

9. LEVERAGING THE POWER OF TECHNOLOGY TO TRANSFORM THE FEDERAL GOVERNMENT

Greater transparency, accountability, and public participation are central to the President's open Government agenda. These principles will allow the American people to have a stronger role in how their Government addresses the challenges we confront as a Nation. New technology has the potential to drive innovation in Government by making it possible to connect Government employees to one another and to the American people, thereby enabling the sharing of information and expertise, and the solving of problems in new and more effective ways.

The President's Budget invests resources to support these goals, coordinated with policies that emphasize sound investments of taxpayer dollars, assure information security, and protect individual privacy. As such, Federal information policies will focus on:

- Fulfilling the President's pledge for a more transparent, participatory, and collaborative Government through the adoption of innovative web 2.0 technologies;
- Modernizing and improving the effectiveness of Government services through the adoption of modern information technology (IT) systems;

- Securing Federal systems and national information infrastructure against natural and malicious threats;
- Saving taxpayer dollars by improving the IT investment planning process through leveraging investments for wider use across Federal agencies, eliminating duplicative and poorly managed projects, and streamlining IT procurement.

The 2010 Budget reflects the growing responsibilities for Federal IT management. Leadership for IT management is assigned to the Federal Chief Information Officer (CIO) in the Office of Management and Budget (OMB). The history of this position goes back to the Information Technology Management Reform Act of 1996 (Clinger-Cohen Act), which created Federal department and agency chief information officers to plan and manage agency information resources and better achieve program missions. The Paperwork Reduction Act of 1980, Federal Information Security Management Act of 2002 (FISMA), E-Government Act of 2002, and the Federal Funding Accountability and Transparency Act of 2006 (FFATA) all contribute to the requirements for managing Federal IT.

GOVERNMENT 2.0

Transparency—The Administration is dedicated to making more Federal data available to the public in more usable forms. To further this priority, *USASpending.gov* is being reoriented, and the *Data.gov* initiative will be launched.

USASpending.gov. On his first full day in office, the President issued a memorandum to the heads of Federal agencies emphasizing that greater openness and transparency is critical to strengthening our democracy and promoting efficiency and effectiveness in Government. Full implementation of the Federal Funding Accountability and Transparency Act of 2006 ("Transparency Act") is a cornerstone of these efforts, and the Administration is committed to achieving the Act's goals.

At *USASpending.gov*, citizens will be able to see how, when, with whom, and on what the Government is spending taxpayer funds, and whether or not that money is delivering results. Visitors to the site will be able to download data and related information from *USASpending.gov* to combine into different data sets, conduct analysis and research, or power new information-based products and businesses. In sum, citizens will be able to track spending and results, participate in holding the Government and

recipients of funding accountable for performance, and use the resulting information to create value for themselves and others.

Data.gov. The Federal CIO Council is creating *Data.gov*, an online repository for access to Government data (not otherwise subject to valid privacy, security, or privilege restrictions, consistent with Federal law). Through information presented in downloadable formats on topics such as the environment, energy, health care, and the operations of Government, *Data.gov* has the potential to drive innovation in the public and private sector. Just as Internet mapping industries developed from the release of public geographic locational information, data transparency can spur economic, scientific, and educational innovation.

Recovery.gov. The American Recovery and Reinvestment Act (Recovery Act) is an extraordinary effort to jumpstart our economy, create and save millions of jobs, and put a down payment on addressing long-neglected challenges so the country can thrive. To give the public a thorough understanding of how and where Recovery Act funds are invested, the Act itself provides for unprecedented levels of transparency and accountability so that citizens will

be able to know how, when, and where their tax dollars are being spent. *Recovery.gov* is the main vehicle for that transparency, giving people the tools to monitor the progress of the Recovery Act, track contracts and Federal grants to an unprecedented degree, and provide feedback on the status and results of those investments at the community level. At the continually evolving website, citizens have the opportunity to download program data and related information, conduct analysis and research, or power new information-based products and businesses.

Participation and Collaboration—The Administration believes that public engagement enhances the Government’s effectiveness and improves the quality of its decisions. Knowledge is widely dispersed throughout society, and the Nation benefits when all levels of government have access to that dispersed knowledge. To offer Americans increased opportunities to participate in policymaking and to provide their Government with the benefits of the public’s collective expertise and informa-

tion, the Federal IT agenda is focused on helping agencies use developing technologies to inform the work of Government.

