (PIV) cards and authenticating external users with PIV-interoperable (PIV-i) credentials and by utilizing the public key infrastructure (PKI) digital signature certificate stored on the PIV cards. DOT employees can currently send and receive digitally-signed emails both within DOT and to and from external partners as well as use the digital signature features of commercial products.

Department of the Treasury

The Treasury Enterprise Identity, Credential, and Access Management (TEICAM) investment program provides a consolidated view of Treasury's identity management activities across the Department. TEICAM will provide Treasury a standard for secure and reliable forms of identification and facilitate secure and timely access to information systems and facilities.

The current environment consists of multiple systems operating in silos and data stores with minimal communication amongst the distributed stacks. Treasury has recognized the challenges and risks associated with this type of environment and developed a phased approach to implementing Federal Identity, Credential, and Access Management (FICAM) by 2015.

The FY 2012-2015 Physical Access Controls (PACS)/Logical Access Controls (LACS) Goals represent the optimal schedule in which Bureaus can realistically achieve implementation:

- Sustain card issuance rate above 90% (FY11-FY15)
- Complete 100% National Capital Region (NCR) PACS rollout (FY11) and 100% nationwide PACS rollout (FY15)
- PIV Data Synchronization (PDS) is implemented for 3 bureaus (FY11) and department-wide (FY12-FY13)
- Complete and deploy a federated Enterprise-Single Sign-On infrastructure (FY13-FY14) and integrate Enterprise applications (FY13-FY15)
- LACS Local Network Access at 25% (FY11), 50% (FY12), and 100% (FY13)
- LACS Remote Network Access at 50% (FY13) and 100% (FY14)

Treasury will maintain a federated PACS/LACS architecture where Bureaus locally manage physical and logical access control systems and privileges. The HSPD-12 PIV credential will be the primary identification and access control badge for all PACS and enterprise LACS.

Department of Veterans Affairs

In accordance with the Homeland Security Presidential Directive 12 (HSPD-12), the VA Personal Identity Verification (PIV) program has enabled the Department of Veterans Affairs to meet the new security standards effectively and cost efficiently. The goal of the PIV program is to integrate and execute a working plan for a common identification card system for Federal Employees and Contractors. The PIV Program has provided the VA Credentialing Team with experience and insight into process improvements. Through the experience gained, the PIV Program has provided a robust system solution that is easily operated and maintained.

Environmental Protection Agency

In accordance with the October 6, 2011, Federal Chief Information Officer Memorandum, "Requirements for Accepting Externally-Issued Identity Credentials," the EPA is exploring potential solutions using existing technology which can be leveraged to implement Level 1 authentication for external partners. By taking advantage of EPA's existing IT Investments, the Agency expects to have a model that is cost effective as well as technically sound.

To date, EPA has conducted a preliminary e-authentication risk assessment to ascertain the assurance level of all websites that allow members of the public and business partners to register or log on. The volume of systems identified exceeded 300 which caused the Agency to issue a more thorough business review. The final e-authentication risk assessments are due March 30, 2013 and we are working to establish a more robust enterprise collaboration capability that can take advantage of the proposed multifactor authentication systems and meet the requirements.

EPA has identified options to leverage existing infrastructure and software systems that creates a gateway for external identity providers to use multiple protocols (e.g. Open ID, SAML, PIV, etc.) to authenticate and access Agency information resources. We anticipate that we will leverage an internal solution (Single Sign-on) with additional services to accept externally-accepted credentials from individuals that have already been vetted and credentialed by entities who operate within a trusted framework.

General Services Administration

In December 2010, the GSA Chief Information Officer issued a policy authorizing the use of digital signatures by GSA employees and contractors using standard GSA desktop applications to encourage the use of digital signatures within the agency, first, with standard GSA desktop applications, and later, with GSA business and administrative processes wherever they are useful.

GSA Digital Signature Policy (GSA Order CIO 2162.1) GSA is currently in the early adoption stage of using digital signatures agency-wide. GSA staff must use their GSA Access Card to create a digital signature. There are multiple digital certificates on the GSA Access Card, and the correct certificate must be selected for use with digital signatures.

National Aeronautics and Space Administration

NASA has begun leveraging externally-issued credentials in an effort to minimize costs and user impacts associated with cross-organizational access to information. Recognizing the business need for identity federation and also the potential gaps in current policy/process, NASA's Identity, Credential, and Access Management (ICAM) team recommended the implementation of a Pilot for Identity Federation. This effort allows collaboration capabilities between the NASA Ground Systems

Development and Operations (GSDO) Program at Kennedy Space Center, the Agency, and external partners. The pilot is essentially enabling two "new" credential types to access a NASA system - access using externally-issued CAC/PIV cards and using federated identity credentials (FICs).

The cost-savings of implementing identity federation for external user access to NASA resources versus the current method of issuing each external user a NASA identity is significant when considering the overhead in issuing/managing credentials, performing audits, and issuing/supporting virtual private networks (VPNs). For this reason and to meet the needs of organizations internal to NASA, this Pilot is cornerstone to the eventual implementation of NASA-wide identity federation service.

National Archives and Records Administration

NARA's Office of the Federal Register (OFR) accepts digitally signed documents for publication in the Federal Register from a wide range of agency customers. Agencies may use any Federal or private sector digital signature provider that operates in compliance with National Institute of Standards and Technology Digital Signature Standard FIPS 186-3. The OFR requires that Federal Register submissions be signed with a medium assurance level digital signature certificate, cross-certified by the Federal Bridge Certification Authority. Electronic original documents may be submitted as email attachments or via web portal, eliminating mailing, handling, and preservation of paper copies. OFR information technology staff work closely with the Federal PKI Policy Authority to develop new tools and processes that promote widespread adoption of digital signature applications.

National Science Foundation

NSF's use of single sign-on credentials allows members of the research community to use one ID to log into all external NSF systems, including FastLane and Research.gov. In order to further increase interoperability for the research community, NSF joined the InCommon Federation to provide simpler and easier access to online services. Using InCommon technology developed under a NSF-funded grant, researchers can use their university-issued user ID and password to login to Research.gov and access agency grants management services. NSF's integration with InCommon improves ease of access to NSF information and services by the public by improving the way institutions conduct business with NSF. Additionally, NSF has implemented "Open ID," which allows the public to use G-mail to log on to Research.gov's public-facing functions.

Nuclear Regulatory Commission

The NRC is currently developing a comprehensive plan to address guidance published by the Chief Information Officers (CIO) Council in the Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance. This plan will address many facets of electronic credential authentication both within the Federal Government and with the public.

Specifically within the area of credentialing, the NRC has been primarily focused on issuing Public Key Infrastructure (PKI) based digital certificates for both internal staff and external partners for electronic credential authentication and other purposes. NRC employees and contractors have been issued Shared Service Provider (SSP) Personal Identity Verification (PIV) cards, as well as SSP Software (SW) certificates that are fully compliant with all relevant standards and policies.

For external partners to the agency that need to interact with the Agency's electronic authentication systems, most notably the Electronic Information Exchange (EIE) and the National Source Tracking System (NSTS), the NRC has issued Federal Bridge Cross-Certified PKI credentials at various

assurance levels: Rudimentary (Level 1), Basic Assurance (Level 3), and Medium Hardware (Level 4). This is in accordance with Title 10 of the Code of Federal Regulations (10 CFR) Part 50, "Domestic Licensing of Production and Utilization Facilities," which requires digital certificate authentication for users of certain NRC systems. The NRC is also developing an implementation plan for a One-Time Password (OTP) solution to be used for lower level electronic authentication (Level 3 and below).

Office of Personnel Management

All applications within OPM's environment have been mapped to the level of authentication defined in NIST 800-63. Most applications are either internal or have a level of authentication that is greater than the E-Government initiative levels. We are actively pushing Personal Identity Verification (PIV) card usage within the agency. Already completed is the requirement for external users to use their PIV cards for access to OPM and OPM systems remotely. Currently in progress is the agency's push for all internal users of computer resources to authenticate using PIV cards. We expect this project to be completed in FY13. The Office of the Chief Information Officer is also working very hard to put in place technical controls that will facilitate the ability of the public to register their personal authentication measures with OPM public facing applications. Significant progress is anticipated during FY13 and OPM expects to be the federal leader in incorporating this innovative strategy and bringing better collaboration for the utmost transparency between the Federal Government and the public.

Office of the Director of National Intelligence

ODNI currently uses PKI certificates for electronic credential authentication across the IC. Each IC agency manages their own PKI certifications, and ensures they are compliant across the community.

Small Business Administration

HSPD-12 falls within the scope of Identity and Access Management. The implementation of HSPD-12 will ensure that identification of Government employees and contractors is reliable and secure. The establishment of the PIV credential as part of a broader enterprise solution enables common service capabilities in secure and reliable transactions. Further, it expedites SBA's ability to enable IT solutions that directly address business needs for disaster response, small business services such as electronic workflow services, and reduction in other existing investments for help desk operations and password management. E-Authentication falls within the scope of Identity and Access Management (IAM). This initiative expands E-Government by providing users access to online services that require authentication, using a solution that is secure and convenient for customers, resulting in an improvement in the taxpayer experience. The IAM initiative provides a robust, secure, centralized solution that automates the provisioning and de-provisioning of user identities, and manages each aspect of the identity lifecycle. By automating these services SBA integrates the independent management frameworks currently in SBA applications. This initiative will provide a secure and operationally focused security services that utilize industry proven solutions and adhere to well defined industry and federal standards.

Social Security Administration

In May, SSA launched a new authentication service to enhance our Internet services. The implementation of MySocialSecurity opens the door to a life-long electronic relationship with our customers. The one-two punch of better authentication through the electronic access application, combined with the user-centric presentation made possible for MySocialSecurity will make the use of the agency's online applications a first of its kind creation in the Federal Government and more akin to

what the public is used to interacting with on the Internet. The new authentication service positions SSA to federate credentials and be interoperable with other agencies' systems.

Efforts to federate with identity providers will be built on our successes federating with other agencies. SSA moved its first Security Assertion Markup Language (SAML) 2.0 federation into production on October 13th, 2012. It is a low-risk social media application hosted on a platform by the National Technical Information Service (www.NTIS.gov). Once managing the new federation software is internalized, the Financial Management Service's Treasury Check Information System is the next SAML 2.0 objective, upgrading from SAML 1.0 to SAML 2.0.

Key Points:

- SSA's has employed authentication federations since 2004.
- SSA has procured Tivoli Federated Identity Manager to enhance our capabilities; it supports most federation protocols, such as WS-Federation, SAML 1.0, SAML 1.1, and SAML 2.0.
- The social media application, hosted by NTIS.gov, is using the SAML 2.0 Web Browser SSO Profile, as it is the only approved SAML profile for federal applications (http://www.idmanagement.gov/pages.cfm/page/ICAM-TrustFramework-Scheme)

U.S. Agency for International Development

HSPD-12 Personal Identification Verification (PIV) cards are identification cards used for logical access into our IT systems and physical access into USAID facilities. USAID's cards are issued by the Department of State (State). State, with OMB support, is working on a solution to issue cards to employees, including contractors and direct hires outside of State, and have been given an approved wavier from HSPD-12 and the requirements of OMB Memorandum 11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12–Policy for a Common Identification Standard for Federal Employees and Contractors*.

The State solution that USAID will also use is anticipated to be complete in 2014. Meanwhile, USAID has implemented control gates within the System Development Life Cycle (SDLC) to ensure that new applications be PIV-enabled prior to deployment and that legacy systems are required to have the implementation on their SDLC roadmap in accordance with OMB M 11-11.

E. USA.gov activities

The E-Gov Act seeks calls for an integrated Internet-based system of providing the public with access to Government information and services. The following section contains URL(s) for agency activities on USA.gov.

Department of Agriculture

USA.gov activities can be found at http://www.usa.gov/Agencies/Federal/Executive/Agriculture.shtml.

Department of Commerce

USA.gov activities can be found at:

- http://www.usa.gov/directory/federal/department-of-commerce.shtml
- http://apps.usa.gov/americas-economy.shtml
- http://apps.usa.gov/national-weather-service.shtml

- http://apps.usa.gov/release-mako.shtml.

Department of Defense

USA.gov activities can be found at http://www.usa.gov/Agencies/Federal/Executive/Defense.shtml.

Department of Education

USA.gov activities can be found at http://www.usa.gov/Citizen/Topics/Education-Training/Education.shtml.

Department of Energy

USA.gov activities can be found at http://www.usa.gov/directory/federal/department-of-energy.shtml.

Department of Health and Human Services

USA.gov activities can be found at http://www.usa.gov/Agencies/Federal/Executive/HHS.shtml.

Department of Homeland Security

USA.gov activities can be found at:

- http://www.usa.gov/directory/federal/department-of-homeland-security.shtml
- http://www.usa.gov/directory/federal/transportation-security-administration.shtml
- http://www.usa.gov/directory/federal/national-flood-insurance-program.shtml
- http://www.usa.gov/directory/federal/federal-emergency-management-agency.shtml.

Department of Housing and Urban Development

USA.gov activities can be found at:

- http://www.usa.gov/directory/federal/department-of-housing-and-urban-development.shtml
- http://www.usa.gov/directory/federal/office-of-fair-housing-and-equal-opportunity.shtml
- http://www.usa.gov/directory/federal/federal-housing-administration.shtml
- http://www.usa.gov/shopping/realestate/mortgages/mortgages.shtml
- http://www.usa.gov/directory/federal/community-planning-and-development.shtml.

Department of the Interior

USA.gov activities can be found at http://www.usa.gov/directory/federal/department-of-the-interior.shtml.

Department of Justice

USA.gov activities can be found at http://www.usa.gov/Agencies/Federal/Executive/Justice.shtml.

Department of Labor

USA.gov activities can be found at:

- http://www.usa.gov/directory/federal/department-of-labor.shtml
- http://www.usa.gov/Citizen/Topics/Benefits.shtml#Jobs_and_Education_Assistance

- http://www.usa.gov/Citizen/Topics/Education-Training.shtml.

Department of State

USA.gov activities can be found at http://www.usa.gov/Agencies/Federal/Executive/State.shtml.

Department of Transportation

USA.gov activities can be found at http://www.usa.gov/directory/federal/department-of-transportation.shtml.

Department of the Treasury

USA.gov activities can be found at:

- http://www.usa.gov/Agencies/Federal/Executive/Treasury.shtml
- http://www.usa.gov/directory/federal/alcohol-and-tobacco-tax-and-trade-bureau.shtml
- http://www.usa.gov/directory/federal/bureau-of-engraving-and-printing.shtml
- http://www.usa.gov/directory/federal/bureau-of-the-public-debt.shtml
- http://www.usa.gov/directory/federal/financial-management-service.shtml
- http://www.usa.gov/directory/federal/internal-revenue-service.shtml
- http://www.usa.gov/directory/federal/office-of-the-comptroller-of-the-currency.shtml
- http://www.usa.gov/directory/federal/united-states-mint.shtml.

Department of Veterans Affairs

USA.gov activities can be found at http://www.usa.gov/directory/federal/department-of-veterans-affairs.shtml.

Environmental Protection Agency

USA.gov activities can be found at http://www.usa.gov/Citizen/Topics/Environment-Agriculture/Environment.shtml.

General Services Administration

USA.gov activities can be found at http://www.usa.gov/directory/federal/general-services-administration.shtml.

National Aeronautics and Space Administration

USA.gov activities can be found at http://www.usa.gov/directory/federal/national-aeronautics-and-space-administration.shtml.

National Archives and Records Administration

USA.gov activities can be found at:

- http://www.usa.gov/directory/federal/national-archives-and-records-administration.shtml
- http://www.usa.gov/Topics/Reference-Shelf/Libraries.shtml.

National Science Foundation

USA.gov activities can be found at http://www.usa.gov/directory/federal/national-science-foundation.shtml.

Nuclear Regulatory Commission

USA.gov activities can be found at http://www.usa.gov/directory/federal/nuclear-regulatory-commission.shtml.

Office of Personnel Management

USA.gov activities can be found at:

- http://www.usa.gov/directory/federal/office-of-personnel-management.shtml
- http://www.usa.gov/Federal-Employees/Federal-Employees-Gateway.shtml
- http://blog.usa.gov/post/11995704485/get-answers-to-your-questions-about-the-new-usajobs
- http://apps.usa.gov/usajobs.shtml
- http://www.usa.gov/Citizen/Topics/Government-Jobs.shtml.

Small Business Administration

USA.gov activities can be found at http://www.usa.gov/directory/federal/small-business-administration.shtml.

Social Security Administration

USA.gov activities can be found at:

- http://www.usa.gov/directory/federal/social-security-administration.shtml
- http://www.usa.gov/directory/federal/office-of-public-inquiries.shtml.

U.S. Agency for International Development

USA.gov activities can be found at http://www.usa.gov/directory/federal/agency-for-inter-development.shtml.

F. eRulemaking

The E-Gov Act seeks to assist the public, including the regulated community, in electronically submitting information to agencies under Federal requirements, by reducing the burden of duplicate collection and ensuring the accuracy of submitted information. The following section contains descriptions the on-line electronic regulatory submission capabilities at agencies, specifically, the usage of Regulations.gov and the Federal Docket Management System.

Department of Agriculture

The eRulemaking Program has simplified the public's participation in USDA’s rulemaking process by making regulatory information more accessible on Regulations.gov. Regulations.gov improves USDA public engagement by supporting the notice and public comment process for rulemakings.

In FY12, USDA posted 290 rules and proposed rules, 850 Federal Register notices, and 38,143 public submissions in Regulations.gov. USDA also posted 119 documents that consisted of supporting and related materials associated with other postings. Overall, USDA provides public access to 39,479 documents in Regulations.gov.

The eRulemaking Program offers streamlined internal rulemaking business processes with agency access to FDMS.gov. USDA had 140 staff using FDMS.gov in FY12, and created 107 regulatory dockets in FDMS for new regulatory actions published in FY12. The agency has received 37,206 public comments via Regulations.gov that are directly stored in FDMS.

USDA Retrospective Plan, required under EO 13563, is posted on the Regulations.gov Exchange at http://exchange.regulations.gov/topic/eo-13563. In addition, USDA has created a docket available on Regulations.gov for public comment on USDA's plan (Docket ID USDA-2011-0001).

Department of Commerce

The eRulemaking program provides substantial benefits as an electronic docket solution for Commerce to manage their regulatory information (FDMS.gov) and to post documents for public comments as well as other submissions (Regulations.gov). Commerce's participation in the eRulemaking E-Government Program enhances the public's access to and participation in the regulatory process, improves Commerce's regulatory processes, and creates transparency for all regulatory decisions. Participation in this program allows Commerce to fulfill the E-Government Act of 2002 requirements by providing a publicly accessible website containing electronic dockets for regulations.

