

United States Country Report

With a \$64 billion [IT budget for FY 2007](#), the U.S. government continues to support the 24 Presidential E-Government (E-Gov) initiatives—most of which have been absorbed into government programs—and has begun to focus on other issues, particularly those surrounding security and privacy and business transformation through consolidation of back office systems (the lines of business initiatives) and implementation of a governmentwide enterprise architecture.

The fiscal year 2007 budget represents a \$2 billion increase in funding for information technology (IT) investments over the fiscal year 2006 level. It includes a total of \$4.6 billion for health-related IT investment, a 5.3% increase over 2006; and a 21% increase for the Department of Homeland Security to improve its operational efficiencies—primarily to improve information-sharing within the department by optimizing office automation and infrastructure.

“This level of investment recognizes the importance of enabling information technology as a critical tool for improving service delivery and producing results for the American taxpayer,” Karen Evans, OMB Administrator for E-government and IT said when the budget was announced.

“E-Government is transforming and improving government service delivery to the citizen, by making more information accessible through common government-wide solutions and eliminating duplicate systems within agencies,” Evans said. “By building on the results of our work thus far, we can optimize taxpayers’ investment and deliver the service quality and efficiency they expect from their government.”

Following are the highlights of the U.S. E-Gov and IT activities for fiscal year 2006.

1. E-Gov Initiatives

In a January 6 report to Congress, the Office of Management and Budget (OMB) identified the benefits realized by the adoption and expansion of e-government principles and best practices in managing IT driven by the President’s Management Agenda’s priorities of making government more efficient, citizen-centered and electronic. Its report, entitled [Report to Congress on the Benefits of the President’s E-Government Initiatives](#), concluded that the government “is increasingly providing timely and accurate information to the citizens and government decision makers while ensuring security and privacy.”

Although the administration sought \$5 million to fund the E-Gov initiatives in 2006, Congress has limited that amount to \$3 million. Most funding for the E-Gov initiatives is contributed by the agencies that collaborate to manage them.

Federal agencies spent almost \$193 million on 30 presidential initiatives, according to the report. Five initiatives account for more than half of the spending. The Integrated

Acquisition Environment program tops the list with \$36 million. It is followed by E-Vital, Social Security Administration, \$21.1 million; Safecom, Department of Homeland Security, \$20.5 million; E-Travel, GSA, \$14.3 million; E-Rulemaking, EPA, \$12.7 million

The results reported by OMB include the following:

- **GovBenefits.gov** - GovBenefits.gov provides a single point of access for citizens to locate information and determine potential eligibility for government benefits and services. Currently, GovBenefits.gov is receiving more than 190,000 visits per month by citizens and, on average, is providing more than 128,000 referrals per month to agency benefits programs.
- **E-Rulemaking** - Since the initiative launched in 2003, over 1.6 million citizens have visited Regulations.gov to participate in the Federal rulemaking process. To date, more than 8.9 million rules and regulations have been downloaded by members of the public.
- **Grants.gov** - Grants.gov currently provides Federal grants-seekers with access to over 1,600 Federal grant programs and is the single access point for all grants offered by the 26 Federal grant making agencies. Of the 2,259 funding opportunities for discretionary Federal assistance in fiscal year 2005, 994 (44%) were available for electronic application submission via Grants.gov.
- **Recruitment One-Stop** – This initiative maintains the Federal online recruitment service, USAJobs.gov. USAJobs.gov receives over 240,000 visits daily from job seekers looking for information regarding career opportunities with the Federal government. Each month, over 100,000 resumes are created on USAJobs.gov.
- **E-Payroll** - To date, E-Payroll has completed the migration of 17 (of 24 planned) departments or agencies from legacy payroll operations to one of the four consolidated payroll service providers. Currently, more than 83% of Federal employees are serviced by one of the four E-Payroll providers.

Others of the E-Gov initiatives have also achieved results. For instance:

USA Services, the citizen-focused presidential E-Gov initiative managed by the GSA Office of Citizen Services and Communications that includes [FirstGov.gov](#), the U.S. Government's Web Portal, has taken many strides in the past year. [FirstContact](#), its multiple-award contract for contact center services was used to provide government information and contact points for the victims of the 2005 hurricanes and for Americans abroad affected by other disasters. USA Services also produced a [Tool Kit](#) that allows any government agency to quickly and accurately put the contract to use in an emergency. USA Services produced a set of recommendations for improving contact center customer service in a March [report](#).

USA Services has also established a [Web Manager University](#) to provide standardized training for content managers on Federal Web sites. One- and two-day courses are offered in topics such as usability, writing for the Web, and Web content management.