Web 2.0 in Government. Agencies will be called upon to take creative action in developing new approaches to citizen involvement, including the utilization of social and visual technologies, such as Web 2.0 tools. Existing Government websites need to be revitalized with community-driven features and functionality. Opportunities for engagement can be developed through context-driven tools that push opportunities for participation to people on the websites and in other daily contexts. This will enable interactions and applications that were never before possible. Through social media, individuals will be able to increase collaboration on web content to create, organize, edit or comment, combine, and share information using Web 2.0 technologies and forms, including syndicated web feeds, video-sharing, podcasts, social networking and bookmarking, widgets, virtual worlds, and micro-blogs.¹

INFORMATION TECHNOLOGY POLICY

Government IT Workforce—With rapid advances in IT, improved program performance depends heavily on those who manage the IT projects. Qualified project managers and an IT workforce with the necessary competencies are needed for agency investments to be well planned and managed. In 2009, an IT Workforce Assessment Survey will be developed from which a gap analysis will evolve, and agencies can adjust plans to improve their workforce staffing and skills. The table below provides a summary of the latest available data on agency progress toward hiring goals.

Policies in agencies seeking to increase the assignment of qualified project managers to major IT investments continue to be in effect. In the 2009 Budget, as reported on agencies’ Exhibit 53 IT spending summaries, 88 percent of major IT investments have qualified project managers, an increase from approximately 83 percent in the prior year. Going forward, agency performance in addressing skill gaps will continue to be important contributors to the success of Federal IT investments, meaning that recruitment and training will need to be enhanced, through enhancements in IT systems and programs of recruitment, innovative and flexible training arrangements, and other programs addressing the need to bring the best IT ideas

and expertise to bear on how Federal IT systems are designed and managed

Securing Government Systems—As the Federal Information Security Management Act of 2002 enters its seventh year, it is clear that agencies and departments are not yet secure. The Government Accountability Office (GAO) continues to find security weaknesses at agencies.² The Nation cannot continue to ignore this threat. In response, the President initiated a 60-day review of the plans, programs, and activities underway throughout the Government that address our communications and information infrastructure. The purpose of the review is to develop a strategic framework to integrate, resource, and coordinate initiatives in this area both within the Executive Branch and with Congress and the private sector.

OMB will work with agencies, IGs, CIOs, Senior Agency Officials for Privacy, GAO, and the Congress to strengthen the Federal Government’s IT security and privacy programs. As part of those activities, OMB will:

Review Agency Business Cases. Part 7 (Exhibit 300) of OMB Circular A-11 requires agencies to submit a Capital Asset Plan and Business Case Justification for major information technology investments. In their justification, agencies must answer a series of security questions and describe how the investment meets the requirements of the FISMA, OMB policy, and NIST guidelines. The justifications are then evaluated against specific criteria to determine whether the system’s cyber-security, planned or in place, is appropriate.

Table 9-1. THE FEDERAL IT WORKFORCE

	Positions Filled	
	30-Jun-08	Current
Enterprise Architecture	1,670	1,673
Solutions Architecture	1,472	1,457
IT Security	8,449	8,407
IT Project Management	6,061	6,248
Total	17,652	17,785

1 See Godwin, Bev, "Matrix of Web 2.0 Technology and Government," USA.gov and Web Best Practices, GSA Office of Citizen Services, http://www.usa.gov/webcontent/documents/Web_Technology_Matrix.pdf.

2 GAO, High Risk Update, GAO-08-271.

Evaluate Reported Security Metrics. OMB will review the security metrics provided by agencies in their quarterly and annual reports for FISMA compliance. Modifications in metrics may be necessary to improve security. One goal for new metrics would be to move beyond periodic compliance reporting to more continuous approach.

Review Current Cyber-Security Activities. The President has requested a 60-day review of all cyber-security activities within the Federal Government.

Homeland Security Presidential Directive 12 (HSPD-12)—This directive, issued August 27, 2004, and entitled “Policy for a Common Identification Standard for Federal Employees and Contractors,” addressed the recommendation of the September 11th Commission to improve the security of Federal facilities and information systems. In accordance with HSPD-12, agencies are required to follow specific technical standards and business processes for the issuance of Federal credentials including a standardized background investigation to verify employees’ and contractors’ identities. The directive applies to individuals with long-term access to Federal facilities and information systems.