The eRulemaking Program has simplified the public's participation in the Commerce rulemaking process by making regulatory information more accessible on www.Regulations.gov. In FY12, Commerce posted 569 rules and proposed rules and 142 Federal Register notices, received 8,508 public comments, and provided public access to 9,779 documents at www.Regulations.gov. Regulations.gov improves the public's engagement with Commerce by supporting the notice and public comment process for rulemaking and promoting public participation for an open exchange of regulatory information.

The FDMS docket management system provides Commerce staff with continuous improvement of internal docket management functionalities, electronic recordkeeping, and the ability to publicly post all relevant documents on Regulations.gov (e.g., Federal register documents, proposed rules, notices, supporting analyses, and public comments). In FY12, 150 Commerce staff members used FDMS.gov, which facilitated the creation and posting of 274 regulatory dockets in FDMS. Commerce received 8,508 public comments via Regulations.gov. These comments are stored directly in FDMS.

Department of Defense

DOD use of the eRulemaking Federal Docket Management System (FDMS) and Regulations.gov has increased citizen access and participation in the DOD rulemaking process. FDMS provides for document management with an electronic record-keeping capability. FDMS enables Department users to create, revise, and manage their docket materials through the use of role-based access controls and workflow and collaboration processes. Regulations.gov provides a centralized location for citizens to provide feedback on DOD rulemaking activities. Regulations.gov provides citizens a user-friendly web form to submit comments and supporting documents, offers simple and sophisticated searches, bookmarking, email notifications, and other social media tools. Additionally, regulatory officials can use Regulations.gov to view, download, and analyze comments submitted for their rulemakings.

Department of Education

ED continues to seek greater and more useful public participation in its rulemaking activities through the use of transparent and interactive rulemaking procedures and new technologies. ED participates in www.regulations.gov (Regulations.gov), an electronic, single, Government-wide access point that enables the public to submit comments on Federal regulatory documents and to read and respond to comments from the public. ED accepts public comments on all of its proposed and interim final regulations, as well as an increasing number of other regulatory documents, through Regulations.gov. In FY12, after a three-month regulatory negotiation with the affected community, ED published Federal Student Aid proposed regulations under title VI of the Higher Education Act of 1965, as amended. ED received 2891 comments on these proposed regulations. Several offices worked on reviewing, organizing, and responding to these comments. ED users of the Federal Docket Management System (FDMS) could access the comments at the same time and at any time day or night. The non-Federal members of the negotiating committee and the public also had immediate access to the comments in Regulations.gov. Public users could respond to other commenters' suggestions. Receipt of FDMS comments will result in final regulations being published faster than ever before.

Department of Energy

Energy's participation in the eRulemaking Program enhances public's capability to access and participate in the regulatory process through electronic systems and improves Energy regulatory processes and transparency of regulatory decisions. This program allows Energy to fulfill the E-Government Act of 2002 requirement to ensure a publicly accessible website containing electronic dockets for regulations. The eRulemaking Program provides value to Energy with cost savings of developing and operating an agency-specific electronic system.

The eRulemaking Program has simplified the public's capability to participate in the Energy rulemaking process by making regulatory information more accessible on Regulations.gov. Executive Order 13563 calls on agencies to promote public participation and an open exchange of information, and perspectives among State, local, and tribal officials, experts in relevant disciplines, affected stakeholders in the private sector, and the public as a whole. Regulations.gov improves Energy capability to engage the public by supporting the notice and public comment process for rulemakings.

The eRulemaking Program increases Energy's capability to post rules, proposed rules and materials related to other postings. In FY12 Energy posted 252 rules and proposed rules in Regulations.gov. Energy also posted 1,831 documents that consisted of supporting and related materials associated with other postings.

The eRulemaking Program also increases Energy's capability to offer streamlined internal rulemaking business processes with agency access to FDMS.gov. This capability enabled Energy to create 99 regulatory dockets in FDMS for new regulatory actions published in FY12. The agency received 407 comments via Regulations.gov that are directly stored in FDMS.

Department of Health and Human Services

All HHS regulatory proposals inform the public about how comments on the proposals can be submitted to Regulations.gov. Notices of proposed rulemaking provide the public with the opportunity for electronic submission of comments before the Agency moves to issue a final rule.

The FDA and CMS use the Federal Docket Management System (FDMS) for their rulemaking business.

Process and Background:

CMS and FDA use FDMS to process all regulations and notices. Specifically, all regulations and notices published in the Federal Register are posted to Regulations.gov. With limited exceptions, public comments are processed and posted at Regulations.gov for public viewing.

CMS issues an average of 150 Federal Register documents per year. FDA issued 705 Federal Register documents in 2009. The number of comments for each regulation varies, but in 2009 CMS received over 25,000 comments.

Benefits to the Public:

Fewer citizens have to go to FDA in person to view a document. The change has been dramatic. FDA public-room visits from visitors have decreased, from 1,203 in 2007 to 351 in 2009. And as a result of increased web accessibility, related FOIA requests decreased from 1,135 in 2007 to 323 in 2009.

CMS staff note that FDMS has provided the public with greater access to CMS's regulations by allowing the public to view the CMS regulations online. In addition, FDMS provides the convenience of allowing the public to submit comments electronically and participate more easily in the rulemaking process

Department of Homeland Security

The eRulemaking Program has simplified the public's participation in the DHS rulemaking process by making regulatory information more accessible on Regulations.gov. Executive Order 13563 calls on agencies to promote public participation and to support the open exchange of information and perspectives among State, local, and tribal officials, experts in relevant disciplines, affected stakeholders in the private sector, and the public as a whole. Regulations.gov improves DHS public engagement by supporting the notice and public comment process for rulemaking.

In FY12 DHS posted 785 rules and proposed rules, 974 Federal Register notices, and 6,551 public submissions in Regulations.gov. DHS also posted 776 documents that consisted of supporting and related materials associated with other postings. Overall, DHS provides public access to 9,307 documents in Regulations.gov.

The eRulemaking Program offers streamlined internal rulemaking business processes with agency access to FDMS.gov. DHS created 1,105 regulatory dockets in FDMS for new regulatory actions published in FY12.

Department of Housing and Urban Development

HUD participates in the Government-wide eRulemaking initiative, Regulations.gov. The goals of this initiative are to increase public access to and participation in developing HUD regulations and other related documents that can impact the public, and to promote more efficient and effective rulemaking through public involvement. HUD believes that Regulations.gov is meeting these goals.

The eRulemaking initiative has increased meaningful public participation by enabling HUD to process large numbers of public submissions related to proposed rules in a much more efficient and timely manner. For example, in a rule relating the FHA Mutual Mortgage Insurance Fund, during FY12 HUD received over 1600 public comments. The fact that the comments are available online at Regulations.gov

is an invaluable resource for the public and has greatly reduced the time required for agency personnel to analyze the issues raised in the public comments.

Additionally, the eRulemaking initiative has simplified the public's participation and reducing barriers to public participation.

Department of the Interior

Interior is a supporting partner to the eRulemaking initiative. Interior fulfills its obligation under the E-Government Act of 2002 to maintain a publicly accessible website containing electronic dockets for regulations. Interior complies with Executive Order 13563, *Improving Regulation and Regulatory Review;* and Executive Order 13609, *Promoting International Regulatory Cooperation*; the Open Government Partnership National Action Plan; and the Presidential Memorandum on Managing Government Records. Interior efficiently processes large numbers of comments electronically. The two best examples of this in FY12 were the following two Fish and Wildlife Service regulations:

- Removal of the Gray Wolf in Wyoming From the List of Endangered and Threatened Wildlife
- 90-Day Finding on a Petition to List All Chimpanzees as Endangered

For these two rules, Interior received 350,000 comments, and it estimates that eRulemaking saved $1,010,208. This is an estimate of the costs saved by not using a completely manual, paper-based system of comment processing. The estimate is based upon an estimated processing time per comment that is 1/8 the time required using a paper-based system, and a processing cost of $24.74 per hour.

Department of Justice

With one single online website, the Federal Docket Management System (FDMS) enables Justice to improve public access to all rulemaking material. Additionally it provides a central location for the public to find and comment on Justice regulatory actions that affect their lives. The components of Justice with more active regulatory and notice programs are the Bureau of Alcohol, Tobacco, Firearms, and Explosives, the Civil Rights Division, the Drug Enforcement Administration, the Executive Office for Immigration Review, and the Federal Bureau of Investigation. In FY12, Justice created 39 regulatory dockets in FDMS for new regulatory actions published. The agency has received 2,013 public comments via Regulations.gov that are directly stored in FDMS. In FY12, Justice posted a total of 48 rules and proposed rules.

Department of Labor

Since 2006 Labor has participated in the Government-wide eRulemaking initiative, which is comprised of the FDMS system and www.regulations.gov. The Department’s use of FDMS provides the public, especially interested stakeholders, easy access to the comments received on proposed rules through Regulations.gov. These E-Government initiatives facilitate an open and transparent rulemaking process. The Department has also developed a new website (www.dol.gov/regulations/) that provides the public a central point to learn more about the regulatory process and specific Labor regulatory activities and facilitate access to Labor regulatory material. This new website also provides the public a live web experience where the Secretary of Labor and other Labor executive leadership staff answered questions about the Labor regulatory agenda submitted online from the public.

Department of State

State uses the Federal Docket Management System (FDMS) to create and manage dockets, docket phases and sequences on Regulations.gov, which is publicly accessible. FDMS is the electronic repository for all Department rulemaking and non-rulemaking documents such as guidance documents, agency directives and policy interpretations. The Department uses a separate docket to manage a regulatory action. Department documents that are published in the Federal Register (FR) are accessed through FDMS. Metadata (e.g. docket phase, point(s) of contact, etc.) is added to the document and is viewable by the public.

The document or documents are posted to Regulations.gov. A docket is created and associated with a document requesting public comment. Metadata (e.g. docket phase, point(s) of contact, etc.) is added to the document and is viewable by the public. State user permissions and assignments are made in the process of creating the docket. Once the document has an associated docket, the public, using Regulations.gov, has access to the FR document. Once posted, the public can view a description of a document currently open for comment, read the full text of the document, and submit comments. Public users may submit a comment on any document open for public comment on the Regulations.gov website.

State uses FDMS and Regulations.gov to support a number of activities beyond rulemaking for public viewing and/or to solicit public comment. These include publication of guidance documents, agency directives and policy interpretations.

Department of Transportation

DOT has a memorandum of understanding (MOU) with the EPA to participate in the Federal Docket Management System (FDMS) at http://www.regulations.gov. DOT also promotes public participation via the Regulation Room.

DOT's Regulation Room pilot is described in Section 4.1 of DOT's Open Government Plan. Regulation Room is a pilot project in partnership with the Cornell eRulemaking Initiative (CeRI) to discover the best ways of using Web 2.0 and social networking technologies to further rulemaking efforts. Normally, an agency issues its proposed rulemaking in the Federal Register and may take such additional steps as issuing a press release and posting the document on its Web site, inviting the public then to submit comments through Regulations.gov, mailing in a letter to the agency, or occasionally by attending a public meeting. The design of this process results in a series of one-way communications, where the Government speaks to the public and then various members of the public speak back to the Government.

FMCSA piloted a rule on electronic on-board recorders (EOBRs). During the time the rule was open on Regulation Room, 5,328 unique visitors came to the site. There were 8,855 total visits, with people spending an average of 3.41 minutes on the site. Of the issue posts, the average time on the page was longest for What Will It Cost (4.48 minutes) and shortest for Would Penalties/Enforcement Change (2.13 minutes). Based on answers to a survey at registration, 27% of those who registered said that they had previously submitted a comment in a federal rulemaking. The pilot is archived at http://regulationroom.org/eobr/use/

Department of the Treasury

Treasury was an early participant in the eRulemaking initiative, Regulations.Gov, and has numerous proposed and interim rules and other materials posted for public comment and review on that site. Treasury uses the Federal Register to publish notices on its rulemaking activities. In addition, it posts its proposed and final rules to Regulations.Gov, the Federal eRulemaking Portal. The public can review, read, and comment on all Treasury's postings on the Portal.

Treasury has been in compliance with the e-rulemaking requirement by posting proposed and interim rules for public comment on Regulations.gov on a regular basis. Treasury links to regulations.gov in the footer on every page of Treasury.gov.

Department of Veterans Affairs

The Office of Regulation Policy and Management's (ORPM) (http://www.va.gov/orpm) was established to remedy deficiencies in VA's rulemaking process by providing centralized supervision and coordination of regulation development, tracking, control, policy integration, and economic impact analyses for proposed VA regulations. The eRulemaking program is a collaborative, inter-agency effort with the EPA to establish a common, automated, and integrated repository for managing Federal rulemakings and non-rulemaking actions that follow a structured notice and comment process. This project consolidates the dockets of various departments and agencies and centrally manages them through a web-based environment offering services such as one-stop access, search capabilities, public comment submission, email notification, bookmarking, and electronic records management.

Environmental Protection Agency

EPA is the managing partner of the eRulemaking Program. The eRulemaking Program operates www.regulations.gov, a web-based application providing public access on one website for all Federal regulatory dockets, and the Federal Docket Management System (FDMS), a single application allowing partner agencies to effectively manage their rulemaking process.

Thirty-eight partner agencies use FDMS to post regulatory dockets on Regulations.gov. All rulemakings published in the Federal Register are available on Regulations.gov, and 92% of those rulemakings have associated rulemaking dockets posted on Regulations.gov by partner agencies. Regulations.gov received 394,870 public comments via the online web form, and an average of 1.7 million visits and 8.3 million hits per month in FY 2012.

To meet the goals of the U.S. National Action Plan and Executive Order 13563 "Improving Regulation and Regulatory Review," the eRulemaking Program enhanced Regulations.gov by re-designing the public interface and deployed a new regulatory docket folder. The eRulemaking Program has also improved public data sharing with the launch of an Application Programming Interface (API), a web service for accessing Regulations.gov data and public comments.

As a participating agency, EPA posted 1,277 rules and proposed rules, 989 Federal Register notices, and 16,518 supporting and related materials for public access and review on Regulations.gov in FY12. In addition, EPA posted over 64,692 comments submitted for consideration in Agency actions. Overall, EPA made available 83,578 documents on Regulations.gov in FY 2012.

General Services Administration

GSA utilizes the common tool eRulemaking.gov. eRulemaking provides the public with a common, automated repository of Federal Government policy and regulatory-related documentation at the Regulations.gov website. The Federal Acquisition Regulation (FAR) and General Services Administration (GSA) dockets and rule-related materials are all consolidated and centrally managed in a web-based environment, providing the public with one location for accessing public documents, and the opportunity to comment on these documents.

GSA with OMB's Office of Information and Regulatory Affairs (OIRA), operates and maintains the Regulatory Information Service Center (RISC)/OIRA Consolidated Information System (ROCIS). ROCIS serves the 65 cabinet executive, and independent agencies. Agencies use the ROCIS system to submit their regulations to OIRA for review. Agencies use the ROCIS system to submit information collections submitting proposed collections for review and approval by OIRA, under the Paperwork Reduction Act. Agencies use the ROCIS system to submit Systems of Records Notices for OIRA review. RISC also supports an open regulatory process. With OIRA, RISC sponsors http://reginfo.gov, which provides reliable, transparent information about regulations under development.

National Aeronautics and Space Administration

NASA's benefits for the eRulemaking initiative are largely focused on public benefits. One-stop access to NASA and other Federal agency information on rulemakings and non-rulemaking activities is included in the more than 2 million documents posted on Regulations.gov. Direct budget cost savings and cost avoidance result from NASA's transition to FDMS and Regulations.gov, enabling NASA to discontinue efforts to develop, deploy, and operate specific individual online docket and public comment systems. Over a five year period, NASA is estimated to save over $700,000 over alternative options that would provide similar services.

National Archives and Records Administration

In addition to online submission of Federal Register documents, the OFR posts agency submissions to its Electronic Public Inspection Desk on OFR.gov and FederalRegister.gov (Federal Register 2.0). The Public Inspection Desk enables the public and agencies to view manuscript copies of Federal Register documents in PDF form at least one day before final publication in the Federal Register. Customers may also subscribe to email and RSS notifications of Public Inspection documents. These services give the public and commercial entities more time to prepare comments on proposed rules or take steps to comply with new regulatory requirements. Recently, the OFR completely integrated its FederalRegister.gov website with Regulations.gov/ Federal Docket Management System (FDMS). This includes a new Regulations.gov sidebar that provides direct access to agency dockets on FDMS. Rather than begin research from scratch on Regulations.gov, Federal Register 2.0 customers now have direct links to comment forms and supporting documents in FDMS, direct access to public comments displayed on Regulations.gov, a countdown clock of days remaining in comment periods, a running count of comments processed, and links to dockets of completed final actions. The Federal Register 2.0 site also contains direct links to the Unified Agenda to trace the regulatory history of significant rules reviewed under E.O. 12866. The OFR manages its own regulatory actions in theFDMS, and provides extensive guidance and technical resources to the eRulemaking program through its membership on the Advisory and Governing Boards.

National Science Foundation

Support of fundamental science and engineering research requires NSF to maintain constant contact with the research community. Regulations.gov, the eRulemaking online portal, provides the research community (as well as members of the public) with a one-stop web-based, central location to track regulations proposed by NSF and to provide comment when applicable. The Federal Docket Management System (FDMS) allows NSF to manage its regulatory information in a system developed through other agency best-practices and collaboration. NSF typically publishes only one to three proposed regulations per year. During FY12, NSF published one proposed regulation.

Nuclear Regulatory Commission

The eRulemaking Program has simplified the public's participation in the NRC rulemaking process by making regulatory information more accessible on Regulations.gov. Executive Order 13563 calls on agencies to promote public participation and an open exchange of information and perspectives among State, local, and tribal officials, experts in relevant disciplines, affected stakeholders in the private sector, and the public as a whole. Regulations.gov improves NRC public engagement by supporting the notice and public comment process for rulemakings. Using the Federal Docket Management System (FDMS), the NRC has created dockets on Regulations.gov for all documents it has published in the *Federal Register* since December 2007. In FY12, the NRC posted 61 rules and proposed rules, 624 Federal Register notices, and 1030 public submissions in Regulations.gov. The NRC also posts to Regulations.gov stakeholder comments on guidance and other non-rulemaking documents, as well as supplemental background information and supporting documents for significant agency actions.

Office of Personnel Management

Since December 6, 2006, OPM has used Regulations.gov and the Federal Docket Management System (FDMS) as its online regulatory system. In FY12, OPM posted 25 rules and proposed rules and 121 comments on Regulations.gov. Overall, OPM has posted 278 rules and proposed rules, 516 Federal Register notices, and 365 public comments in Regulations.gov. OPM provides public access to 1,203 documents in Regulations.gov.