FirstGov.gov saw many improvements this year. Its search function was upgraded and expanded. FirstGov.gov searches now cover 40 million government documents and uses clustering technology to organize thousands of results into logical categories. FirstGov.gov also added new features, like podcasts, Really Simple Syndication (RSS) feeds and e-mail alerts when new content is added to the website.

FirstGov.gov also established a Web Solutions Task Order that enables agencies to obtain hosting and other Web services under a governmentwide acquisition contract. Initially, the Task Order will provide hosting and other web services for FirstGov.gov and the Small Business Administration's Forms.gov and Business.gov. Under a \$71 million spending limit, up to 25 other citizen-facing initiatives could use the task order during its five-year life.

The United States ranked first in the annual U.N. Global E-government Survey, largely because of the effectiveness of FirstGov.gov and other E-gov initiatives. The survey, published in December in the [Global E-Government Readiness Report 2005: From E-Government to E-Inclusion](#), ranked the 191 U.N. member nations on e-readiness, based on their websites, telecommunications infrastructure and human resource endowment. The U.N. report also favorably noted that the U.S. promotes language accessibility for Spanish speakers by providing a comprehensive [Spanish version](#).

2. Lines of Business Initiatives

The Lines of Business initiatives are aimed at achieving a widespread business transformation and significant cost savings by consolidating the back-office systems used by many different agencies using shared services providers. The Lines of Business activities identify common government-wide solutions to consolidate, standardize, and share services across multiple Federal agencies. The initiatives were described in a General Issue paper submitted at the 2005 ICA Conference, [The U.S. Line of Business Consolidation Initiatives](#).

Six of these lines of business initiatives are underway to a greater or lesser extent. They are:

- **Financial management** – Consolidating financial management systems
- **Human resource management** – Consolidating human resources services
- **Case management** – Sharing information for law enforcement and investigations and civil and criminal litigation
-
- **Grants management** – Providing a single “storefront” for Federal grants

-
- **Health information architecture** – Enabling governments to share health information
-
- **IT security systems** – Consolidation of common IT security processes and controls.

The Financial Management Line of Business is the most well-developed. Four agencies have been designated as Centers of Excellence to provide financial management services to the others. Agencies will continue to use their existing legacy systems for the remainder of their system life-cycle, but when an agency needs to replace or upgrade its financial management system, it will migrate to one of these service providers or a commercial provider. OMB envisions migration of all agencies being completed within 10 years.

OMB has issued draft [guidance](#) for migrating agencies. It offers a competitive framework, a template for migration project plan, change management best practices and a menu of services that financial-management shared-service providers can deliver. The Migration Planning Guidance aims to answer procedural questions and provide insight when agencies conduct competitions for financial-management services from a public or private shared-service provider.

Three new lines of business were introduced in the fiscal year [2007 Budget](#). They are under development and will be operational by fiscal year 2007. They are:

- **IT Infrastructure** - to further refine the opportunities for IT infrastructure consolidation and optimization and develop Government-wide common solutions. The Federal Government could potentially save between 16 percent and 27 percent annually on its IT infrastructure budget and between \$18 billion and \$29 billion over 10 years by taking a more coordinated approach to spending on commodity IT infrastructure, such as help desks, data centers, and telecommunications.
- **Geospatial** - to identify opportunities for optimizing and consolidating Federal geospatial-related investments to reduce the cost of Government and improve services to citizens through business performance improvements.
- **Budgeting** - to build toward a "budget of the future" employing standards and technologies for electronic information exchange to link budget, execution, performance, and financial information throughout all phases of the annual budget formulation and execution cycle.

3. Cyber-Security

Cyber Security has been a major concern this year, along with the physical security provided by personal identification cards required under Homeland Security Presidential Directive – 12 (HSPD-12) and the need to protect personally identifiable information

maintained by the government that was highlighted by the theft of personal data from government computers.

The Federal Information Security Management Act (FISMA), which was signed into law as part of the E-Gov Act of 2002, lays out the framework for annual IT security reviews, reporting and remediation planning for Federal agencies. It requires agency heads and inspectors general to periodically assess and report to OMB on the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency.

“Over the past year, agencies made steady progress in closing the Federal government’s information technology security performance gaps,” Karen Evans, OMB E-Gov and IT Administrator, reported to Congress. “Analysis of baseline performance measures indicates policy compliance improvements in a number of programs. However, uneven implementation of security measures across the Federal government leaves weaknesses to be corrected.”