HSPD-12 credentials provide for digital signature, encryption, archiving of documents, multi-factor authentication, and reduced sign-on to improve security and facilitate information sharing. They also provide for a very high level of trust in identity credentials during disaster response, disaster recovery, and reconstitution of Government scenarios.

As of March 1, 2009, more than 2.7 million credentials (48 percent) have been issued to the Federal workforce and 3.3 million background investigations (58 percent) have been completed. Additionally, 20 credential issuance infrastructures are in operation nationwide to issue credentials, and 37 providers and 416 products are on the Approved Products and Services list maintained by GSA. The current focus of agencies is on completing the issuance of credentials to their remaining employees and contractors, and implementing plans to leverage the electronic capabilities of the credentials.

To support this effort, the Federal Identity, Credential, and Access Management (ICAM) segment architecture provides Federal agencies with a consistent approach for managing the vetting and credentialing of individuals requiring access to Federal information systems and facilities. By using enterprise architecture techniques this alignment will provide clarity and interoperability to eliminate redundancies across agency ICAM initiatives.

Current efforts are underway to develop the ICAM segment architecture to unify Federal Public Key Infrastructure

(PKI), the E-Authentication program, and HSPD-12 implementation into a single program activity, while reducing or eliminating duplicative efforts related to identity vetting and credentialing. One of the major outcomes of this effort is to allow agencies to create and maintain information systems that deliver more convenience, appropriate security, and privacy protection, with less effort and at a lower cost.

The ICAM segment architecture will serve as an important tool for providing awareness to external mission partners and drive the development and implementation of interoperable solutions. ICAM solutions will leverage the existing investments in the Federal Government while promoting efficient use of tax dollars when designing, deploying, and operating ICAM systems.

Securing the National Information Infrastructure—The Government’s security concerns extend beyond Federal systems. The Federal Government has the responsibility to protect and defend the country and ensure the well-being of the citizens. However, approximately 85 percent of critical information infrastructure in the United States is owned by interests other than the Federal Government. Therefore, industry and Government share the responsibility for the security and reliability of the Nation’s information infrastructure. The Government Accountability Office has raised concerns about the implementation of protection of the national critical information infrastructure.³ The Federal Government must review the current structure of public-private partnerships and determine what is working and why. As part of the 60-day cyber review ordered by the President, the characteristics of successful public-private partnerships are being evaluated.

Protecting Privacy—Federal agencies are tasked to implement breach notification plans, eliminate unnecessary collection and use of Social Security numbers in agency programs, reduce unnecessary holdings of personally identifiable information, and develop policies outlining rules of behavior and identifying consequences and corrective actions to address non-compliance.⁴ Agencies are expected to demonstrate progress in all aspects of privacy protection.

The Federal Government must continue to improve information security for Federal systems and the information sector overall. This focus, along with a commitment to ensuring privacy as investments are made in the widespread implementation of electronic health records, must be leveraged to set a high bar for the goal of protecting the personal information of all Americans.

IMPROVING INNOVATION, EFFICIENCY AND EFFECTIVENESS IN FEDERAL IT

Businesses facing market pressures from which the Government is more insulated are forced to innovate, adopting emerging technologies with agility, to achieve maximum efficiency. Where appropriate, the Government needs to adopt innovations with the same agility.

Optimizing Common Services and Solutions/ Cloud-Computing Platform—The Federal technol-

ogy environment requires a fundamental reexamination of investments in technology infrastructure. The Infrastructure Modernization Program will be taking on

³ GAO, *National Cybersecurity Strategy: Key Improvements are Needed to Strengthen the Nation’s Posture*, GAO-09-432T.

⁴ OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.

new challenges and responsibilities. Pilot projects will be implemented to offer an opportunity to utilize more fully and broadly departmental and agency architectures to identify enterprise-wide common services and solutions, with a new emphasis on cloud-computing. The pilots will test a variety of services and delivery modes, provisioning approaches, options, and opportunities that cloud-computing brings to Federal Government. Additionally, the multiple approaches will focus on measuring service, cost, and performance; refining and scaling pilots to full capabilities; and providing financial support to accelerate migration. These projects should lead to significant savings, achieved through basic changes in future Federal information infrastructure investment strategies and elimination of duplicative operations at the agency level.