OPM’s participation in the eRulemaking Program enabled the agency to fulfill the E-Government Act of 2002 requirement to make available a publicly accessible website containing electronic dockets for regulations. In addition, participation in the eRulemaking Program allows OPM to comply with Executive Order 13563 - *Improving Regulation and Regulatory Review* and Executive Order 13609 - *Promoting International Regulatory Cooperation*, the *Open Government Partnership National Action Plan*, and the *Presidential Memorandum - Managing Government Records*.

Small Business Administration

SBA is an active participant in electronic rulemaking. eRulemaking is a collaborative, inter-agency effort whose purpose is to establish a common, automated, and integrated repository for managing Federal rulemaking and non-rulemaking actions that follow a structured notice and comment process. The project consolidates the dockets of various departments and agencies and centrally manages them through a web-based environment offering services such as one-stop access, search capabilities, public comment submission, email notification, bookmarking, and electronic records management. During FY12, SBA created 25 rulemaking dockets through the Federal Docket Management System (FDMS) for inclusion on regulations.gov.

Social Security Administration

SSA is a partner agency in the eRulemaking initiative known as the Federal Docket Management System (FDMS), and publicly accessible at http://www.regulations.gov. SSA began working with EPA and the partner agencies in the development of FDMS in June 2004. Since 2006, we continue to use the FDMS and provide information to the public to increase their understanding of our mission, our programs, and actions we take. In FY12, we posted 13 rules and proposed rules, 22 Federal Register notices, and 106 public submissions. 11 Social Security documents published in the Federal Register can be found by accessing the Federal eRulemaking web portal. All comments we receive from members of the public are available on the Federal eRulemaking portal at http://www.regulations.gov.

The Office of Regulations (OR) is the focal point for the development of SSA's regulations, Social Security Rulings, and Federal Register Notices. OR staff draft regulations and steer documents through the clearance process in SSA, the Office of Management and Budget (OMB), and the Office of the Federal Register. Additionally, OR is responsible for developing and submitting the annual Regulatory Plan and semi-annual Unified Agenda of Federal Regulations to OMB for review and approval, and to the Office of the Federal Register for publication.

U.S. Agency for International Development

USAID partners with EPA on the eRulemaking Program. The Program is a collaborative, inter-agency effort, whose purpose is to establish a common, automated, and integrated repository for managing Federal rulemakings and non-rulemaking actions that follow a structured notice and comment process. The program consolidates the dockets of various departments and agencies and centrally manages them through a web-based environment offering services such as one-stop access, search capabilities, public comment submission, email notification, bookmarking, and electronic records management. The eRulemaking Program is designed to enhance public access and participation in the regulatory process through electronic systems; reduce burden for citizens and businesses in finding relevant regulations and commenting on proposed rulemaking actions; consolidate redundant docket systems; and improve agency regulatory processes and the timeliness of regulatory decisions. eRulemaking has simplified the public's participation in the rulemaking process and has helped make USAID's rulemaking business processes more accessible as well as transparent.

To date, the investment has met the performance targets set for FY12. Release milestones achieved include:

- Regulations.gov Release 3.0: Web site Re-Launch Phase One. Site redesign including home page and search results refresh. New features such as browse categories, agency pages, new display of comments.
- Regulations.gov 3.1: Web site Re-Launch Phase Two. Revised Docket Folder including rulemaking timeline/lifecycle, features incorporated from site-wide search, additional data from Unified Agenda and elsewhere.
- Federal Docket Management System (FDMS) 4.0 Beta: Introducing a new user interface to FDMS, search redesign, and reporting features.
- FDMS.gov 3.6.1: new user requirements
- Regulations.gov 3.2: features Home, Search and Docket folder page updates

G. National Archives Records Administration (NARA) Recordkeeping

The E-Gov Act requires the adoption by agencies of 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. The following section contains descriptions of agency adherence to NARA recordkeeping policies and procedures for electronic information online and other electronic records.

Department of Agriculture

The USDA has well-established processes and procedures to ensure the proper management, scheduling, and disposition of USDA records at http://www.ocio.usda.gov/policy-directives-records-forms/records-management (protected by USDA's eAuthentication Service). The USDA's OCIO Records Management Program continues to lead the department-wide effort to comply with the detailed requirements of NARA Bulletin 2006-002, "NARA Guidance for Implementing Section 207(e) of the E-Government Act of 2002" and the requirements of the Office of Management's (OMB) Circular A-130.

The USDA records management program staff members are in the process of systematically revising the agency's records schedules to ensure that the USDA continues to identify electronic system containing records as part of our Capital Planning and Investment Control process. As a result, 539 major and minor electronic systems have been identified Department-wide at the close of FY12. A total of 294 schedules have been submitted to NARA. Of those submitted schedules, 285 have been approved, and 9 are still pending NARA review. USDA expects to submit the remaining 245 electronic systems to NARA by October 2013.

Department of Commerce

Based on the nature of Commerce's business and ensuring effective program management, the Department has taken an incremental approach to migrating from a paper-based system of records through planning technologies that can make these records less burdensome to manage allowing greater access and use. Commerce's electronic records management strategy supports the President, NARA and OMB's Government-wide effort to reform and improve records management policies and practices within the Department. As our strategy is further implemented, Commerce's bureau will focus on: 1) Creating a bureau-wide records management framework that is more efficient and cost effective; 2) Promoting records management policies that enhance the capability of Commerce to fulfill its statutory mission; 3) Maintaining accountability through documentation of bureau actions; 4) Increasing open Government and appropriate public access to Government records; 5) Supporting bureau compliance with applicable legal requirements related to the preservation of information relevant to litigation; and 6) Transitioning from paper-based records management to electronic records management where feasible.

Commerce will continue to explore ways to improve the Department's records management capability based on programmatic needs and identified systems that require e-records management schedules. Commerce will look to develop practical aspects of complying with the presidential memo and will seek additional support and guidance from the NARA. In addition, Commerce will focus on the following additional tools for both the short and long-term planning: training, accountability and enforcement, and standard operating procedures and directives.

Department of Defense

The DOD continues to improve its capabilities for records management (RM) of electronic records through policy and implementation. The DOD CIO recently revised and is coordinating department-wide policy that addresses the challenges of managing the high volume of electronic records being received or created within the DOD. The revised policy emphasizes that RM requirements be considered during business process design, enterprise architecture, and systems development processes. For unstructured electronic records, the policy calls for the deployment of a RM solution that is compliant with DOD 5015.02-STD, "*Electronic Records Management Software Applications Design Criteria Standard*." In all cases, the policy calls for scheduling of any records, electronic or otherwise.

In anticipation of the policy described above, and in order to realize the efficiencies of electronic management of records, the agencies across DOD continue to adopt and implement RM Applications (RMAs). In response to the Presidential Memorandum, "*Managing Government Records*," November 28, 2011, DOD agencies provided updates on their activities, which include the use of RMAs by the Departments of the Navy, Army, and Air Force, and the anticipated acquisition of an RMA by the Office of the Secretary of Defense.

Moving forward, DOD is designating a Senior Agency Official and is establishing an accompanying governance structure to comply and make progress in record keeping in accordance with the OMB/NARA Memorandum M-12-18, "*Managing Government Records Directive*," August 24, 2012. Through this governance structure, the DOD will continue its progress in improving the management of electronic records.

Department of Education

ED complies with all NARA policies for the management of electronic records, including online records. ED has currently scheduled 82 electronic information systems. It has another 10 records schedules under development, with approximately 15 electronic information systems remaining to be scheduled, including the agency's Internet and intranet websites. The Department has developed mandatory all-employee records management training that includes specific requirements for managing electronic records, including email records. A Department-wide internal evaluation of component records management programs is under way and will assess adherence to the agency's policies and procedures for managing electronic records. ED is currently conducting a pilot of a DOD 5015.2 certified electronic recordkeeping system (HP TRIM) to assess its capabilities for managing all agency electronic records, including email records.

Department of Energy

Energy's Records Management Division ensures the agency adheres to NARA's recordkeeping policies and procedures. An assessment of the DOE O 243.1, Records Management Program analyzed guidance provided to Energy staff. Based on this assessment, a determination was made to revise the Order to enhance proper maintenance of electronic information. The objective was to incorporate current and up to date guidance provided by NARA. One area of focus was technical capability to capture, preserve, access and appropriately dispose of electronic records. Guidance was provided to maintain electronic records by building electronic records keeping functionality into the native electronic information system (EIS) or by capturing the EIS records in an electronic records management application. The Order also identifies records management requirements during the planning, development, or redesign of EIS. Emphasis was given to business processes that support the records management lifecycle; the identification, description, and preservation of record content; and the design and development practices

that incorporate records management requirements, to ensure new systems and systems redesign address legal requirements for managing electronic records. The revised Order was approved and is Energy O 243.1A.

Energy is progressing in the implementation of the Electronic Records Archives system developed and managed by NARA. Records management staff are participating in the required training and identifying specific roles of responsibility. Guidance and information sharing to essential points of contact is being provided by the Headquarters records management office. These efforts allow for a cohesive path forward as objectives are met by Energy.

Department of Health and Human Services

It is HHS policy to use NARA's General Records Schedule (GRS) whenever possible for disposition instructions concerning HHS records. For records that are not covered by NARA's GRS, HHS Operating Divisions follow NARA approved records schedules for their Operating Division.

In 2012 HHS revised its Records Management (RM) policy. The updated policy combined numerous subject specific policies into a single yet concise document. Guidance reflecting the ever changing environment of Information Management was incorporated into the rewritten policy. Working closely with the Information Technology team, the RM office developed and refined the records departure/transfer process for departing personnel by incorporating RM transfer requirements into the IT Products and Services Catalog.

Department of Homeland Security

DHS uses several methods to ensure NARA recordkeeping policies and procedures are adhered to for electronic records. The Chief Information Officer (CIO), along with the Chief Administrative Officer (CAO), is responsible for the seamless capture and storage of electronic records and associated metadata. Additionally, the CIO and CAO coordinate with the Department on any new enterprise systems as well as changes to or decommissioning of current systems to ensure records integrity.

To ensure metadata is captured, DHS outlines metadata forms associated with electronically stored information. DHS policy includes information on storing email records, the use of the enterprise vault along with specific information on what classifies as a permanent or temporary email record or non-record. Furthermore, DHS oversees the departure of employees to ensure email and shared drive records are properly maintained for their retention period.

A working group is in place to oversee any program office plans to transfer electronic records to a records management application. All new systems developed must have a records management plan approved by the working group.

DHS promulgates these policies and procedures through Directives, Instructions, and training. Mandatory training is provided during employee in-processing as well as through DHScovery (the DHS Learning Management System) to Federal and contract staff.

Department of Housing and Urban Development

The Department has record schedules for all electronic information systems under the HUD Records Disposition Schedules and the General Record Schedules as appropriate. The Office of the Chief Human Capital Officer and the Office of the Chief Information Officer are working together to ensure that

information systems, as required by the Privacy Act, have completed a required System of Records Notice (SORN) which includes an approved HUD or General Record Schedule.

Online information copies of records have already been established under an approved HUD or General Record schedule.

On line information published on HUD.Gov, HUD@Work and HUDConnect is covered under approved HUD record schedules and/or the General Record Schedules as appropriate.

Department of the Interior

In response to NARA Bulletin 2006-2 and 2010-2, Interior reported that there are a total of 424 electronic systems as of FY12, of which 341 have been scheduled. DOI submitted 83 electronic systems to NARA for approval, of which 68 were approved and 15 are pending approval. The NARA-approved records schedules and description of the records systems are available at http://www.doi.gov/archive/ocio/egov/index.html. Interior 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 the following four systems: Enterprise Forms System (EFS), Enterprise eArchive System (EES), Enterprise Dashboard System (EDS), and Enterprise Content System (ECS). These systems provide a Department-wide solution to increase cost savings and improve greater efficiencies for managing records in a DOD 5015.2 compliant records management environment.

Department of Justice

In this fiscal year, Justice has continued to follow its ongoing practice of scheduling electronic records that contain federal records. In the most recent report to NARA, Justice reported 914 electronic information systems (EIS) (that contain Federal records), of which 746 have been scheduled (approved for final disposition) by the National Archives and Records Administration (NARA), and 33 schedules have been submitted by Justice and are awaiting approval by NARA. Following is a link to all of Justice's records schedules that are posted on NARA's public website at: http://www.archives.gov/records-mgmt/rcs/schedules/index.html?dir=/departments/department-of-justice/rg-0060. In addition, Justice has an approved records retention schedule for its public facing websites including a separate schedule for social media tools used on those sites.

Department of Labor

Labor has 149 approved record schedules covering the retention and disposition of Labor agency electronic information systems (EIS). In 2011, in accordance with Section 207(e) of the E Government Act of 2002 [44 U.S.C. 3601] and NARA Bulletins 2008 03, Scheduling Existing Electronic Records, and 2006 02, NARA Guidance for Implementing Section 207(e) of the E Government Act of 2002, Labor submitted a total of five record schedules covering EIS. In 2012, two schedules were submitted for previously identified systems. Of the 149 systems, 51 are already scheduled and ten are pending approval with NARA.

We are continuing to work on improved communication channels with the IT programs. One of our upcoming events will be an information exchange session with the records management community, the Office of the Chief Financial Officer and officials from NARA. Among the topics on the agenda we plan to cover is the importance of records management and its relationship to IT. Other topics we plan on

including are as follows: the importance of scheduling an EIS; information about NARA's Semi-Annual EIS Survey; and information required for the SF 115 for an EIS in an Electronic Records Archive (ERA).

Department of State

State has fulfilled the IT scheduling requirements of NARA Bulletin 2006-02. State developed and implemented a NARA approved comprehensive plan to schedule all unscheduled program systems in accordance with NARA Bulletin 2006-02. State submitted records schedules to NARA for four IT systems in FY12.

Department of Transportation

In FY11, DOT launched a multi-year initiative to modernize its records management (RM) program. This initiative, which continues through FY15, seeks to implement an overarching approach to records management that ensures agency records are properly managed from creation to final disposition and, in doing so, allows DOT to effectively and efficiently accomplish its mission, support its business goals, protect the rights and interests of citizens, and identify, preserve, and transfer its permanently valuable records to NARA. The modernization effort is being led by DOT's Chief Information Officer (CIO) and Senior Agency Official for Records Management, in consultation with focus area stakeholders, including Information Technology (IT) staff, Operating Administration (OA) RM Officers (RMOs), the DOT Office of General Counsel, and functional business owners.

The governance of the DOT RM program reflects the federated nature of DOT and utilizes a tiered model to ensure the program efforts are coordinated across the Department, while providing flexibility at the OA level based on each OA's individual statutory mission requirements. The Departmental Records Management Office (DRMO) within the Office of the Chief Information Officer (OCIO) identifies the vision and strategic direction of the program. The actual execution of the program is conducted at the OA level with each OA having its own RMO.

Department of the Treasury

Treasury will continue to schedule newly identified electronic systems on an ongoing basis as part of the bureau assessment plans. Upon identification, Treasury evaluates and schedules these systems at the bureau-level. Treasury developed an Electronic Records Retention schedule and consolidated disparate electronic systems lists into a centralized spreadsheet utilized for tracking. Treasury has provided public access to the information that identifies the disposition authorities for the 1,265 electronic systems.

Treasury Department's Records Schedules: http://www.archives.gov/records-mgmt/rcs/schedules/index.html?dir=/departments/department-of-the-treasury

Department of Veterans Affairs

The VA's Records Management Service is the principle means of providing a structured review of all records management programs and operations. Its goal is to directly enable continuous improvement in VA records management activities through ongoing evaluation and measurement of program work efficiency, and to develop recommendations and projects to increase productivity, reduce errors and optimize VA resources in the delivery of service.

VA has completed the following in support of the NARA electronic recordkeeping:

- Designated a Senior Agency Official (SAO) for Records Management
- Developed and disseminated an Electronic Records Archive (ERA)/Electronic Records Management (ERM) fact sheet Department-wide
- Identified ERA User Roles for each VA administration and staff offices
- VA Enterprise Records Service has completed ERA User Training supporting the new NARA Transfer Requirements
- Established a Records Management Steering Committee to facilitate cooperation on records management issues Department-wide
- Developed an awareness plan for disseminating records management updates and information to Records Officers and Records Liaison Officers Department-wide

The following effort is currently in progress:

- Currently developing a comprehensive implementation plan to achieve goals and objectives outlined in the NARA/OMB Managing Government Records Directive

Environmental Protection Agency

During FY2012, EPA has submitted to and received records schedule approval from NARA for one major electronic system, the Program Tracking, Advisories, Water Quality Standards, and Nutrients (PRAWN) system. Records schedules for two electronic systems, the Underground Injection Control (UIC) National Database (UIC DB) and the Superfund Enterprise Management System (SEMS) are currently in the development and approval phases within EPA, and should be submitted to NARA in FY2013. Eleven minor electronic systems, primarily managed by EPA's regional offices, were scheduled as part of previously approved consolidation of schedules for electronic systems. There are currently 23 transfers of electronic systems to NARA in process, with one approved in August 2012.

General Services Administration

GSA has been actively improving our records program to ensure compliance with all records keeping regulations and other requirements, especially those involving electronic records. In FY12, GSA contracted with NARA to help our agency develop a new records management policy that specifically addresses cloud-based systems, social media and other electronic records keeping challenges. GSA also did a thorough inventory of our electronic data systems in FY12 and is working with NARA to schedule them. The capital planning process is working to include requirements of OMB Circular A-130 to ensure GSA offices incorporate records keeping requirements when implementing electronic data systems. Also in FY12, GSA piloted an electronic records keeping system in our Office of General Counsel and has a working group to discuss how to implement better electronic document management agency-wide. GSA is also actively developing several new records management training courses specifically for senior leadership, program managers, records officers and all GSA employees.

National Aeronautics and Space Administration

NASA follows Agency policy and procedures for the management of federal records, independent of the media or format of the records. A NASA inventory of its electronic information systems identifies whether they contain Federal records, and whether there are proper approved retention schedules that govern the disposition of the records. Of the 2,187 information systems identified in 54 subject categories, 1,330 contain records. NASA continues to create and submit to NARA retention schedules

for newly identified records determined to be unscheduled. Most new schedules have been approved with records in 1,236 of NASA's systems now covered by appropriate retention schedules.

NASA now has NARA approved schedules for 96.3% of the categories of systems. NASA continues work on developing proposed schedules for the remaining 3.7% of the subject categories of systems containing 94 systems or applications whose records require schedules. NASA partners with NARA as it studies uses of, and works toward developing guidance, policies, and schedules for social media and resultant e-records. Further, NASA is developing new guidelines and procedures that increase instructions for e-records and better integrates management of electronic records into IT governance. These will be incorporated into revisions of new policy documents during the coming 18 months.