The OMB report, [FY 2005 Report to Congress on Implementation of the Federal Information Security Management Act of 2002](#), reported that about \$5 billion of the \$62 billion spent on IT in 2005, was spent to secure systems. The report found progress in meeting several key security performance measures:

- Certifying and accrediting systems. The number of certified and accredited systems rose from 77% to 85%. At the same time, agencies reported a 19% increase in the total number of IT systems – from 8,623 in FY 2004 to 10,289 in FY 2005.
- Assigning a risk impact level. The overall certification and accreditation percentage for the 1,941 high-impact systems was 88%, higher than the overall certification and accreditation average, showing that agencies are prioritizing their systems and working first to secure the systems presenting the highest risk impact level.
- Quality of certification and accreditation. Inspectors General reported the overall quality of the certification and accreditation processes at agencies increased with 17 of 25 agencies having a process in place rated as “satisfactory” or better, up from 15 agencies last year.
- Quality of agency corrective plans of action and milestone process. IG reports show that 19 of 25 agencies have effective POA&M processes, an increase from 18 agencies last year.

The [Federal Plan for Cyber Security and Information Assurance Research and Development](#) was issued by the National Science and Technology Council in the White House as the first step in developing a national R&D agenda for strengthening the security of the nation's IT infrastructure.

The plan presents a coordinated interagency framework for addressing critical gaps in current cyber security and information assurance capabilities and technologies by focusing on interagency R&D priorities that complement agency-specific efforts. It calls for concerted Federal activities on several fronts, as well as collaboration with the private sector.

The strategy includes findings and recommendations to guide cyber security R&D:

- Target Federal R&D investments to strategic cyber security and information assurance needs;
- Focus on threats with the greatest potential impact;
- Make cyber security and information assurance R&D both an individual agency and an interagency budget priority
- Support sustained interagency coordination and collaboration on cyber security and information assurance R&D;
- Build security in from the beginning;
- Assess security implications of emerging information technologies;
- Develop a roadmap for Federal cyber security and information assurance R&D;
- Develop and apply new metrics to assess cyber security and information assurance;
- Institute more effective coordination with the private sector; and
- Strengthen R&D partnerships, including those with international partners.

The top technical and funding priorities listed in the plan include authentication, authorization, and trust management; access control and privilege management; attack protection, prevention, and preemption; wireless security; and software testing and assessment tools.

Federal Information Processing (FIPS) Standards, minimum security requirements for Federal information and information systems have been established by the National Institute of Standards and Technology (NIST), which published them in several publications:

- The first, FIPS Publication 199, [Standards for Security Categorization of Federal Information and Information Systems](#), was issued in February 2004. It set standards for categorizing IT systems as low, moderate or high-impact depending on the effect of a system's loss of confidentiality, integrity or availability

- FIPS Publication 200, [Minimum Security Requirements for Federal Information and Information Systems](#), was issued in March. Its requirements are designed to protect the confidentiality, integrity and availability of Federal information systems, and the information processed, stored and transmitted by those systems.

Information Security Performance Metrics. NIST also released a draft of its [Guide for Developing Performance Metrics for Information Security \(SP 800-80\)](#), which provides a methodology for linking agencies' IT security program performance to agency performance, "tying information security controls, implementation, efficiency and effectiveness to an agency's success in its mission-critical activities."

Along with two other NIST publications, [Security Metrics Guide for Information Technology Systems \(SP 800-55\)](#) and [Recommended Security Controls for Federal Information Systems \(SP 800-53\)](#), it will help agencies comply with the Federal Information Security Management Act (FISMA).

4. Identity Management: Homeland Security Presidential Directive 12 (HSPD-12)

What has been termed "the biggest governmentwide technology mandate ever" takes effect by the end of October, and Federal agencies are working hard to acquire the equipment and software and to develop the procedures necessary to meet the deadline.

The White House issued [Homeland Security Presidential Directive 12 \(HSPD-12\)](#), *Policy for a Common Identification Standard for Federal Employees and Contractors*, in 2004 requiring all agencies to provide secure and reliable forms of identification for federal employees and contractors to use in gaining access to Federal buildings and computer systems.

The credentials must carry a digital unique identification number, scanned fingerprint data protected by a personal identification number that employees would memorize, and a digital certificate guaranteeing the card's authenticity.

The ID cards must be "interoperable"—that is, the ID readers at one agency should be able to read credentials issued by other agencies if authorized. Card issuance systems must meet governmentwide standards.