Cloud-computing is a convenient, on-demand model for network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The cloud element of cloud-computing derives from a metaphor used for the Internet, from the way it is often depicted in computer network diagrams. Conceptually it refers to a model of scalable, real-time, internet-based information technology services and resources, satisfying the computing needs of users, without the users incurring the costs of maintaining the underlying infrastructure. Examples in the private sector involve providing common business applications online, which are accessed from a web browser, with software and data stored on the "cloud" provider's servers.

Implementing a cloud-computing platform incurs different risks than dedicated agency data centers. Risks associated with the implementation of a new technology service delivery model include policy changes, implementation of dynamic applications, and securing the dynamic environment. The mitigation plan for these risks depends on establishing a proactive program management office to implement industry best practices and government policies in the management of any program. In addition, the Federal community will need to actively put in place new security measures which will allow dynamic application use and information-sharing to be implemented in a secure fashion. In order to achieve these goals, pilot programs will provide a model for scaling across the Government.

Pilots supporting the implementation of a cloud-computing environment include:

- End-user communications and computing—secure provisioning, support (help desk), and operation of end-user applications across a spectrum of devices; addressing telework and a mobile workforce.
- Secure virtualized data centers, with Government-to-Government, Government-to-Contractor, and Contractor-to-Contractor modes of service delivery.
- Portals, collaboration and messaging—secure data dissemination, citizen and other stakeholder engagement, and workforce productivity.

- Content, information, and records management—delivery of services to citizens and workforce productivity.
- Workflow and case management—delivery of services to citizens and workforce productivity.
- Data analytics, visualization, and reporting—transparency and management.
- Enterprise Software-as-a-Service—for example, in financial management.

Cloud-computing will help to optimize the Federal data facility environment and create a platform to provide services to a broader audience of customers. Another new program, the "work-at-a-distance" initiative, will leverage modern technologies to allow Federal employees to work in real time from remote locations, reducing travel costs and energy consumption, and improving the Government's emergency preparedness capabilities.

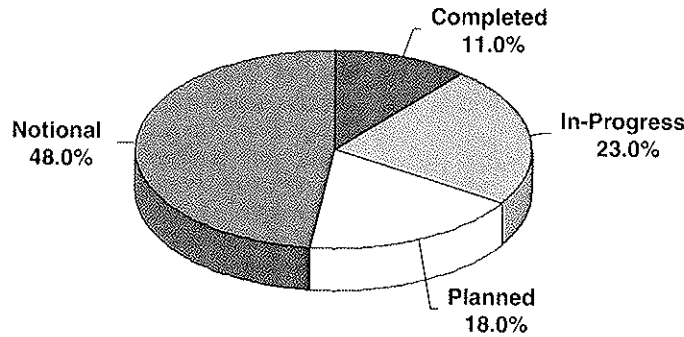
Cloud-computing and "work-at-a-distance" represent major new Government-wide initiatives, supported by the CIO Council under the auspices of the Federal CIO (OMB's E-Government Administrator), and funded through the General Services Administration (GSA) as the service-provider.

Of the investments that will involve up-front costs to be recouped in outyear savings, cloud-computing is a prime case in point. The Federal Government will transform its Information Technology Infrastructure by virtualizing data centers, consolidating data centers and operations, and ultimately adopting a cloud-computing business model. Initial pilots conducted in collaboration with Federal agencies will serve as test beds to demonstrate capabilities, including appropriate security and privacy protection at or exceeding current best practices, developing standards, gathering data, and benchmarking costs and performance. The pilots will evolve into migrations of major agency capabilities from agency computing platforms to base agency IT processes and data in the cloud. Expected savings in the outyears, as more agencies reduce their costs of hosting systems in their own data centers, should be many times the original investment in this area.

Similarly, investments to extend the use of collaborative computing technologies across the Federal Government, including online meeting capabilities and an increased capacity for telework, will contribute to more efficient, effective service for the American people. Inter-agency collaboration will be enhanced as will the President's goal of opening governmental business to the public. Energy savings and environmental benefits will be important byproducts of reduced travel, and the Government will be better able to function smoothly in emergencies, as remote work capabilities are made more robust.