National Archives and Records Administration

In FY 2012, NARA's Corporate Records Management (CRM) staff implemented a major initiative to position NARA at the forefront of agency records management programs. CRM developed a Plan to Create a Model Program for NARA's Corporate Records. The Director briefed the Management Team on the plan and reported progress using a Milestone matrix. The CRM staff met with all NARA Executives and identified Information Management Officer (IMO) and Records Custodian (RC) positions to cover recordkeeping responsibilities in all major NARA business functions.

As part of the Plan, CRM's completed milestones included: benchmarking and reporting on the recordkeeping situation in each office; kicking off the network of IMOs and RCs (RIM Network); developed a new RM Policy Directive; trained the IMOs and RCs on "Identifying NARA's Records" and "Using NARA's Records Schedule"; as part of this training RCs drafted disposition plans to use in planning the disposition of NARA's legacy records.

In addition to implementing the model program plan, CRM ensures that records management requirements are included where appropriate in policies and in systems development. Examples include: procuring recordkeeping functions for NARA's new cloud email system, coordinating NARA's input to the Presidential memorandum on Improving Records Management, managing NARA's vital records program and participating in NARA's Continuity of Operations (COOP) exercise; participating as a pilot agency on the CRO's Email Management 2.0 Pilot; participating on multiple technical working groups; providing recordkeeping guidance to support new mailbox size limitations.

In FY13, CRM will continue implementing the model program and recordkeeping in NARA's new cloud email system.

National Science Foundation

NSF recognizes the importance of managing all of its records. The agency continuously reviews NARA-approved records schedules to ensure they correctly represent the organization's current business practices. NSF's largest permanent record group is the Grant/Proposal Awards group. That records schedule was updated to reflect the agency's move from paper-based to an electronic format. We are using the Electronic Records Archives (ERA) to transfer eligible permanent electronic records from that group to NARA for archival. The NSF records office is working together with the information technology office during the electronic records transfer process. These groups' collaborative efforts ensure that records and archival management functions are incorporated into the design of new electronic systems and are compliant with NARA guidelines.

NSF has implemented an Electronic Records Management System (ERMS), Documentum. The agency is working to bring all legacy paper records and electronic records into the Documentum system. The

organization is analyzing every opportunity to transition its business practices from paper-based record keeping to electronic records management. These opportunities continue to present themselves as legacy systems are replaced and the life-cycles of their record outputs are evaluated and brought into alignment with current organizational goals and practices. NSF also recognizes the importance of records management training for all agency staff. The agency is enhancing training programs to make sure all employees are aware of their responsibility to identify and protect agency official records.

Nuclear Regulatory Commission

Budgetary constraints and refocused priorities have challenged the ability of the NRC's records management program to remain as a model for records excellence. In 2010, NARA's Records Management Self-Assessment Report ranked the NRC as being at moderate risk of noncompliance. In response, the NRC Records Officer conducted a study whose findings provided the roadmap for the future of the agency's records management program. Plans were developed and are scheduled for implementation over the next five years to include: 1) Revising records policy and governance; 2) Developing and using records and information tools/methodologies; 3) Training; 4) Embedding records controls in business processes; 5) Designing and implementing a records management application; and 6) Addressing NRC's records management top priority of updating records retention schedules based on lines of business. In 2012, the NRC completed records management activities in support of E-Government to include the development of an agency wide Digitization Plan and an Enterprise Content Management Plan. The NRC has also completed a design for the first implementation of the records management applications to ensure proper file retention and disposition, and categorization of agency records consistent with NRC lines of business. Also, in response to NARA's biannual call for scheduling electronic records, the NRC reported 95 out of 108 electronic systems have NARA-approved retention schedules. The NRC has submitted proposed retention schedules to NARA for the remaining 13, which are currently pending their approval.

Office of Personnel Management

OPM's Record Management Program has an online recordkeeping guide of policies and procedures for electronic information and other electronic records for all of OPM located at http://www.opm.gov/RecordsManagement/policies/index.asp. OPM has also issued a new employee course outlining OPM's policy and procedures to ensure records are in compliance with Federal laws and regulations that establish principles, responsibilities, best practices, and requirements for managing such records. OPM has updated the System Development lifecycle to include Records Management in all nine phases of the OPM SDLC. The SDLC includes a checklist that provides three to five basic questions about records management and recordkeeping for each phase of the SDLC process. OPM has drafted an update to the existing Records Management Directive. This directive contains guidelines for the creation, organization, maintenance, and disposition of OPM records. It implements the requirements of Title 36 Code of Federal Regulations, Subchapter B, Records Management, along with providing information on flexible schedules, "big bucket" schedules, and flexible retention periods.

Office of the Director of National Intelligence

ODNI, as a relatively new agency, is closely following NARA guidance for identifying, describing, scheduling, and archiving electronic records, which are the majority of the agency's records.

- ODNI keeps a running inventory of all electronic records systems and series which is updated semi-annually.

- Electronic records and systems are all accounted for in draft, submitted, and NARA-approved records control schedules governing their ultimate disposition.
- Records control schedules are media neutral, flexible schedules that follow NARA guidance to prepare for future adoption of electronic records management systems.
- Records control schedules anticipate the maintenance of electronic records for continued readability and eventual transfer of permanent records to NARA in useable formats far into the future by specifically requiring updating and migration.
- ODNI email is preserved in a NARA-approved system and the permanent email of senior officials is specifically identified and archived.
- The ODNI's IC-CIO is leading the initiative to move Intelligence Community information to a cloud environment through the establishment of the Intelligence Community Information Technology Environment (IC-ITE), which is in direct compliance with the President's Memorandum on Managing Records and NARA/OMB follow-on guidance. This move will support enhance information sharing and collaboration. Further, IC-ITE is being developed to adhere with NARA Bulletin 2010, Guidance on Managing Records in Cloud Computing Environments.

Small Business Administration

Presently, SBA has 27 approved electronic systems—one of which comprises 33 subsystems. This system is scheduled under job number NI-309-05-23. During the last fiscal year, one electronic schedule has been submitted to the National Archives and Records Administration (NARA) for approval. One paper-based schedule has been submitted to SBA's appraisal archivist for preliminary approval. Two electronic schedules are being prepared for submission to NARA.

Social Security Administration

SSA schedules records under agency-specific or the General Records Schedules (GRS). The National Archives and Records Administration (NARA) maintains public access to the GRS at http://www.archives.gov/records-mgmt/grs/. NARA maintains public access to SSA-specific schedules at http://www.archives.gov/records-mgmt/rcs/schedules/index.html?dir=/independent-agencies/rg-0047.

In FY12, all required records schedules met the requirements outlined in NARA Bulletin 2010-02 (http://www.archives.gov/records-mgmt/bulletins/2010/2010-02.html). We obtained NARA's approval and fully implemented all five of the submitted schedules (Enumeration System, Earnings Recording and Self-Employment Income System, Master Beneficiary Record, Supplemental Security Income System, and Social Security Administration Internet Websites).

U.S. Agency for International Development

USAID Automated Directives System's (ADS) Chapter 502 outlines the agency's adherence to federal recordkeeping policies, including NARA (ADS Section 502.1). Under the ADS policy, the agency is directed to identify records that need to be created and maintained to conduct USAID business (and);

- Create and preserve records that document the organization, functions, programs, policies, decisions, procedures, and essential transactions of USAID. This includes records necessary to protect the legal and financial rights of the Government and of persons directly affected by USAID's activities;
- Manage records according to NARA-approved records schedules that determine where and how long records need to be maintained, and transfer permanent records to NARA; and

- Address the creation, maintenance, use, and disposition of records, including databases, e-mail, web records, digital audiovisual materials, and records created from new and emerging technologies.

H. Freedom of Information Act (FOIA)

The E-Gov Act requires agency websites to include direct links to information made available to the public under the Freedom of Information Act. The following section contains agency URLs for their primary FOIA website.

Department of Agriculture

FOIA information can be found at http://www.dm.usda.gov/foia/.

Department of Commerce

FOIA information can be found at http://www.osec.doc.gov/omo/foia/foiawebsite.htm.

Department of Defense

FOIA information can be found at http://www.dod.mil/pubs/foi/dfoipo/.

Department of Education

FOIA information can be found at http://www.ed.gov/policy/gen/leg/foia/foiatoc.html.

Department of Energy

FOIA information can be found at http://energy.gov/management/office-management/operational-management/freedom-information-act.

Department of Health and Human Services

FOIA information can be found at http://www.hhs.gov/foia/.

Department of Homeland Security

FOIA information can be found at http://www.dhs.gov/freedom-information-act-and-privacy-act.

Department of Housing and Urban Development

FOIA information can be found at http://portal.hud.gov/hudportal/HUD?src=/program_offices/administration/foia.

Department of the Interior

FOIA information can be found at http://www.doi.gov/foia/index.cfm.

Department of Justice

FOIA information can be found at http://www.justice.gov/oip/.

Department of Labor

FOIA information can be found at:

- http://www.dol.gov/dol/foia/
- http://www.dol.gov/dol/foia/guide6.htm
- http://www.dol.gov/dol/foia/readroom.htm.

Department of State

FOIA information can be found at http://www.state.gov/m/a/ips.

Department of Transportation

FOIA information can be found at http://www.dot.gov/foia.

Department of the Treasury

FOIA information can be found at http://www.treasury.gov/foia/Pages/index.aspx.

Department of Veterans Affairs

FOIA information can be found at http://www.foia.va.gov.

Environmental Protection Agency

FOIA information can be found at www.epa.gov/foia.

General Services Administration

FOIA information can be found at http://www.gsa.gov/portal/content/105305.

National Aeronautics and Space Administration

FOIA information can be found at http://www.hq.nasa.gov/office/pao/FOIA/agency/.

National Archives and Records Administration

FOIA information can be found at:

- http://www.archives.gov/foia/
- https://foiaonline.regulations.gov/foia/action/public/home).

National Science Foundation

FOIA information can be found at http://www.nsf.gov/policies/foia.jsp.

Nuclear Regulatory Commission

FOIA information can be found at http://www.nrc.gov/reading-rm/foia/foia-privacy.html.

Office of Personnel Management

FOIA information can be found at http://www.opm.gov/efoia/.

Office of the Director of National Intelligence

FOIA information can be found at http://dni.gov/index.php/about-this-site/foia.

Small Business Administration

FOIA information can be found at http://www.sba.gov/about-sba-services/foia.

Social Security Administration

FOIA information can be found at http://www.socialsecurity.gov/foia/index.htm.

U.S. Agency for International Development

FOIA information can be found at http://www.usaid.gov/foia-requests.

I. Privacy Policy and Privacy Impact Assessments

The E-Gov Act seeks to ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government. Additionally, the E-Gov Act requires agencies to conduct a privacy impact assessment; ensure the review of the privacy impact assessment by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and if practicable, after completion of the review under clause, make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means. The following section contains the URL(s) for agency privacy policies and the website where your agency's privacy impact assessments are available.

Department of Agriculture

Privacy information can be found at:

- http://www.usda.gov/wps/portal/usda/usdahome?navtype=FT&navid=PRIVACY_POLICY.
- http://www.usda.gov/wps/portal/usda/usdahome?navid=PRIVACY_POLICY_ES.

Department of Commerce

Privacy information can be found at:

- http://ocio.os.doc.gov/ITPolicyandPrograms/IT_Privacy/DEV01_002682
- http://ocio.os.doc.gov/ITPolicyandPrograms/IT_Privacy/dev01_003746.

Department of Defense

Privacy information can be found at:

- http://dpclo.defense.gov/privacy/About_The_Office/policy_guidance.html
- http://dodcio.defense.gov/Home/Issuances/DoDCIOPrivacyImpactAssessmentsPIAs.aspx.

Department of Education

Privacy information can be found at:

- http://www.ed.gov/notices/privacy/index.html
- http://www.ed.gov/notices/pia/index.html.

Department of Energy

Privacy information can be found at:

- https://www.directives.doe.gov/directives/0206.1-BOrder/at_download/file
- http://energy.gov/cio/office-chief-information-officer/services/guidance/privacy/impact-assessments.

Department of Health and Human Services

Privacy information can be found at:

- http://www.hhs.gov/Privacy.html
- http://www.hhs.gov/ocio/policy/hhs-ocio-2011-0003.html
- http://www.hhs.gov/pia/.

Department of Homeland Security

Privacy information can be found at:

- http://www.dhs.gov/privacy-policy
- http://www.dhs.gov/privacy-office-privacy-impact-assessments-pia.

Department of Housing and Urban Development

Privacy information can be found at:

- http://portal.hud.gov/hudportal/HUD?src=/program_offices/cio/privacy
- http://portal.hud.gov/hudportal/HUD?src=/program_offices/cio/privacy/pia/piachrt.

Department of the Interior

Privacy information can be found at:

- http://www.doi.gov/privacy.cfm
- http://www.doi.gov/ocio/information_assurance/privacy/ppia.cfm.

Department of Justice

Privacy information can be found at:

- http://www.justice.gov/privacy-file.htm
- http://www.justice.gov/opcl/pia.htm.

Department of Labor

Privacy information can be found at:

- http://www.dol.gov/dol/privacynotice.htm
- http://www.dol.gov/oasam/ocio/programs/pia/mainpia.htm.

Department of State

Privacy information can be found at:

- http://www.state.gov/misc/415.htm
- http://www.state.gov/m/a/ips/c24223.htm.

Department of Transportation

Privacy information can be found at:

- http://www.dot.gov/citizens/privacy/privacy-policy
- http://www.dot.gov/individuals/privacy/privacy-impact-assessments.

Department of the Treasury

Privacy information can be found at:

- http://www.treasury.gov/SitePolicies/Pages/privacy.aspx
- http://www.treasury.gov/about/organizational-structure/offices/Mgt/Pages/pia_bureaus.aspx
- http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Privacy,-Transparency-and-Records.aspx
- http://www.treasury.gov/about/role-of-treasury/orders-directives/Pages/to102-25.aspx.

Department of Veterans Affairs

Privacy information can be found at:

- http://www.va.gov/privacy/
- http://www.privacy.va.gov/privacy_impact_assessment.asp
- http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=404&FType=2
- http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=414&FType=2.

Environmental Protection Agency

Privacy information can be found at:

- http://www.epa.gov/privacy/policy/2151/index.htm
- http://www.epa.gov/privacy/assess/index.htm.

General Services Administration

Privacy information can be found at:

- http://www.gsa.gov/portal/content/116609
- http://www.gsa.gov/portal/content/102237

- http://www.gpo.gov/fdsys/pkg/FR-2009-12-15/pdf/E9-29122.pdf
- http://www.gsa.gov/portal/content/104246
- http://www.gsa.gov/graphics/staffoffices/1878_2B_GSA_PIA_Policy.docx.

National Aeronautics and Space Administration

Privacy information can be found at:

- http://www.nasa.gov/about/highlights/HP_Privacy.html
- http://www.nasa.gov/privacy/PIA.html
- http://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPD&c=1382&s=17H.

National Archives and Records Administration

Privacy information can be found at:

- http://www.archives.gov/global-pages/privacy.html
- http://www.archives.gov/foia/privacy-program/privacy-impact-assessments/.

National Science Foundation

Privacy information can be found at:

- http://www.nsf.gov/policies/privacy.jsp
- http://www.nsf.gov/policies/pia.jsp.

Nuclear Regulatory Commission

Privacy information can be found at:

- http://www.nrc.gov/site-help/privacy.html
- http://www.nrc.gov/site-help/plans/privacy-impcat-asess.html.

Office of Personnel Management

Privacy information can be found at:

- http://www.opm.gov/privacy/web.aspx
- http://www.opm.gov/privacy/pia.aspx.

Office of the Director of National Intelligence

Privacy information can be found at:

- http://www.dni.gov/index.php/about-this-site/privacy-policy
- The ODNI does not publish PIAs for national security systems.

Small Business Administration

Privacy information can be found at:

- http://www.sba.gov/about-sba-info/privacy-policy
- http://www.sba.gov/about-sba-services/7473/13815.

Social Security Administration

Privacy information can be found at:

- http://www.socialsecurity.gov/gix/privacyinfo.html
- http://www.socialsecurity.gov/privacy.html
- http://www.socialsecurity.gov/foia/html/pia.htm
- http://www.socialsecurity.gov/OP_Home/cfr20/401/401-0000.htm.

U.S. Agency for International Development

Privacy information can be found at:

- http://transition.usaid.gov/policy/ads/500/508.pdf
- http://transition.usaid.gov/policy/egov/pia.html.

J. Information Resources Management Strategic Plan

The E-Gov Act requires that agency websites include direct links to the strategic plan of the agency developed under Section 306 of Title 5, United States Code. The following section contains the URL to agency Information Resources Management Strategic Plans.

Department of Agriculture

In August 2012, the USDA Chief Information Officer convened a team to develop an Interim USDA IT Strategic Plan (FY 2013-2014) to communicate immediate priorities, to provide continuity, and to lay a foundation for a long-term IT Strategic Plan. The development team has since expanded the scope of the plan to a 3-year, long-term strategic plan that aligns with the expiration date of the Department Strategic Plan in 2015. OCIO has developed the first draft of the Department's IT Strategic Plan (2013 – 2015) and it is anticipated to be vetted, approved and published by the end of March 2013.

Department of Commerce

The IRM Strategic Plan can be found at
http://ocio.os.doc.gov/s/groups/public/@doc/@os/@ocio/@osds/documents/content/prod01_009501.pdf

Department of Defense

The IRM Strategic Plan can be found at
http://dodcio.defense.gov/Portals/0/Documents/Campaign%20Plan%20Summary.pdf.

Department of Education

The IRM Strategic Plan can be found at
http://www.ed.gov/about/reports/annual/ocio/irmstratplan2012.pdf.

Department of Energy

The IRM Strategic Plan can be found at
http://energy.gov/sites/prod/files/2011_DOE_Strategic_Plan_.pdf.

Department of Health and Human Services

The IRM Strategic Plan can be found at http://www.hhs.gov/ocio/ea/documents/hhs_irm_strategic_plan_2007_2012.pdf.

Department of Homeland Security

No publicly-available DHS Information Resources Management Strategic Plan exists. A currently available, internal DHS Enterprise Data Management document does exist and meets the intent of OMB Memorandum 06-02. DHS is continuing to work with our external-publishing organization, the DHS Office of Public Affairs (OPA), to publically post said document.

Department of Housing and Urban Development

The IRM Strategic Plan can be found at http://www.hud.gov/offices/cio/documents/itstratplan3.pdf. HUD has developed a draft IT Strategic Plan FY 2012-2017, which articulates the IT goals and objectives. The new IT plan will be aligned with the HUD's new strategic goals.

Department of the Interior

The IRM Strategic Plan can be found at http://www.doi.gov/ocio/index.cfm.

Department of Justice

The IRM Strategic Plan can be found at http://www.justice.gov/jmd/ocio/it-strategic-plan.htm.