[OMB](#) requires implementing the HSPD-12 policy by October 27, 2007, but all agencies must have systems in place by October 27, 2006 for issuing compliant credentials for all new Federal employees and contractors. Federal Information Processing Standard (FIPS) 201, entitled [Personal Identity Verification of Federal Employees and Contractors](#), sets minimum requirements for common identification, security and privacy, and detailed specifications to support government-wide technical uniformity and interoperability. It specifies that by October 27th:

- All departments and agencies must issue interoperable biometrically encrypted ID credentials for new employees and contractors.

- All Federal agencies must begin conducting background investigations for all current employees not already investigated. (Investigations of current employees or contractors must be completed by October 27, 2007, except for those who have been employed more than 15 years. They are allowed another year, until October 27, 2008.)
- All departments and agencies must begin deploying products and operational systems that meet the HSPD-12 requirements. Federal [policy](#) requires the acquisition of only approved products and services that meet the standard. GSA, the executive agent for government-wide acquisition of information technology, will ensure that approved suppliers provide compliant products and services and make them available to all Federal agencies.

Once the presidential directive is fully implemented, government departments and agencies will be able to issue, recognize and accept identity credentials for their employees and for contractors who require long-term access to government-controlled facilities and information systems. Eventually, anyone who works in a Federal agency will require the new identification.

Federal-State Interoperability. State and territorial homeland security directors identified “interoperable communications for first responders” as the top homeland security issue for their states. In a [survey](#) conducted by the National Governors Association Center for Best Practices, 83% of the 55 officials named interoperability, for the second consecutive year.

Two kinds of collaborative efforts—coordinating the efforts of state and local agencies and developing a “fusion” center for intergovernmental development of intelligence—were second highest priority. Each received 70% of the mentions. The remaining choices were: identifying and protecting critical infrastructure (55%); planning for a possible influenza pandemic (43%) and improving preparedness for and response to natural disasters (40%).

5. Privacy: Protection of Personally Identifiable Information

In the wake of the theft of a government laptop containing data on millions of veterans and active duty military personnel (which was later recovered intact) and other breaches of data security by Federal agencies, the government is moving aggressively to safeguard personally identifiable information.

After discovery of the theft of the laptop from the house of an employee who had been permitted to take home the data on 26.5 million veterans and work on it there, the employee and his supervisors were disciplined, and privacy safeguards were strengthened governmentwide.

OMB tightened its [guidance](#) for agencies to review and report on their privacy policies and procedures by requiring that agencies report all incidents involving personally identifiable information within one hour—whether the breach is electronic or physical in form, confirmed or only suspected.

[An earlier directive](#) called on all agencies to properly safeguard their information assets using a checklist developed by the National Institute for Standards and Technology (NIST). It directs agencies to take specific actions to protect high- or moderate-impact personally identifiable information:

1. Confirm identification of personally identifiable information protection needs;
2. Verify adequacy of organizational policy;
3. Implement protections for personally identifiable information being transported and/or stored offsite; and
4. Implement protections for remote access to personally identifiable information.

All Federal agencies were also urged to take the following actions to tighten security:

1. Encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by [the] Deputy Secretary or an individual he/she may designate in writing;
2. Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access;
3. Use a “time-out” function for remote access and mobile devices requiring user re-authentication after 30 minutes inactivity; and
4. Log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required.

6. Enterprise Architecture

The Federal Enterprise Architecture Project Management Office in OMB has been working steadily to provide the tools and guidance for agencies to implement an enterprise architecture infrastructure to improve the efficiency and effectiveness of their programs. In the past year, the last of the five EA reference models, the Data Reference Model (Version 2.0), was published, and the EA was linked to the transition plan for IPv6, and

[***Data Reference Model Version 2.0***](#) is a framework whose primary purpose is to enable information sharing and reuse across the Federal government via the standard

description and discovery of common data and the promotion of uniform data management practices. It provides a standard means by which data may be described, categorized and shared, over three standardization areas:

- **•Data Description:** Provides a means to uniformly describe data, thereby supporting its discovery and sharing.
- **•Data Context:** Facilitates discovery of data through an approach to the categorization of data according to taxonomies. Additionally, enables the definition of authoritative data assets within a COI.
- **•Data Sharing:** Supports the access and exchange of data where access consists of ad-hoc requests (such as a query of a data asset), and exchange consists of fixed, re-occurring transactions between parties.