The Federal Government also is leveraging its buying power through the SmartBUY program, achieving cost savings through blanket agreements with commercial

Chart 9-1. Maturity of Segment Architectures -- Major Agencies (*)



(*) 86% of segments reported from major agencies.

software providers. The GSA manages the agreements and investigates new programs.

Federal Enterprise Architecture (FEA). Working cooperatively with agency CIOs, the FEA program helps agencies to improve their enterprise architectures. These architectures describe the agency mission and the resources needed to achieve satisfactory program performance and/or cost savings. The Federal architecture needs to mature through the definition, development, and implementation of segment architectures. In February 2009, major agencies identified a total of 566 discrete segments in varying levels of maturity ranging from Completed, In-progress, Planned, or Notional.

A "segment" is a discreet portion of an overall enterprise, whether mission critical (e.g., law enforcement), business services (e.g., financial management) or an infrastructure-related segment. By focusing on priority segments, agencies should produce actionable architectures that improve performance, reduce redundancies and costs, improve information sharing, and streamline business processes.

The National Information Exchange Model (NIEM). NIEM is designed to develop, disseminate, and support enterprise-wide information sharing standards and processes across the justice, public safety, emergency and disaster management, intelligence, and homeland security enterprise at all levels and across all branches of Government. Currently, 42 States have adopted NIEM, mostly in law enforcement and justice-orientated applications. It is anticipated that all 50 States will participate in NIEM in less than 18 months. Due to the success of NIEM with state and local justifications, the program has been adopted by the Program Manager for the Information Sharing Environment (PM-ISE) as the basis for its work to promote law enforcement, homeland security, and counter-terrorism information sharing. The collaboration and extension of the NIEM environment

demonstrates significant progress for standardized, reusable information exchanges across Federal agencies.

OVERVIEW OF FEDERAL IT SPENDING

The Fiscal Year 2010 estimate of total Federal IT spending represents a more complete accounting of IT investments than presented in previous Budgets. The most current 2010 estimate represents a seven percent increase from the 2009 Budget. Forthcoming agency summaries of IT spending will provide more complete information.

TABLE 9-2. FEDERAL IT SPENDING, BUDGETS OF 2008-2010 INCLUDING MAJOR FEDERAL IT INVESTMENTS
(investment counts, spending in millions of dollars)

	2008	2009	2010
Number of Major IT Investments	830	901	785
All IT Investments	6,267	6,566	7,165
Major IT Investment Spending	35,510	36,746	40,587
All IT Investment Spending	66,405	70,716	75,829

New directions for Federal information technology in 2009, as well as final determinations on investments funded in the American Recovery and Reinvestment Act, mean that estimates for spending on IT systems over 2009-2010 will likely change as firm plans are made to address the Administration's goals of greater openness in Government, wider participation by citizens in Government, and a more collaborative, cost-effective Federal IT enterprise.

As final plans on new IT initiatives and investments funded by the Recovery Act are implemented, new oversight approaches will be introduced to see that Federal IT dollars are spent effectively. The need for more effec-

tive high-level engagement in early strategic planning processes across agencies, and early articulation of fundamental architecture and design considerations as part of planning decisions, will be expressed in new policies on the management of agency IT spending. These changes will be complemented by continued agency reporting on major project justifications and implementation, and improvements to the process for the Federal CIO to intercede where projects are not meeting initial objectives, in order to quickly implement remedial actions which are timely and appropriate.

CONCLUSION

The Administration will continue to work with agencies, Inspectors General, Chief Information Officers, the GAO, and the Congress to strengthen the Federal Government's

IT investment planning and project execution and provide accountability for spending on information technology. The President's 60-day review of all cyber-security activities within the Federal Government and a planned directive on Open Government are part of how the new Administration will seek to transform the management of Federal data and information systems.

The path forward for Federal IT will make the process of Government more transparent and accountable. At the same time, Americans will know that information technology investments by their Government are being leveraged to produce maximum value, and that the security of information systems nationally, and the privacy of Americans, are being protected. Strategic investments in IT are at the heart of the efforts to make Government services more effective, accessible, and transparent.