Department of Labor

The IRM Strategic Plan can be found at http://www.dol.gov/oasam/ocio/programs/ITStrategicPlan2006/IT-Strategic-Plan.htm. Labor is actively in the process of developing an updated IT Strategic Plan, which is expected to be completed and made available on DOL.gov by the end of the third quarter 2013.

Department of State

The IRM Strategic Plan can be found at http://www.state.gov/m/irm/rls/c39428.htm.

Department of Transportation

The IRM Strategic Plan can be found at http://www.dot.gov/cio/docs/IRM_StrategicPlanFY07-2012.pdf.

Department of the Treasury

The IRM Strategic Plan can be found at http://www.treasury.gov/about/organizational-structure/offices/Mgt/Documents/ITMB_Volume_2_IT_Strategic_Plan_v1%2002.pdf. An updated IRM plan is forthcoming a result of Treasury's IT Enterprise Roadmap. This plan will be reviewed for redaction, cleared for public release, and should be publicly available in January 2013.

Department of Veterans Affairs

The IRM Strategic Plan can be found at http://www.oit.va.gov/docs/OIT_CIO_Annual_Report_FY_2011_Final.pdf.

Environmental Protection Agency

The IRM Strategic Plan can be found at http://epa.gov/oei/policies.htm.

General Services Administration

The IRM Strategic Plan can be found at http://www.gsa.gov/graphics/staffoffices/itstrategicplan2012.pdf.

National Aeronautics and Space Administration

The IRM Strategic Plan can be found at:

- http://www.nasa.gov/offices/ocio/IRM_Plan.html
- http://www.nasa.gov/offices/ocio/Tactical_Plan.html.

National Archives and Records Administration

The IRM Strategic Plan can be found at http://www.archives.gov/about/plans-reports/info-resources/.

National Science Foundation

The IRM Strategic Plan can be found at http://www.nsf.gov/oirm/dis/.

Nuclear Regulatory Commission

The IRM Strategic Plan can be found at http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1908/.

Office of Personnel Management

The IRM Strategic Plan can be found at http://www.opm.gov/strategicplan/pdf/information-resource-management-plan-2010-2013.pdf.

Office of the Director of National Intelligence

Not Applicable.

Small Business Administration

The IRM Strategic Plan can be found at http://www.sba.gov/sites/default/files/SBA_IT_Strategic_Plan_2012-2016.pdf.

Social Security Administration

The IRM Strategic Plan can be found at http://www.socialsecurity.gov/irm/index.htm.

U.S. Agency for International Development

The IRM Strategic Plan can be found at http://transition.usaid.gov/policy/coordination/USAIDITStrategicPlan2011-2015.pdf.

K. Public Access to Electronic Information

The E-Gov Act requires that agency websites assist public users to navigate agency websites, including the speed of retrieval of search results and the relevance of the results. The following section provides the URL(s) that contain agency customer service goals and 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 uses innovative technologies to improve customer service at lower costs.

Department of Agriculture

Information on public access to electronic information can be found at:

- http://www.usda.gov/documents/usda-customer-service-plan-nov2011.pdf
- http://www.usda.gov/wps/portal/usda/usdahome?navid=ASK_EXPERT2.

Department of Commerce

Information on public access to electronic information can be found at:

- http://open.commerce.gov/
- http://open.commerce.gov/news/2011/10/24/department-commerce-customer-service-plan.

Department of Defense

Information on public access to electronic information can be found at http://www.defense.gov/.

Department of Education

Information on public access to electronic information can be found at:

- http://www.ed.gov/open/
- http://www2.ed.gov/about/customer-service-plan.pdf
- http://www.ed.gov/digitalstrategy/.

Department of Energy

Information on public access to electronic information can be found at:

- http://energy.gov/downloads/department-energy-customer-service-plan
- http://www.energy.gov/about/budget.htm
- http://www.goals.performance.gov/agency/doe
- http://www.cfo.doe.gov/strategicplan/strategicplan.htm
- http://www.energy.gov/about/budget.htm.

Department of Health and Human Services

Information on public access to electronic information can be found at http://www.hhs.gov/open/execorders/customerservice.html.

Department of Homeland Security

Information on public access to electronic information can be found at:

- http://www.dhs.gov/dhs-information-quality-standards
- http://www.dhs.gov/how-do-i/by-type
- http://www.dhs.gov/main-contact-us.

Department of Housing and Urban Development

Information on public access to electronic information can be found at:

- http://portal.hud.gov/hudportal/HUD?src=/Digital_Strategy/report
- http://portal.hud.gov/hudportal/documents/huddoc?id=CustServPlan11292011.pdf
- http://www.usa.gov/webreform/agency-plans/hud.pdf
- http://portal.hud.gov/hudportal/HUD?src=/library/bookshelf11.

Department of the Interior

Information on public access to electronic information can be found at:

- http://www.doi.gov/open/index.cfm
- http://www.doi.gov/open/upload/Customer-Service-Plan-DOI-10-23-2011.pdf
- http://www.doi.gov/digitalstrategy/index.cfm
- http://www.doi.gov/notices_soc.cfm
- http://www.doi.gov/archive/ocio/egov/products.html.

Department of Justice

Information on public access to electronic information can be found at http://www.justice.gov/open/.

Department of Labor

Information on public access to electronic information can be found at:

- http://www.dol.gov/open/customer-service-plan.htm
- http://www.dol.gov/open/
- http://www.dol.gov/open/ourplans.htm
- http://www.dol.gov/dol/aboutdol/content.htm
- http://www.dol.gov/dol/foia/readroom.htm.

Department of State

Information on public access to electronic information can be found at:

- http://www.state.gov/digitalstrategy
- www.state.gov/documents/organization/176165.pdf.

Department of Transportation

Information on public access to electronic information can be found at:

- http://www.dot.gov/mission/open/dot-customer-service-plan
- http://www.usa.gov/webreform/agency-plans/dot.pdf.

Department of the Treasury

Information on public access to electronic information can be found at:

- http://www.treasury.gov/about/budget-performance/Pages/default.aspx
- http://www.treasury.gov/about/budget-performance/strategic-plan/Pages/index.aspx
- http://www.treasury.gov/open/Documents/Treasury%20Customer%20Service%20Plan%20FINAL.pdf.

Department of Veterans Affairs

Information on public access to electronic information can be found at:

- http://www.va.gov/OPEN/docs/Customer_Service_Plan_VA_Oct242011.pdf
- http://www.va.gov/bluebutton/
- http://www.va.gov/BLUEBUTTON/Resources.asp.

Environmental Protection Agency

Information on public access to electronic information can be found at:

- http://www.epa.gov/open/EPACustomerServicePlan2011.pdf
- http://www.epa.gov/open/
- http://www.epa.gov/digitalstrategy/.

General Services Administration

Information on public access to electronic information can be found at http://gsa.gov/portal/category/26751.

National Aeronautics and Space Administration

Information on public access to electronic information can be found at:

- http://www.nasa.gov/open/index.html
- http://www.nasa.gov
- http://www.nasa.gov/about/contact/information_inventories_schedules.html
- http://science.nasa.gov/
- http://www.nasa.gov/pdf/598263main_NASA%20Customer%20Service%20Plan.pdf.

National Archives and Records Administration

Information on public access to electronic information can be found at:

- http://www.archives.gov/about/customer-service/
- http://www.archives.gov/digitalstrategy/
- http://www.archives.gov/open/
- http://www.archives.gov/developers/.

National Science Foundation

Information on public access to electronic information can be found at:

- http://www.nsf.gov/news/strategicplan/nsfstrategicplan_2011_2016.pdf
- http://nsf.gov/open/
- http://www.nsf.gov/digitalstrategy/.

Nuclear Regulatory Commission

Information on public access to electronic information can be found at:

- http://www.nrc.gov/public-involve/open/customer-service.html
- http://www.nrc.gov/public-involve/open/customer-service/nrc-customer-service-plan.pdf
- http://www.nrc.gov/public-involve/open/cio-council-reform-initiative.html
- http://www.nrc.gov/public-involve/open/cio-council-reform-initiative/initial-web-improvement-plan.pdf
- http://www.nrc.gov/about-nrc/plans/data-center-consolidation-plan.pdf
- http://www.nrc.gov/public-involve/open/digital-government.html
- http://www.nrc.gov/public-involve/open.html
- http://www.nrc.gov/public-involve/open/philosophy.html#plan.

Office of Personnel Management

Information on public access to electronic information can be found at:

- http://www.opm.gov/publications/2012-customer-service-plan.pdf
- http://www.fedscope.opm.gov/.

Office of the Director of National Intelligence

Information on public access to electronic information can be found at www.odni.gov.

Small Business Administration

Information on public access to electronic information can be found at:

- http://www.sba.gov/sites/default/files/SBA%20Customer%20Service%20Plan.pdf
- http://www.sba.gov/sites/default/files/serv_strategic_plan_2010-2016.pdf
- http://www.sba.gov/about-sba-services/199
- http://www.sba.gov/content/sba-open-government-plan-0.

Social Security Administration

Information on public access to electronic information can be found at:

- http://www.socialsecurity.gov/open
- http://www.socialsecurity.gov/open/customerserviceplan/
- http://www.socialsecurity.gov/asp/plan-2013-2016.pdf.

U.S. Agency for International Development

Information on public access to electronic information can be found at http://transition.usaid.gov/open/USAIDCustomerServicePlan2011-10-26.pdf.

L. Research and Development (R&D)

The E-Gov Act calls for the development and integration of a Government-wide repository that fully integrates, to the maximum extent feasible, information about research and development funded by the Federal Government. This section highlights those agencies that participate in research and development (R&D) efforts; URL(s) are listed below that provide publically accessible information related to federally funded R&D activities and/or the results of the Federal research. In FY 2012, Federal agencies expanded the publically available information related to their R&D activities and/or the results of the Federal research, including greater efforts to integrate information across Federal agencies (see science.gov and research.gov and itdashboard.nitrd.gov, below) and increased integration and improved availability of data resulting from Federally funded research on data.gov.

Department of Agriculture

R&D information can be found at:

- http://www.fs.fed.us/research/
- http://www.nal.usda.gov/research-and-technology/research-and-development
- http://cris.nifa.usda.gov/.

Department of Commerce

R&D information can be found at:http://ocio.os.doc.gov/ITPolicyandPrograms/E-Government/PROD01_003924.

Department of Defense

R&D information can be found at:http://comptroller.defense.gov/Budget2013.html.

Department of Education

R&D information can be found at:

- http://ies.ed.gov/
- http://nces.ed.gov.

Department of Energy

R&D information can be found at:

- www.osti.gov
- www.scienceaccelerator.gov/
- www.osti.gov/energycitations
- www.osti.gov/bridge
- www.osti.gov/doepatents
- www.osti.gov/accomplishments
- www.osti.gov/dataexplorer
- www.science.gov.

Department of Health and Human Services

R&D information can be found at:

- http://taggs.hhs.gov/index.cfm
- http://publicaccess.nih.gov/policy.htm
- http://report.nih.gov/index.aspx.

Department of Homeland Security

R&D information can be found at:

- http://www.safecomprogram.gov/default.aspx
- http://www.dhs.gov/directorate-science-and-technology.

Department of the Interior

R&D information can be found at:http://www.doi.gov/archive/ocio/egov/research.html.

Department of Justice

R&D information can be found at:

- www.nij.gov
- www.bja.gov/
- www.ojjdp.gov/
- www.it.ojp.gov
- www.dna.gov
- www.ojp.usdoj.gov
- www.bjs.gov/
- www.ovc.gov/
- www.ncjrs.gov.

Department of Labor

R&D information can be found at:

- http://wdr.doleta.gov/research/
- http://www.osha.gov/dte/sharwood/index.html
- http://www.dol.gov/asp/programs/REIDL/index.htm.

Department of Transportation

R&D information can be found at:

- http://ntlsearch.bts.gov/researchhub/index.do
- http://www.faa.gov/data_research/research
- http://www.fhwa.dot.gov/research
- http://www.fta.dot.gov/about/12351.html
- http://www.marad.dot.gov/environment_safety_landing_page/maritime_safety/rnd_act/rnd_act.htm
- http://www.nhtsa.gov/Driving+Safety/Research+&+Evaluation
- http://www.phmsa.dot.gov/doing-biz/r-and-d_opps.

Department of Veterans Affairs

R&D information can be found at:

- http://www.research.va.gov
- http://www.cider.research.va.gov.

Environmental Protection Agency

R&D information can be found at:

- http://cfpub.epa.gov/si/
- http://ofmpub.epa.gov/sor_internet/registry/systmreg/home/overview/home.do
- http://www.epa.gov/crem/knowbase/index.htm
- http://yosemite.epa.gov/ee/epa/eed.nsf/webpages/homepage
- http://www.epa.gov/osa/fem/methcollectns.htm
- http://www.epa.gov/ncea/iris/index.html
- http://www.epa.gov/ttn/direct.html
- http://epa.gov/otaq/models.htm
- http://www.epa.gov/oswer/cleanup/science.html
- http://www.epa.gov/superfund/remedytech/
- http://water.epa.gov/scitech/
- http://www.epa.gov/research/
- http://www.epa.gov/ncer/
- http://www.epa.gov/gateway/science/.

National Aeronautics and Space Administration

R&D information can be found at:

- http://ntrs.nasa.gov/
- http://www.sti.nasa.gov/ .

National Archives and Records Administration

R&D information can be found at:

- http://www.archives.gov/applied-research/
- http://perpos.gtri.gatech.edu/
- http://isda.ncsa.illinois.edu/drupal/project/census
- http://isda.ncsa.illinois.edu/drupal/project/nara
- http://isda.ncsa.illinois.edu/drupal/software/CSR
- http://isda.ncsa.illinois.edu/drupal/software/polyglot
- http://polyglot.ncsa.illinois.edu/polyglot/convert.php
- http://isda.ncsa.illinois.edu/drupal/software/Versus
- http://isda.ncsa.illinois.edu/drupal/biblio
- http://www.ncsa.illinois.edu/News/Stories/bigdata/
- http://www.ncsa.illinois.edu/News/Stories/ImageMiners/
- http://ci-ber.blogspot.com/p/about-ci-ber.html
- http://bit.ly/H97nJC
- http://www.casc.org/papers/2012Brochure.pdf
- http://quipu.psc.teragrid.org/slash2/.

National Science Foundation

R&D information can be found at:

- http://www.nsf.gov/
- http://www.nsf.gov/recovery/
- http://www.research.gov/
- http://rd-dashboard.nitrd.gov/
- http://itdashboard.nitrd.gov/.

Nuclear Regulatory Commission

R&D information can be found at:

- http://www.nrc.gov
- http://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/index.html
- http://www.nrc.gov/about-nrc/regulatory/research.html.

Office of Personnel Management

Not applicable.

Office of the Director of National Intelligence

R&D information can be found at:

- www.fbo.gov
- www.iarpa.gov.

Small Business Administration

R&D information can be found at:

- http://www.sba.gov/advo/research/
- http://www.sbir.gov/.

Social Security Administration

R&D information can be found at:

- http://www.socialsecurity.gov/policy/rrc/index.html
- http://www.socialsecurity.gov/policy/drc/index.html
- http://www.socialsecurity.gov/retirementpolicy/index.html
- http://www.socialsecurity.gov/policy/index.html
- http://www.socialsecurity.gov/policy/docs/contractreports/index.html
- http://www.socialsecurity.gov/disabilityresearch/index.html.

U.S. Agency for International Development

R&D information can be found at:

- http://transition.usaid.gov/our_work/environment/climate/policies_prog/science.html
- http://www.usaid.gov/climate.

M. Privacy

The E-Gov Act seeks to ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government. Specifically, the E-Gov Act requires agencies to conduct a privacy impact assessment; ensure the review of the privacy impact assessment by the Chief Information Officer, 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 section contains agency descriptions of their adherence to OMB guidance pertaining to the use of IT to collect, maintain, or disseminate identifiable information, or the procurement of systems for this purpose. In addition, agencies have described their process for performing and updating privacy impact assessments for IT systems.

Department of Agriculture

USDA collectively adheres to OMB guidance regarding the collection, maintenance, and dissemination of personally identifiable information. In FY11, USDA embarked on a social security number (SSN)/tax payer identification number (TIN) elimination, encryption, masking effort. Prior to this initiative, USDA

reported masking, eliminating, and encrypting 75 percent of its information systems containing SSN/TIN. In FY12, the Department has increased its information systems compliance to 91 percent.

Privacy documentation to include privacy threshold analysis (PTA), privacy impact assessments (PIA), and other internal privacy checklists are reviewed and updated annually. The USDA Privacy Office completed the latest update to the USDA PTA in August 2012. This update was based on the NIST's draft special publication 800-53 revision 4, and the Appendix J privacy controls. The USDA Privacy Office is currently seeking feedback and answering questions from agency Privacy Officers on the PTA.

Along with the release of the updated PTA, a co-author of the NIST 800-53 guidance presented at the September 2012 USDA Privacy Council meeting. The briefing on 800-53 rev 4 and the privacy controls was attended by a record number of Privacy Officers, Information Security System Program Managers, and System Administrators. The Privacy Council also stood up a subcommittee to review NIST's draft guidance and controls and how to implement them within USDA. The objective of the working group is to provide the agencies with an opportunity to comment on privacy documentation and provide input early in the drafting process.

Department of Commerce

Commerce maintains an active role in protecting the privacy of both persons and businesses. The Privacy Provisions (Section 208) of the E-Government Act of 2002 establish requirements for the maintenance and security of privacy information maintained on agency information technology systems.

The Commerce OCIO provides guidance and resources to help users understand these requirements and how they are implemented in the Department of Commerce IT Privacy Policy. The Department's Chief Privacy Officer is responsible for the development and maintenance of privacy policies, procedures, and guidance essential to safeguarding the collection, access, use, dissemination, and storage of PII and Privacy Act information in accordance with the Privacy Act of 1974, the E-Government Act of 2002, the Federal Information Security Management Act (FISMA), and policy and guidance issued by the President and OMB.

Commerce adherence to OMB guidance pertaining to the use of IT to collect, maintain and disseminate identifiable information, or the procurement of new systems for this purpose can be found at the following URL: http://ocio.os.doc.gov/ITPolicyandPrograms/IT_Privacy/index.htm.

Guidance pertaining to the performance and updating of IT privacy impact assessments be found at the following URL: http://ocio.os.doc.gov/ITPolicyandPrograms/Policy___Standards/DEV01_002682.

Department of Defense

The Defense Privacy and Civil Liberties Office (DPCLO) works with DOD CIO to ensure that DOD meets OMB privacy compliance requirements for completion of, and updates to System of Records Notices (SORNS) and (Privacy Impact Assessment) PIAs. The DPCLO and CIO collaborate on Federal Information Security Management Act quarterly and annual reporting, which includes reviews of SORNS and PIAs compliance across DOD.