Federal Transition Framework provides guidance for agencies that are participating in a cross-agency project such as an E-Gov initiative or Line-of-Business consolidation. The FTF is a catalog of architectural information and implementation guidance for cross-agency initiatives using a simple, familiar structure aligned with the Federal Enterprise Architecture Reference Models. The FTF allows agencies to:

- Receive more consistent, complete and detailed information about cross-agency initiatives more quickly to inform their enterprise architecture, capital planning and implementation activities;
- Use information describing cross-agency initiatives to make better informed decisions about their IT investments; and
- Improve the effectiveness and efficiency of IT investments to realize service improvements and cost savings.

Federal Enterprise Architecture Security and Privacy Profile (FEA SPP) is a methodology for addressing information security and privacy from a business-centric enterprise perspective. Produced by the Federal Enterprise Architecture Program Management Office in OMB, this document integrates the disparate perspectives of program, security, privacy and capital planning into a coherent process, using an organization's enterprise architecture. Enterprise architecture provides a common language for discussing security and privacy in the context of agencies' business and performance goals, enabling better coordination and integration of efforts. This document "fills the gap" between an agency's enterprise architecture and its system-level security and privacy activities.

To support that endeavor, the FEA SPP methodology:

- Promotes an understanding of an organization's security and privacy requirements, its capability to meet those requirements, and the risks to its business associated with failures to meet requirements;

- Helps program executives select the best solutions for meeting requirements and improving current capabilities, leveraging standards and services that are common to the enterprise or the Federal government as appropriate; and
- Improves agencies' processes for incorporating privacy and security into major investments and selecting solutions most in keeping with enterprise needs.

7. Internet Protocol version 6

Recognizing the limitations of Internet Protocol version 4 (IPv4), the set of rules computers use to communicate over the Internet, OMB is requiring all Federal agencies to upgrade and adopt IP version 6 (IPv6) by June 30, 2008. This transition is "essential to the continued growth of the Internet and development of new applications leveraging mobile Internet connectivity."

Transition Planning for Internet Protocol Version 6 (IPv6) transition guidance issued by the CIO Council, lays out the process for all agencies to follow to prepare for the future of networking and Internet technology by enabling their networks to support IPv6 addresses and data packets.

Agencies are required to ready their network backbone to transmit both IPv4 and IPv6 traffic, and support IPv4 and IPv6 addresses, by June 30, 2008. Agencies must be able to demonstrate they can perform at least the following functions, without compromising IPv4 capability or network security:

- Transmit IPv6 traffic from the Internet and external peers, through the network backbone (core), to the LAN;
- Transmit IPv6 traffic from the LAN, through the network backbone (core), out to the Internet and external peers; and
- Transmit IPv6 traffic from the LAN, through the network backbone (core), to another LAN (or another node on the same LAN).

The requirements for June 30, 2008 are for the network backbone (core) only. IPv6 does not actually have to be operationally enabled (i.e. turned on) by June 30, 2008. Agencies had to meet 2006 deadlines to develop a transition plan, a transition impact analysis and an inventory of IP-aware applications and peripherals with dependencies on network backbone.

8. PART: Online Agency Performance Assessments

To maximize the transparency of Federal agency performance, OMB has launched a website, www.ExpectMore.gov, where performance assessments of nearly 1,000 Federal programs are posted online where the public can review them.

The assessments are based on the Program Assessment Rating Tool (PART), a standard questionnaire with approximately 25 questions about a program's performance and management. The answers determine an overall rating of how well a program is performing.

Programs that are performing are rated Effective, Moderately Effective, or Adequate. Programs categorized as not performing are rated Ineffective or Results Not Demonstrated. Programs rated Ineffective have been unable to achieve results due to a lack of clarity regarding the program's purpose or goals, poor management, or some other significant weakness. A rating of Results Not Demonstrated (RND) indicates that a program has not been able to develop acceptable performance goals or collect data to determine whether it is performing.

All assessed programs are held accountable for having an action plan to improve their performance and management. However, sometimes a program assessment finds that a program is duplicative of other, better-run programs, or that the program has already achieved its original purpose. In these cases, the action plan might be to work with Congress to terminate the program.

Conclusion:

Phase I of the President's E-Gov initiatives—the original 24 E-Gov initiatives—has essentially become “the way we do business.” Phase II—effecting cost savings and business transformation through the consolidation of back office systems—is well underway. The nine Line-of-Business initiatives promise to deliver great efficiencies and cost savings well into the billions. At the same time, the role of IT officials is becoming increasingly critical to the effective functioning of government, and new initiatives designed to improve security, prevent breach of privacy, protect IT investments, support homeland security and ensure unfettered U.S. access to the Internet have become high-profile, high-priority programs for the Federal government, and other governments in the U.S.