The DOD IT PIA program protects the privacy of individuals by systematically ensuring controls are in place to protect data, assessing and minimizing vulnerabilities of DOD information systems containing Personally Identifiable Information (PII).

The PIA Program:

- Establishes PIA policy, DoDI 5400.16 "*DoD Privacy Impact Assessment Guidance*," and procedures to reflect current and new emerging requirements;
- Ensures PIAs are conducted on electronic collections of PII and adequate controls are in place to protect public, Federal employees and contractors' PII;
- Provides continuous outreach, training and education to Components to assist with establishing and maintaining PIA programs that increase the completion rate of PIAs in compliance with the law.

Per OMB and DOD guidance, PIAs are required to be performed, and updated as necessary, where a system change creates new privacy risks including, but not limited to, significant system management changes, new public access, conversion from paper-based records to electronic systems and significant merging. Every three years a PIA must be reevaluated to ensure any changes to the system that could impact privacy are reviewed and updated as part of the Certification and Accreditation process.

Department of Education

The Privacy Safeguards Division (PSD) is responsible for ensuring that the Department adheres to OMB guidance about the use of IT to collect, maintain, or disseminate identifiable information from or about members of the public. When the Department develops or procures such a system or when a PRA collection is initiated, the PSD works with the system owner (SO) to conduct a PIA and post it to ED.gov. If changes to a system create new privacy risks, the PSD will initiate or update a PIA with the SO. ED also meets the requirement of posting privacy policies on its public websites. When a new public website is developed, the PSD works with the project lead to develop and post a privacy policy addressing all elements in OMB directives. Our process for performing and updating PIAs for IT systems is as follows: To determine the necessary privacy documentation, the PSD provides the SO with a Privacy Threshold Analysis (PTA) to complete. If the PTA shows no PII, the process is complete. If a PIA is necessary, the PSD provides the SO with the PIA template, and the SO completes. The PSD then collaborates with the CIO, Office of General Counsel, and Records Management to address any issues. Changes are communicated with the SO, who updates the PIA, collects internal signatures, and returns the final draft to the PSD. Systems with social security numbers require additional approval. The Chief Privacy Officer signs the document, and it is posted to ED.gov.

Department of Energy

Energy has three main documents related to privacy compliance for automated collections of personally identifiable information (PII): Privacy Needs Assessment (PNA), Privacy Impact Assessment (PIA), and Systems of Record Notice (SORN). While each of these documents has a distinct function to ensure adherence with OMB protection guidelines pertaining to automated collections of PII, together these documents further the transparency of Energy activities and convey accountability. DOE O 206.1, "Department of Energy Privacy Program", provides the procedural requirements for each document and establishes roles and responsibilities associated with the completion and updating of these documents. In addition to DOE O 206.1, the Privacy Act SORN requirements are codified at 10 CFR 1008 "Records Maintained on Individuals (Privacy Act)."

The PNA is the first document program elements complete to assess whether an automated system will collect and maintain PII. This threshold assessment determines if additional compliance documentation is required such as a PIA or SORN. The PIA, an important tool Energy uses to examine privacy risks associated with automated collections of PII, is required when IT systems contain PII. The PIA

addresses critical areas such as authority for PII collection, scope of collection, use of PII, information security, Privacy Act SORN applicability, and information sharing. The PIA serves to reinforce early consideration of ways to enhance PII protection by including privacy in early stages of system development. If the PIA analysis concludes a SORN is required, a SORN is prepared and published in the Federal Register.

Additional information regarding these processes:

- http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&rgn=div5&view=text&node=10%3A4.0.3.5.6&idno=10
- http://energy.gov/cio/downloads/privacy-impact-assessment-template-and-guidance

Department of Health and Human Services

The HHS Office of the CIO established the *HHS-OCIO Policy for Information Systems Security and Privacy* (henceforth "the Policy") to provide direction to the information technology (IT) security programs of Operating Divisions and Staff Divisions for the security and privacy of HHS data in accordance with the Federal Information Security Management Act of 2002.

The Policy is a reissuance, establishing comprehensive IT security and privacy requirements for the IT security programs and information systems of OPDIVs and STAFFDIVs. A complementary *HHS-OCIO Policy for Information Systems Security and Privacy Handbook* is included as an appendix to the Policy . The Handbook outlines IT security and privacy policy requirements for IT security and privacy programs and information systems in more detail, and is organized according to information assurance (IA) control families to make the document easy to use and scalable for the future.

The HHS Office of the CIO's Office of IT Security also provides direction to the Operating Divisions and Staff Divisions with regard to the conduct of Privacy Impact Assessments. The Privacy Impact Assessment Guide outlines a standard approach for conducting a PIA for all Departmental systems, including developmental, operational, FISMA, contractor-owned, grantee, information technology (IT) general support systems (GSS), major applications (MA), and non-major applications. It also provides detailed instructions which aid in properly populating the PIA.

Department of Homeland Security

The DHS Privacy Office provides extensive guidance on the use of personally identifiable information, including DHS policies on when and how to conduct a Privacy Impact Assessment and System of Records Notice. DHS requires that all new and existing IT systems conduct a Privacy Threshold Analysis (PTA), performed by the program manager and validated by the DHS Privacy Office prior to security authorization. More information can be obtained at www.dhs.gov/privacy under "Privacy Compliance."

Department of Housing and Urban Development

All Privacy Impact Assessments (PIAs) are published for access by the general public per OMB requirements. Prior to drafting a PIA, program offices must contact the Privacy Office to discuss appropriate steps, and to coordinate E-Government Act efforts. The Privacy Office is notified and aware of similar initiatives in other program offices and seeks to reduce redundant work where possible and when in accordance with the Privacy Act. The Program Office then submits the draft PIA document to the Privacy Office which reviews all PIAs and provides feedback to the Program Office. Once the Privacy Office has approved the PIA, the Office of General Counsel (OGC) reviews the PIA. Once OGC

approves the PIA, the Senior Agency Official for Privacy signs all PIAs. Upon approval of the document(s), the Privacy Office publishes the PIA to HUD's website for public access.

All PIA's are published for access by the general public per OMB Requirements. PIA's that may contain sensitive information may be exempt from the publication requirement at the discretion of the HUD Privacy Officer. The results of the PIA will be recorded in the PII Inventory for use later in meeting OMB, or internal HUD, reporting requirements.

Department of the Interior

The Interior Privacy Impact Assessment (PIA) Guide, issued March 1, 2004, includes a PIA template and guidance on conducting PIAs in accordance with the E-Government Act of 2002 and OMB M-03-22. Interior policy requires a completed PIA for all systems that handle personally identifiable information to ensure privacy implications are addressed when planning, developing, implementing, and operating information systems that maintain information on individuals. Interior privacy personnel collaborate with system owners and IT security to assess new or proposed programs, systems or applications for privacy risks, and recommend methods to protect individual privacy. In FY12, Interior developed a new electronic PIA form to facilitate the PIA completion process and improve PIA compliance which includes specific questions designed to assess privacy risks. Interior also implemented an Interior Adapted PIA for agency use of third-party websites and applications in accordance with OMB policy Interior completed a Department-wide PIA inventory in FY12 that included an evaluation of bureau PIAs and conducted reviews with findings for bureau privacy and security personnel to identify and correct deficiencies in the PIA completion process for Interior applications within the Cyber Security Assessment and Management (CSAM) system, Interior's official information system repository.

Department of Justice

Justice's privacy compliance process begins with its 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 in Justice's IT security framework, Justice also reviews information technology systems that contain PII and/or information in identifiable form to determine whether the privacy requirements under the E-Government Act and OMB guidance would apply. If these privacy requirements apply to the IT system, Justice conducts a Privacy Impact Assessment for the system to ensure that system developers and owners have made technological choices that incorporate privacy protections into the underlying architecture of the system. In addition, if the IT system is further modified to impact the privacy of information maintained in the system, a subsequent IPA must be conducted to determine again whether additional privacy requirements and considerations must be applied to the modified system.

Department of Labor

Labor's policy in regards to privacy and security including personally identifiable information can be found at: http://www.dol.gov/dol/privacynotice.htm.

All major information systems are required to complete Labor's annual Privacy Impact Assessment (PIA) process and document the results in Labor's Cyber Security Assessment and Management (CSAM) tool. The Labor PIA process is two-fold and requires all systems to first undergo an initial screening review to determine if the system meets the pre-requisite criteria (e.g. System collects

Personally Identifiable Information for members of the public) requiring the completion of the full PIA questionnaire. If a PIA is not required the process is complete and there is no further action until the anniversary date. If a PIA is required, the PIA questionnaire is completed by agency, and submitted to the Office of the Chief Information Officer (OCIO) for review and approval. Once approved, the PIA questionnaire is signed by the Agency official and maintained in CSAM. Within 30 days of this approval, the PIA is redacted for public consumption and posted on the Labor public website at: http://www.dol.gov/oasam/ocio/programs/pia/mainpia.htm.

Department of State

State's Privacy Office is responsible for ensuring that privacy protections are incorporated into State systems, initiatives, and programs as they are developed and modified. To accomplish this objective, the Office integrates privacy into State business processes by reviewing and approving all privacy compliance documentation including privacy impact assessments (PIAs) and system of records notices (SORNs).

The Office is also responsible for ensuring that State meets the statutory requirements of privacy reporting as stated in the E-Government Act of 2002. To comply with the Federal Information Security Management Act of 2002 (FISMA), the Privacy Office submits quarterly and annual FISMA reports when required by the Office of Management and Budget (OMB). The reports provide an inventory of State information technology (IT) systems that contain federal information in identifiable form, which require a PIA and/or a SORN. For the third quarter, FY12 FISMA Report, State reported a 98 percent compliance rate for PIAs and SORNs FISMA reportable systems. All new and updated PIAs and SORNS are posted on State's public-facing websites at http://www.state.gov/m/a/ips/c24223.htm and http://www.state.gov/m/a/ips/c25533.htm, respectively. Lastly, as part of the annual OMB 300 budget review process, the Privacy Office conducts continual reviews of State IT investments for compliance with privacy requirements.

The Privacy Office's engagement with stakeholders at the early stages of IT system and/or program development assures integration of compliance into State processes. The Privacy Office's strong relationship with stakeholders throughout State demonstrates a mature privacy compliance framework.

Department of Transportation

The DOT Privacy Officer (PO) under the auspices of the Senior Agency Official for Privacy is responsible for establishing policy and standards for the identification, mitigation, and documentation of privacy risk resulting from the acquisition, development, and implementation of IT throughout the Department, and for verifying compliance with the same. All IT systems prior to receiving an Authority to Operate must at a minimum have a documented Privacy Threshold Assessment (PTA) reviewed and adjudicated by the DOT PO, the results of which determine if additional privacy compliance documentation, included but not limited to Privacy Impact Assessments (PIAs). Those systems requiring PIAs must have compliance material review and approved by the DOT PO prior to entering the operational stages. DOT PIA's are aligned with Appendix J – Privacy Controls of NIST SP 800-53v4 Privacy and Security Controls DRAFT.

Once SP 800-53r4 is finalized, the DOT PO in concert with the DOT Chief Information Security Officer (CISO) will establish additional requirements from the privacy control family to be integrated into the Department's continuous monitoring program. All contracts for externally produced tools and/or services are required to contain standard Federal Acquisition Regulation Part 24 Protection of Privacy

and Freedom of Information language. The DOT PO and Office of Procurement are developing standardized contract language.

Department of the Treasury

Treasury has an established commitment to information privacy which is reflected in a number of concrete ways. The aforementioned URLs reflect Treasury's diligence in ensuring that user privacy on Treasury's publicly facing and third-party websites is a paramount concern.

The Office of Privacy and Civil Liberties routinely provides guidance and to Treasury's bureaus regarding the preparation and completion of PIA, and when appropriate to do so, reviews completed assessments to ensure they meet the requirements outlined in Section 208 of the E-Government Act of 2002.

In addition, Treasury just submitted its FY12 Annual FIMSA Report. In the Senior Agency Official for Privacy (SAOP) Section of the report, Treasury had 305 systems which contain personal information in identifiable form and of those 240 are required to have a PIA. As of September 30, 2012, all 240 systems (100 percent) in fact have completed and current PIAs.

Finally, in its on-going effort to enhance its Privacy Program, Treasury has begun an initiative to implement the PIA Management System (PIAMS) which was developed by the IRS. This endeavor represents a significant effort to promote a paperless environment and will provide a stronger capability that will further ensure that all Treasury systems that require PIAs in fact have PIAs.

Department of Veterans Affairs

The OI&T has developed a comprehensive methodology on the use of information technology (IT) to collect, maintain, or disseminate identifiable information or when new systems are procured based on OMB's guide to privacy impact assessments.

The VA's privacy impact assessment (PIA) process is a practical method of evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The assessment provides a framework to ensure vital data stewardship issues are incorporated into all phases of the system development life cycle (SDLC). Through the assessment, VA employees and system owners are able to identify and address potential information privacy infractions and risks.

PIAs form the basis for the privacy reviews as mandated by VA Directive 6502, VA Enterprise Privacy Program, Section 3.d. (7). Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates VA's commitment to protect the privacy of any personal information we collect, store, retrieve, use and share. When a system is being designed or when a major change is being made to a system a PIA is conducted. Once in operation, a full PIA is required every three years. A validation letter, instead of a full PIA, is allowable for the intervening years if no significant changes involving PII have been made.

The VA classifies their systems based upon NIST Federal Information Processing Standards (FIPS) 199. During this classification process, they will determine if a system is a general support system (GSS), local area network (LAN), major application, or minor application. The different types of classifications require different versions of the PIA form to be submitted. The PIA reviewer must be trained in differentiating the different types of requirements, providing quality, accurate information in the assessments, and communicating the final reviews for prompt, appropriate action.

The VA's PIA process is well on its way to becoming a tested and proven methodology which will ensure that 99% of the time our systems and veteran's personal information is protected.

Environmental Protection Agency

The Agency's Chief Information Officer who is the Senior Agency Official for Privacy (SAOP) ensures the Agency adheres to OMB guidance by participating in all agency information privacy compliance activities, evaluating privacy implications, and assessing the impact of the agency's use of technology on privacy and the protection of personal information. The SAOP signs all policies, procedures, and guidance documents concerning the collection, maintenance, and dissemination of personally identifiable information (PII). To stay abreast, there is a quarterly report provided that outlines the administration of the National Privacy Program including: number of Privacy Impact Assessments (PIAs), System of Record Notices (SORNs), Privacy Act requests received, number of forms submitted to collect PII, newly developed policies and procedures, the number of privacy incidents or reviews conducted, and trainings conducted.

The PIA provides a framework for examining the risks and ramifications of collecting, maintaining and disseminating information in identifiable form in an electronic system, and for identifying and evaluating protections and alternative processes to mitigate the impact to privacy on individuals and identify where potential disclosure risks may lie. Informed decision making and the ability to design a system which addresses potential privacy concerns are dependent on early identification of privacy issues. Privacy concerns should always be considered when requirements are being analyzed and decisions are being made about data collection, usage, storage and system design. The PIA incorporates privacy into the development life cycle so that all system development initiatives can appropriately consider privacy issues from the earliest stages of development.

General Services Administration

GSA's Privacy Office collaborates with the Senior Agency Information Security Officer (SAISO) to ensure that Personally Identifiable Information (PII) is collected, maintained, or disseminated in adherence with OMB guidance. Several policy documents illustrate this. GSA Order CIO P 2100.1H, GSA Information Technology (IT) Security Policy requires annual privacy awareness training for all employees and contractors so they are aware of how to handle and protect PII and instructs individuals to encrypt outgoing email attachments that contain Social Security Numbers (SSNs). Those attachments that aren't encrypted are blocked from transmission. Also, the IT Security Policy Privacy Impact Assessments (PIAs) are part of the Certification and Accreditation (C&A) process and reviewed annually. Additional policies are 2180 HCO Rules of Behavior for Handling Personally Identifiable Information (PII), http://www.gsa.gov/portal/content/104276, which explains how to handle PII and the possible consequences when it's improperly handled. 9297.1, GSA Data Release Policy, http://www.gsa.gov/portal/content/104280, explains what information is and is not suitable for Freedom of Information Act (FOIA) release which helps employees and contractors know what information can be released without penalty. Also, 9297.2B, GSA Information Breach Notification Policy, explains what process should be followed in the event of an information breach, meaning who should be notified, who will convene to discuss the incident, and how remedy will be dispensed to impacted individuals.

National Aeronautics and Space Administration

It is NASA policy to protect privacy information that is collected, used, maintained, and disseminated by the Agency. NASA's protections for privacy information shall be compliant with requirements outlined in the Privacy Act of 1974 and amendments, and in other Federal statutes and guidance including the E-

Government Act of 2002, the Children's Online Privacy Protection Act (COPPA), the Health Insurance Portability and Accountability Act and the Office of Management and Budget (OMB) memoranda and circulars. These laws and regulations restrict disclosure of records containing privacy information, grant individuals rights of access and to request an amendment to agency records pertaining to themselves, and require agencies to comply with statutes for the collection, maintenance, and dissemination of records containing privacy information. Collection, maintenance, use, and dissemination of privacy information for both electronic mechanisms and for non-electronic media shall be in compliance with the Federal statutes and guidance.

Adherence to all Federal laws, statutes and guidance is ensured through NASA Procedural Requirements (NPR 1382.1), requiring Information Privacy Threshold Analysis (IPTAs) on all applications, systems and Web sites. IPTAs are accomplished through the internally developed, enterprise-wide electronic Privacy and CUI Assessment Tool (PCAT), resulting in a completed PIA when required.

Managed by the Privacy Program Manager, PCAT is designed specifically to automate all aspects of compliance when Information in Identifiable Form (IIF) or PII is identified and aids in breaking out the applicable requirements modularly, so that information owners can appropriately and efficiently make their way through all of the required steps to reach compliance.

National Archives and Records Administration

NARA’s Senior Agency Official for Privacy is the General Counsel, and staff within that office is responsible for managing the privacy program. This ensures the privacy program staff has access to senior management officials and is abreast of the agency’s large IT acquisitions and policy direction.

For each IT system the agency procures, the Privacy Program staff receives information about what, if any, personally identifiable information will be collected. If PII is collected, the staff and program office complete a Privacy Impact Assessment and, if the Privacy Act requires, update existing or create new System of Records Notices. Two NARA internal policies cover this process.

In advance of the annual FISMA report deadline, the Privacy Program staff asks each system owner to review the PIA for their system to update it or confirm that no changes have been made to the system in the previous year. Staff responsible for public-facing social media outlets must review social media specific PIAs.

NARA’s internal policies also require that any time an office initiates a new information collection, updates, or renews a form that is covered by the Paperwork Reduction Act, Privacy Program staff review what information is collected and the (e)(3) notice statement required by the Privacy Act.

For all IT systems hosted, maintained or accessed by contractors that contain PII, each contract includes the standard Federal Acquisition Regulation clauses for Privacy Act systems and a NARA standard clause on the protection of PII.

National Science Foundation

NSF recognizes the importance of protecting the privacy of personally identifiable information (PII) in information technology (IT) systems. NSF’s goals in this regard are to ensure personal information in electronic form is only acquired and maintained when necessary, and that IT systems developed and used in support of the Foundations’ work protect and preserve the privacy of NSF staff and the public.

NSF is compliant with privacy provisions of the E-Government Act of 2002 (Section 208), which established Government-wide requirements for conducting, reviewing, and publishing Privacy Impact Assessments (PIA), and with subsequent OMB guidance on PIAs issued in September 2003. NSF uses PIAs to explain how the agency addresses privacy issues when developing new or altering IT systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public. Privacy issues are considered for all systems and collections that involve information in identifiable form. NSF's PIAs and Privacy Act Systems of Record Notices are available on the agency's public-facing website.

NSF conducts an annual review of Privacy Act PII holdings. The review of all PII includes all forms, including paper and electronic formats, in any information system. As part of the review, NSF will validate or revalidate the need for its personally identifiable information holdings.

Nuclear Regulatory Commission

Privacy Impact Assessments (PIA) are an integral part of the development process for new IT systems, or the enhancement or modification of existing systems. The PIA has become one of many critical elements of the CPIC process. A PIA must be completed and approved before a business case will be approved under the NRC's Project Management Methodology (PMM). The PIA is an essential part of the OMB Exhibit 300, the "Capital Asset Plan and Business Case." The Exhibit 300 is used under the PMM to demonstrate that the Agency has "employed the disciplines of good project management, represented a strong business case for the investment, and met other Administration priorities to define the proposed cost, schedule, and performance goals for the investment if funding approval is obtained."

A PIA manual and template is provided to assist the sponsoring office in submitting their PIA. This process requires the involvement of the subject matter experts from IT, privacy, records management, information collections, and other programs. The sponsoring office must update its PIAs to reflect changed information collection authorities, business processes, or other factors affecting the collection and handling of information in identifiable form.

Completing a PIA ensures that system owners and developers consider and evaluate existing statutory and key information management requirements that must be applied to new or modified Government systems that contain information about individuals. Applying the PIA process will also help to identify sensitive systems so that appropriate information assurance measures are in place.

Office of Personnel Management

In order to collectively encompass documenting the review of OPM's compliance pertaining to the use of IT to collect, maintain, or disseminate identifiable information, or when new systems are procured for this purpose with information privacy laws, regulations, and policies, OPM has internally developed the "Information Security and Privacy Policy", "System of Records Notice Guide", "Privacy Impact Assessment Guide", and "Process for Analyzing New and Emerging Information Security and Privacy Policy Requirements" policies. These policies, in aggregate, outline the roles, responsibilities, and procedures for all OPM program offices to adhere to when dealing with personally identifiable information. The OPM Senior Agency Official for Privacy incorporated a Privacy Threshold Analysis process for each IT system. This process identifies the privacy implications of each IT system to include implications for collecting information from third party social media websites and determines whether a Privacy Impact Assessment (PIA) needs to be conducted in accordance with OMB guidance and the E-Government Act. This process is outlined in our PIA guidance published on the OPM website to include

guidance on when to update PIAs for IT. Our PIA Guide is located at http://www.opm.gov/privacy/PIAs/PIAGuide.pdf.

Office of the Director of National Intelligence

All IT requirements for the ODNI are vetted through an IT Project Management Review Board, consisting of stakeholders from across the ODNI to include from the Civil Liberties and Privacy Office (CLPO). Before ODNI IT requirements are approved, the developers and system owners work with CLPO to ensure privacy protections and safeguards are incorporated as part of the system design and data lifecycle.

The ODNI does not conduct privacy impact assessment on national security systems which involve the conduct of intelligence activities, as defined by Executive Order 12333. The ODNI has, however, conducted privacy impact assessments for the agency's use of third-party social media websites and applications to engage with the public and in support of the Open Government Directive.

Small Business Administration

SBA.gov automatically collects some technical information from each page analytics to the site in order to provide the best possible experience. SBA.gov uses web measurement technology to automatically track how visitors interact with SBA.gov including where they came from, what they did on the site and whether they completed any pre-determined tasks while on the site. This type of usage is classified by the OMB as Tier 2 usage since it is a multi-session web measurement. Aggregate data is used to help SBA improve the user interface and diversify the content offerings to meet the needs of customers, track operational problems, prevent fraud and improve the effectiveness, security and integrity of the site.

This information does not identify individuals personally and data is only retained in accordance with the SBA data retention policy. This information is only used to help make the site more useful. With this SBA can learn about the number of visitors to the site and the types of technology that visitors use. SBA does not track or record information about individuals and their visits and this data is not shared with anyone outside SBA unless required for law enforcement purposes.

SBA is committed to protecting the privacy of information that is collected from the American people during the course of conducting business. SBA policy, through SOP 40 04 3 "Privacy Act Procedures," directs SBA to conduct periodic reviews of how information is handled within SBA when information technology is used to collect information. Compliance with privacy guidance is considered whenever new systems are developed or new systems are acquired. SBA provides detailed guidance on Privacy Act activities at this URL: http://www.sba.gov/about-sba-services/6752

Social Security Administration

Our use of information technology to collect, maintain, or disseminate identifiable information is governed by a mature Systems Process Improvement program that incorporates best practices for software development and standard processes and procedures for ensuring high quality privacy compliance. We integrate our Enterprise Architecture activities and reflect our governance practices throughout our Systems Development Lifecycle (SDLC). A typical new software release takes six months from conclusion of the planning and analysis to production. The Office of Privacy and Disclosure is involved during the planning and analysis stage, thus we are able to conduct our initial privacy assessment early in the SDLC. We use our Privacy Threshold Analysis (PTA) process to assess the privacy risks in new or revised systems or applications and to determine if a Privacy Impact

Assessment (PIA) or System of Records Notice (SORN) is required. As stated, our initial review occurs early in the SDLC via the Control, Audit, Security, and Privacy Certification checklist. We then subsequently approve Project Scope Agreements and Business Process Descriptions associated with the system or application. In FY12, we continued our practice of training systems development staff on the importance of privacy and privacy risk assessment via the SDLC Configuration Control Board (CCB). We also review any proposed changes to lifecycle roles, activities, or work products that affect the administration of personal information.

U.S. Agency for International Development

USAID's ADS Chapter 508 details the policy directives and required procedures of the USAID Privacy Policy Program. USAID's privacy stance in regard to the protection of personally identifiable information (PII) and privacy-related protections of its employees and business partners complies with the Privacy Act of 1974 (Privacy Act). Section 508.3.3 addresses USAID's policy requirements for the creation and maintenance of Privacy Impact Assessment (PIA) statement documents.

Information handling practices include both manual processes, and automated technology processes implemented by USAID. When conducting a PIA, a Chief Privacy Officer (CPO) representative may assist System Owners to identify the following:

- PII data elements contained within the system;
- Risks to PII that may arise from the electronic collection and maintenance of such data;
- Sharing of PII data elements with other departments or agencies; and
- The physical security of the environment where PII is processed.

System Owners are responsible for conducting or updating the system of record's PIA for the following circumstances:

- For every electronic information system and manual information collection system. The Privacy Office staff will assist System Owners in this identification process;
- Before developing, procuring, or initiating IT systems that provide for the electronic collection of information from ten or more persons (excluding federal agencies or employees);
- When system changes, create a new privacy risk;
- When other factors affecting the collection and handling of PII, information collection authorities, or business processes change; or
- Once every three years for existing systems.

N. IT Training Programs

The E-Gov Act calls for agencies to establish and operate information technology 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. The following section provides descriptions of agency IT training program, privacy training program, cross-agency development programs, and competencies reviews for IT workforce.

Department of Agriculture

In FY12, USDA piloted the Information Technology (IT) Program Management Career Track that aligns with published federal guidance and OMB's 25 Point Implementation Plan. USDA also formulated, initiated, and instituted a Department-wide IT Program Management Career Track Pilot (*PILOT*).

Both the *PILOT* and resultant Certification framework are based on the OPM Competency Model for IT Program Management, which consists of three certification levels. A prerequisite course in the USDA CIO Governance Process is mandatory for all potential and current IT Program Managers.

The Department of Veteran Affairs Acquisition Academy offers a no cost training module for Other Government Agencies, in which USDA is participating as part of the *PILOT.* USDA has achieved nearly $50,000 in cost savings to date by partnering with the Veterans Administration Academy.

Also, the USDA Privacy Office implemented in late FY11 an online Privacy training course, *"Protecting Personally Identifiable Information."* Based on a Defense Information Security Agency privacy training program, this course was modified to include USDA-specific privacy protection information. It is available Department wide via AgLearn, USDA's online learning management system.

In less than one year, over 3,600 USDA employees, contractors, and stakeholders have completed the course. An additional 600 learners have signed-up for this course At deployment, the course was mandatory for Privacy Officers, Freedom of Information Act Officers, and Information Security System Program Managers. Citing the need for enhanced training, and constrained resources several USDA agencies elected to make this training mandatory for all employees.

Department of Commerce

IT Security Training Program: Commerce is building off successes from policy implementation that requires professional IT security certifications and role-based training for individuals with IT security responsibilities. Using the Awareness and Training family of security controls as a framework, Commerce is increasing IT security role-based training opportunities and content to reflect current changes in IT security special publications, new IT security requirements, and topics relevant to the dynamic nature of IT security. Commerce is expanding the delivery methods used for role-based training through the use of webinars to reach members of the geographically-dispersed IT security workforce.

Privacy Training Program**:** Commerce requires all new employees to receive initial privacy training during their orientation briefing. To address general user training, Commerce created an interactive, web-based training that addresses protecting PII which is available on the Commerce Learning Center. Additionally, the Commerce Office of General Council provides training on FOIA and the Privacy Act upon request.

Cross-Agency Development Programs: NIST leads the National Initiative for Cyber Security Education (NICE). The NICE initiative is comprised of over 20 federal departments and agencies to ensure coordination, cooperation, focus, technology transfer, and sustainability for IT security training and education.

Competency Reviews: The Commerce CIO Memo on February 24, 2010 required critical elements be integrated into Senior Executive/Professional Performance Agreements for individuals assigned as

Authorizing Officials or System Owners. As part of Operating Unit compliance assessments, spot checks are performed on development agreements to verify compliance with the requirement.

Department of Defense

DOD employs various methods to deliver training, education, and professional development opportunities for the IT workforce. These include traditional classroom training, computer-aided instruction, web-based training, professional military education, support for undergraduate, graduate, and post-graduate coursework, and a cooperative training/certification venture with the private sector, which serves as the cornerstone of DOD's Information Assurance Workforce Improvement Program. DOD academic institutions such as the iCollege at the National Defense University and the Defense Acquisition University provide collaborative IT educational experiences within DOD and with federal agency partners. DOD implemented its pilot IT Exchange Program (ITEP) to provide personnel exchange opportunities with the private sector. In 2012, DOD instituted an IT Program Management (PM) Certificate at the iCollege based on the OPM-developed IT PM competencies and completed an assessment of the competencies required by the DOD IT Acquisition workforce. DOD completed an update to the Clinger-Cohen Core Competencies on behalf of the Federal CIO Council; these competencies will be used to update curricula at the academic institutions, which comprise the CIO University consortium.

In accordance with the Privacy Act training requirements of OMB Circular A-130, "*Management of Federal Information Resources*," and DOD 5400-11R, "*Department of Defense Privacy Program*," DOD offers various instructional programs. These include a 4-day Defense Privacy Officer Professionalization Program; a Privacy Act Compliance & Management (PACMan) Course for privacy support personnel; SORN training workshops; PIA/systems owner training; Component provided annual and refresher Privacy Act training courses offered through various modalities; and other targeted privacy conferences and workshops.

Department of Education

The Privacy Safeguards and Information Assurance Programs develop and update general IT security and privacy training awareness training for all staff and contractors and specialized role-based privacy training for senior officials, system administrators and others dealing with data and IT.

ED uses a mobility assignment program (MAP) as one piece of its overall career development strategy, which includes formal details and developmental assignments, classroom as well as on-the job training, individual career counseling, Individual Development Planning, and special programs such as the Upward Mobility Program, the Mentoring Program, and other leadership development programs.

Performance management is one of the Department's top priorities. It is a results-oriented process to help improve individual performance to achieve the Department's mission. The REsults ACHieved (REACH) system is designed to promote consistency and transparency across the organization in how work is defined and evaluated. REACH focuses on employees and supervisors working together to develop performance plans, maintaining ongoing feedback about expected outcomes, rewarding good performance, and creating development plans to improve results. Competency reviews for the agency's IT workforce are performed as part of ED's overall performance management system.

Department of Energy

The Energy Office of the Chief Information Officer (OCIO) has developed and implemented an IT Project Management Qualification process to ensure that project managers for key IT investments as identified on the Energy Budget Exhibit 300s are certified. The IT Project Management Qualification initiative was implemented in accordance with Office of Management and Budget (OMB) mandates and has been integrated with Energy's Capital Planning Investment Control Program review and oversight activities for all new/future major IT investments. IT staff who do not currently manage major IT investments as identified on Budget Exhibit 300s are provided the opportunity to develop project management skills to support future investments. OCIO tracks and approves Energy IT project managers throughout the certification process. The process provides an assessment of project managers' skills, level of project manager-related experience and training, and then follows up with appropriate provision of training to ensure proper certification of Energy IT project managers.

Energy participates in the Federal CIO and Office of Personnel Management (OPM) Government-wide Information Technology Workforce Capability Assessments (ITWCA) to capture key information on workforce competencies, IT skills and Specialized Job Activities. Assessment results provide critical information to enable agency and federal IT leaders to meet human capital goals, perform mission-critical occupation reporting, and prepare future IT human capital initiatives, such as training.

Department of Health and Human Services

HHS' mission and diversity of services make it imperative that the Department maintain a well-trained IT workforce that exhibits technical knowledge and expertise. The HHS OCIO is working diligently to meet the rapidly growing training needs of HHS' IT Workforce. In order to meet these needs, the OCIO uses the following guidelines to assess its IT Workforce:

- Assess the established OCIO knowledge and skill training requirements for IT personnel and determine if the requirements are adequate.
- Assess the extent to which management levels of HHS meet the OCIO knowledge and skill requirements.
- Develop strategies for the hiring, training, and professional development of HHS personnel in the area of information technology (IT).

As a result of these assessments, the OCIO has already implemented Basic Project Officer's training and Project Management training for its employees. The OCIO has plans to build upon its training curriculum by adding additional programs to meet the diverse needs of all HHS IT Workforce personnel. The following information is available: HHS OCIO IT Workforce Roadmap, What is Workforce Planning, Why is Workforce Planning Important, IT Workforce Committee, and IT Workforce Policy.

Department of Homeland Security

The DHS Information Technology (IT) Program Management (PM) Development Track (the "Track") is an IT-focused, program/project management training program sponsored by the DHS Chief Information Officer. The purpose of the DHS ITPM program is to provide the framework and training to the program/project managers, who oversee the Department's IT programs/projects. The certification program is designed to develop a cadre of qualified and well-trained professional managers who are eligible for formal assignment to IT programs/projects within the Department. Depending on the level of experience, after completion of the DHS IT Program Managers Track, graduates are eligible to obtain DHS Program Managers Certification up to Level III. The focus of the Track is on practical IT

program/project management training, which addresses applicable DHS directives, policies, methods, and practices.

Further emphasis was recently placed on the need to incorporate IT specialization training when OMB published "Contracting Guidance to Support Modular Development" on June 14, 2012. After its publication, market research found that no vendors currently offered training in modular contracting methods although one course was in development and is expected to be available in Q1 FY13.

Department of Housing and Urban Development

IT training complies with the guidance of the Federal Acquisition Certification for Program/Project Managers (FAC-P/PM) as set forth by the Office of Federal Procurement Policy's guidance. This policy sets the requirements for training in the following areas: acquisition management, Government-specific, program/project management, earned value management, business/finance, life cycle cost analysis, and leadership development and communications management at the entry, mid and senior levels. OCIO awarded a 250-seat contract to provide training to the OCIO workforce.

The Privacy Office provides training designed to focus on the importance of protecting employee and citizen data. This training includes the annual mandatory privacy protection training and "as needed" training for the Department and/or Privacy Liaisons Officers.

HUD's 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 HUD employees, and security alerts as circumstances warrant.

HUD's Computer Self-Help Desk (CSHD) is a one-stop website providing tricks and tips on frequently used applications that is available to all employees. The OCIO's Virtual Training site also offers HUD employees additional training opportunities via online meeting rooms or classroom sessions. New classes are added monthly.

The HUD Virtual University (HVU) offers HUD employees access to over 2,000 online courses from the SkillSoft courseware libraries as well as custom courses developed by HUD program organizations.

Department of the Interior

Interior surveyed its IT workforce in spring 2012 to assess IT capabilities with regards to 1,000+ skills and for proficiencies in 14 behavioral and business competencies. Competencies were selected based on the types of IT and technology management roles performed by IT professionals. In FY13, it is expected that Interior will define additional operational details for the IT future state and identify the related competencies needed to achieve that future state. Interior will compare the IT workforce future state requirements against the IT workforce skills and competency assessment data to determine gaps. To close the gaps, Interior will develop a comprehensive, IT workforce training and development plan to ensure execution of the IT future state. Interior's Privacy Training Program includes mandatory Privacy Act training as part of the Federal Information System Security Awareness (FISSA) training for all new employees and contractors. Specialized computer-based training courses and individual or group training is also provided. Interior developed The Privacy for IT Personnel course, a computer-based privacy training course for IT personnel in accordance with OMB M-07-16 which requires that agencies provide targeted, role-based training to managers, Privacy Act officers and employees with privacy responsibilities. Interior continues to focus on the importance of having qualified, skilled IT project and program managers. In collaboration with DOI University, Interior offers the following two certificate

programs in support of this focus: Project Management Associates Certificate or Masters Certificate from George Washington University, and a FAC-P/PM certification program. Individual classes or the full curriculum resulting in certifications are available.

Department of Justice

For FY12, the Justice IT Security Staff (within Justice's OCIO) led Department-wide IT training efforts through its Information Security Employee Services (ISES) Team. Comprised of IT training points of contact from each of the Department's Components, the ISES Team is responsible for drafting annual IT security training policy and procedures for Computer Security Awareness Training (CSAT) and IT professional training offerings.

Justice utilized three learning management systems (LMS) for self-launched delivery of learning offerings and recordation of training completions. In addition, the LMS were used for external training approvals and creation of Individual Development Plans (IDP).

Justice holds membership in the Federal CIO Council's IT Workforce Committee and chairs or participates in several cross-agency programs such as the IT Job Shadow Day, Scholarship for Service: Cyber Corps, and the IT Workforce Capability Assessment. The Department also has an internal CIO Council, IT Security Council, and various training and developmental working groups.

The Justice Office of Privacy and Civil Liberties (OPCL) provided training on the Privacy Act of 1974, the interface between the Privacy Act and the privacy provisions of the E-Government Act, and the interface between the Privacy Act and the Freedom of Information Act, through the Office of Legal Education. These training courses were open to all Justice employees, and videos of the courses are available to Justice employees through the Justice's LMS. The OPCL also reviewed the privacy portion of the Justices's CSAT course to ensure that it contained appropriate information on federal information privacy laws.

Department of Labor

Labor provides annual CPIC and IT investment related training classes to Labor IT Project Managers and Integrated Project Team members, including contractors. The training classes include such topics as the budget submission and CPIC (i.e., Exhibit 300 and Exhibit 53, eCPIC training, Post Implementation Review, Operational Analysis, Earned Value Management, Baseline Management training, and Integrated Baseline Review training) and System Development Life-Cycle Management training including Acquisition Strategy, Risk Management, Alternatives Analysis, Cost Benefit Analysis, and project planning software training. The Office of the Chief Information Officer (OCIO) believes in the value of its IT training program as it has led to better managed and higher performing IT investments.

In addition to the CPIC and IT investment training, Labor conducts a comprehensive computer security training program that includes general security, privacy awareness and specialized training. All federal employees and contractor staff are required to meet the Department's annual computer security and privacy awareness training requirements as mandated by the Federal Information Security and Management Act.

Annually, Labor ensures all current users receive basic information system security and privacy awareness training. All new hires receive basic information system security and privacy awareness training before they are permitted access to any information system. Users with significant security roles and responsibilities leverage free federalized training opportunities available through the Information Systems Security Line of Business Center of Excellence for training, webinars and conferences. In

addition to the annual awareness training, the OCIO provides additional awareness materials via "all hands" email notifications, IT newsletters, elevator posters, and conferences or webinar sessions.

Department of State

The Foreign Service Institute (FSI) is an OPM-designated Government service provider that makes available e-training services to several agencies. Recently, FSI completed a major project to host an Internet-accessible virtual training system for a Government-wide audience of up to 125,000.

FSI, along with the Bureaus of Diplomatic Security and Information Resource Management provides annual Cyber Security training that State employees must complete to gain access to State networks. FSI's School of Applied Information Technology offers four Information Systems Security and six Federal Information Risk Assessment courses annually to State IT systems administrators.

State's IT Skills Incentive Pay program provides incentives to Civil and Foreign Service IT professionals to ensure they stay current with IT and IT security developments.

FSI develops online training toolkits for Foreign Service and Civil Service IT professionals that assist them in determining appropriate training paths. IT professionals include Information Management Specialists, Information Management Technology Specialists, and Information Technology and Telecommunication Managers.

The Bureau of Human Resources' Career Development and Assignments Division provides an online Career Development Program Playbook for Foreign Service IT Professionals to help them fulfill the requirements for the most senior level positions.

The Bureau of Administration's Privacy Division has developed several options for training State employees on privacy issues. In collaboration with FSI, the Privacy Division implemented an on-line training module PA459, Protecting Personally Identifiable Information (PII). This mandatory course instructs employees on their responsibilities for identifying, protecting, and reporting PII breaches.

The Privacy Division offers privacy briefings in State's orientation program for new Civil Service employees and Presidential Management Fellows and offers on-site PII training to offices for contractors. The Privacy Division also makes privacy training resources available to employees on State's Intranet including a Privacy Tip of the Week.

Department of Transportation

The DOT CIO's office conducts trainings known asTechnology, Evaluation and Learning Series (TELS) sessions. By way of example, here is a notification to DOT of an upcoming TELS session on Cybersecurity, but please note that the TELS sessions cover a wide range of IT Training areas including privacy, CPIC related (Exhibit 300's and Exhibit 53's), EA related, budgeting for IT projects, etc. The only training not covered directly by OCIO related to managers training and supporting staff members; these are either conducted by the agency HR department, or are offered off-site.

The "Your Mission Focus in Cybersecurity" collaborative session will illustrate how cybersecurity and operations are integral components, dependent upon each other to defend and assure the mission. Following the session, participants will be better prepared to:

- Identify cybersecurity's place in your mission space
- Describe your mission's contribution to cybersecurity

- Discuss ways to improve your security posture and mission collaboratively
- Explain what other partners and agencies do for cybersecurity

Department of the Treasury

Treasury offers and uses a variety of methods for IT training purposes:

- Treasury CPIC operational metrics training. Sessions included an overview on the development of good metrics, metric types, issues with metrics, and Treasury's specific approach to reporting metrics. Treasury then reviewed the metrics with investment owners to identify how they could improve or replace measures that needed further work.
- OCIO used the Treasury Hamilton Fellows program to fill key vacancies within the organization. The Hamilton Fellows program was designed to attract recent graduates from a variety of academic disciplines with strong analytic, research, and writing skills. The program required fellows to fulfill training obligations for successful completion of the fellowship program. Future hires will be made through OPM's new Pathways Program.
- The Implementation of the Federal Acquisition Certification for Project and Program Managers (FAC-P/PM) program at Treasury has been delegated to the Treasury CIO in Treasury Directive 12-11. At a minimum, bureaus shall apply the FAC-P/PM requirements to all program and project managers assigned to major acquisitions as defined in OMB A-11.
- Cross-agency development: Employee detail assignment to Interior, Assistant Deputy Director Organizational Transformation, to implement assessment recommendations for Interior's corporate university; restructure bureau-level training & development offices to streamline operations and reduce redundancy.
- Treasury Learning Management System (TLMS): used for annual training programs, competency reviews, and offers a selection of additional online learning courses for the Treasury workforce.

Department of Veterans Affairs

The Office of Information Technology (OI&T) through the IT Workforce Development Office (ITWD) has successfully implemented several information technology (IT) training initiatives to include security, competency modeling and certification programs as demonstrated by the following:

ITWD provides FISMA training for all users of VA information and role-based security training for those with significant information security functions. The ITWD security training program is designated as both a Tier I and Tier II service provider under the E-Government shared service center program administered through the Department of Homeland Security (DHS). ITWD represents VA on components (3) three and (4) four for the Federal National Initiative for Cybersecurity Education (NICE).

IT role-specific competency models provide a framework for all of VA's IT professionals to assess their skills and provide targeted training maps to close identified skill gaps. This year in support of the *25-Point Implementation Plan* to reform federal IT management, ITWD implemented the IT Project and Program Manager's competency model.

ITWD's IT certification program provides vouchers, guidance and procedures for obtaining professional certifications for OI&T employees. Individuals are strongly encouraged to have an approved certification for their particular job classification.

The New Hire Orientation Program is designed to provide OI&T new hires, supervisors, and new hire coordinators a comprehensive, convenient location for checklists and resources necessary to assist new hires in acclimating to the VA during their first six months of employment. The new ISO training program provides a comprehensive 2-year training program for newly appointed ISOs to receive one-to-one guidance from a mentor as well as standard training. A separate 2-year intern program (Technical Career Field Program) is targeted for IT specialist interns new to OI&T.

Environmental Protection Agency

The Office of Environmental Information (OEI) provides Information Technology (IT) training to EPA employees through a variety of mechanisms, including instructor-led courses, webinars, and online courses. OEI is responsible for developing, administering, and hosting online training that includes:

- Agency-wide, mandatory training - IT Security Awareness, IT Role-based Training, No Fear Act, Ethics Training, and Continuity of Operations Planning (COOP).
- IT Technical Training – EPA eLearning, Remote Access for Telework, , Email Optimization and Single Sign-on.
- Program Specific training – EPA Quality Management, Working Effectively with Tribal Governments, Compass (financial system), Environmental Modeling, Health and Safety, Privacy, and Children's Health & Safety.

OEI manages the EPA eLearning tool, which is the primary platform for the Agency's online training. EPA eLearning is a cloud service (provided via the Internet) and therefore is accessible to all employees 24 hours a day, 7 days a week from any location. OEI also manages and conducts Instructor-led IT Training for the Agency, via both classroom and webinars.

General Services Administration

GSA offers Information Technology courses to employees via an internal On-Line University and GSA's University for People program. GSA's privacy training policy is found in GSA Order CIO P 2100.1H, GSA Information Technology (IT) Security Policy. GSA participated in the CIO Council's 2011 IT Workforce Capability Assessment which led to the development of GSA's IT Human Capital Strategic Plan. GSA OCIO used the results to assess the capabilities, skills, and potential resource gaps within GSA's IT Workforce.

As one of GSA's four Mission Critical Workforces (MCWs), IT is critical. GSA created a Technology Learning Map which provides the employee a series of courses across three (3) proficiency levels and pre-defined skill sets. Upon completion of select technology training opportunities, the employee is prepared to fulfill recommended certifications and address applicable reinforcing activities. For cross-agency development programs, GSA's Office of Citizen Services and Innovative Technologies (OCSIT) manages DigitalGov University (DGU), the Federal Government's training program for digital media and citizen engagement. Since 2004, DGU has sponsored more than 200 training events with more than 18,000 attendees.

CIO University, managed by GSA's Office of Governmentwide Policy, is a cooperative venture between the Federal Government and select institutions of higher learning to offer graduate level programs that directly address federal executive core competencies based on Clinger-Cohen legislation. Students from government and industry who graduate from IT graduate degree programs at any of the six universities receive a CIO University Certificate from the Government. Since 2000 more than 1,500 people have graduated.

National Aeronautics and Space Administration

NASA utilizes an online training system called the System for Administration, Training, and Educational Resources (SATERN) to provide IT technical, IT security and privacy training to the NASA community. Specifically, in accordance with the Federal Information Security Management Act, Information Technology (IT) security awareness training is mandatory for all NASA employees and contractors involved with Agency information or information systems.

Per OMB Memorandum M-07-16, NASA employees and contractors are provided annual privacy and sensitive information training with recurring training also provided for IT Security and Privacy related topics. Additionally, Centers conducts Incident Response and Privacy Breach Response exercises to ensure employees are prepared in advance of an incident or breach of sensitive privacy information. Finally, monthly video conferences are conducted with the Center Chief Information Security Officers and the Center Privacy Managers during which there is policy and program updates, and discussions/ collaboration on issues facing the community.

NASA provides training opportunities and cross-agency development through programs such as career development details, NASA FIRST, NASA Mid-Level Leaders, and participates in several industry developmental programs such as ACT/IAC Voyagers & Fellows, SIM Fellow, and the Year-Up Student Intern. Competencies are managed through annual IT surveys and implementation of NASA's IT Workforce Development plan.

National Archives and Records Administration

NARA provides most of its IT training via its Learning Management System (LMS), an Internet-based software package that delivers and manages learning content and resources. Application-specific training (as needed) is provided by commercial vendors or other Government agencies.

FISMA-compliant IT security training is provided at the time of on-boarding of all NARA staff and annually as required. In FY12 NARA developed Tier II training program for Information System Security Officers, IT Security Staff. Annual IT Security briefings are provided to Administrative Officers, Facilities Officers, Field Office System Administrators, and Network Operations support staff.

NARA provides annual privacy training on personally identifiable information and the Privacy Act to all employees as part of the online IT Security and Awareness training. In addition, employees responsible for screening archival records for release to the public receive in-depth Privacy and Freedom of Information Act training regularly.

All new employees receive a written training packet with information on privacy compliance. NARA has many term employees that may not receive access to agency computers for their jobs or may miss training cycles because of their entry and exit dates. Thus, providing hard copies of PII information is an essential part of the training program.

NARA provides a wide array of cross development opportunities for our IT workforce (e.g., GS-2210s). For ease of use and targeted development, the curriculum and activities are mapped to the Clinger-Cohen required competencies. Competency gaps are identified, integrated into staff Individual Development Plans (IDPs), and tracked and reported on using NARA’s Learning Management System.

National Science Foundation

NSF's mission depends on information systems that operate continuously, maintain high availability and protect information from inappropriate disclosure. NSF recognizes the importance of maintaining a first-rate IT workforce, and has implemented IT training programs for NSF staff and contractors to that end.

NSF requires all staff and contractors to complete Security and Privacy Awareness training course as mandated by the Federal Information Security Management Act (FISMA). All staff and contractors must complete the IT Security training each year. Staff members also have the option of attending an instructor-led session to review IT Security and Privacy Awareness issues. In recent years, NSF has achieved an average 98% Foundation-wide completion rate for IT Security and Privacy Awareness training.

In alignment with federal IT workforce initiatives and other drivers, NSF conducts periodic IT competency assessments to evaluate the current and future needs of the agency's technology staff. As appropriate, NSF uses the results of competency assessments in developing strategies related to recruitment, retention, and training of the agency's IT workforce.

Nuclear Regulatory Commission

The NRC's Office of Information Services (OIS), Computer Security Office (CSO), and the Office of the Chief Human Capital Officer (OCHCO) partner to deliver training to build the needed general and specialized IT competencies for NRC staff.

General IT competencies include mandatory annual training such as Personally Identifiable Information and Computer Security Awareness for all staff as well as IT system deployment training. Specialized training is offered for different roles, e.g. Project Managers and Information System Security Officers.

A systematic approach determines the best method for training delivery offering a blend of instructor-led and on-line courses as appropriate to build the needed competency.

During FY12, the NRC did an in-depth review of employee training records and vendor payments to assess the status of IT training and subsequently awarded a contract to conduct a training needs assessment to identify the specific training needs of IT staff agency-wide, to begin in FY 2013. The assessment results will be used to develop a Statement of Work for an enterprise-wide contract to meet the training needs of IT staff. NRC's goal is to continuously improve the efficiency and effectiveness of IT Training delivery, minimize training costs, provide IT staff competencies in alignment with critical competencies identified through the Office of Personnel Management (OPM), and provide NRC with a foundation for implementing the White House's "25 Point Implementation Plan to Reform Federal Information Technology Management".

Finally, NRC supports cross-agency competency assessments, such as the CIO Council's current IT Workforce Assessment for Cybersecurity.

Office of Personnel Management

All OPM employees and contractors who have access to the agency's local area network (LAN) participate in annual online IT security and privacy training. Compliance is 100%; those who do not comply lose access to the LAN until they complete the training. During FY12, we conducted the following actions toward closing skill gaps identified in FY11:

- Linked competency paths for IT Program Managers to courses in Learning Connection (OPM's learning management system) for grades 13, 14 &15.
- Launched an agency-wide Learning Center offering online and classroom instruction on a variety of professional development topics.
- Met with Learning Connection representatives to discuss additional online instruction needs for IT Program Manager development. The curriculum is now mapped and courses are communicated to staff for inclusion in their Individual Development Plans.
- Identified 2210s as IT Program Managers: (a) all 2210s at grade 13 and above have been identified agency-wide and (b) certification paths for improvement were mapped using Learning Connection.(Federal employees are classified by series. (2210 is a professional series for IT Specialists. They are highly skilled professionals who require ongoing training and development to maintain the competencies needed to lead IT Projects.)

We established a Program Management Community of Practice (CoP) to allow experienced Program Managers to share knowledge, help build competencies in others, and drive IT Program Management succession planning beyond the 2210 series (among those with significant IT roles). Participation in this CoP also constitutes certified training for Federal Acquisition Institute (FAI) Program/Project Manager. We have created a CIO Action Learning Team to form an IT Program Management Skill Gap CoP to better identify and meet staff needs. Closure of these skill gaps will be verified in the coming 2012 survey.

Office of the Director of National Intelligence

The Civil Liberties and Privacy Office (CLPO) provides an overview briefing of privacy and civil liberties as part of the Entrance-On-Duty orientation for all ODNI personnel, which include cadre employees, detailees, assignees and contractors. A specific web-based training module was recently developed for the National Counterterrorism Center (NCTC). Geared towards personnel directly involved with the analysis of information potentially concerning U.S. Persons, this module provides NCTC analysts with job-specific and comprehensive privacy training. A web-based training module, covering the Privacy Act and Personally Identifiable Information, is currently under development for the rest of the ODNI workforce. In addition, CLPO has provided privacy and civil liberties presentations as part of other ODNI-sponsored training, conferences and seminars.

Small Business Administration

The Federal Information Security Management Act (FISMA) of 2002 requires Federal agencies to provide mandatory periodic computer security awareness training to all individuals who are involved with the management, use, or operation of a Federal computer system, or those who have access to SBA's sensitive data. The goal of this training is to provide employees and contractors with an overview of computer security laws, regulations, and SBA policies. This training teaches users good security practices and informs them about their computer security responsibilities. Through this program SBA ensures that all employees and contractors are training annually on IT security and privacy. OCIO also provides portfolio management training to IT Investment Managers on budget submission processes, supporting tools (including eCPIC) and related topics. Other training resources including a training calendar, procedures to request training and training opportunity announcements and information notices are provided to SBA employees.

Social Security Administration

SSA places a high priority on cyber security training and education, using a variety of methods to raise awareness by providing computer based training, video training, classroom training, and interactive-format anti-phishing training. Externally, SSA participates with the National Initiative for Cybersecurity Education (NICE)/Federal Chief Information Officers Council (CIOC) IT Workforce Assessment for Cybersecurity.

The Systems Training and Communications Branch (STCB) manage the Office of System's Technical Training Program, using:

- Training Needs Assessment Survey (TNAS) – Comprised of courses satisfying the relevant areas of competency. Components identify critical needs in the following four areas; succession planning, skill gaps, agency initiatives, and new hire training.
- Special Request Form – Used to request training not listed on the TNAS or planned for in initial training plans.
- Skills Inventory – STCB analyzes current skills and gap data in detail and develops a training solution for skill gap areas.

STCB schedules courses and distributes training allocations based on identified critical needs. Each component makes the final determination as to who is scheduled for the training. STCB also considers training requests that identify critical training needs and schedules courses based on priority and available training funds. Other training delivery options made available:

- SSA National Learning Management System (LMS)
- Books 24x7
- Webinars covering subjects applicable to agency systems
- Internal training developed by ahency systems subject matter experts

U.S. Agency for International Development

USAID provides IT initial and awareness training in online and classroom formats accessible through USAID University, AIDConnect and the training division in Human Resources. General IT courses cover office productivity software as well as software and applications specific to USAID, such as the Global Acquisition and Assistance System (GLAAS) and Phoenix (USAID's financial management system).

The USAID Information Assurance division (IA) targets training on security topics for general users and users with specialized security responsibilities. Classroom-based initial information security awareness is required for all new users to the Agency with network access. Annual information systems security awareness training is provided through the "Tips of the Day" program. Specialized information security awareness training is provided annually to those with elevated administrative privileges, system ownership, and managerial security responsibilities. Information Systems Security Policy is outlined in ADS 545.