9. INTEGRATING SERVICES WITH INFORMATION TECHNOLOGY

As one of the largest users and acquirers of data, information and supporting technology systems in the world, the United States Government will continue its efforts to strengthen its capabilities in managing technology and information in order to be the world's leader in information technology. This year, the President proposes to spend about $65 billion for Information Technology (IT) and the associated support services. Departments and agencies continue to build upon their successes including their efforts with portfolio management by applying the principles and methods of Earned Value Management (EVM) to achieve greater savings, better results and improved customer service levels.

ACHIEVING RESULTS FOR THE AMERICAN PEOPLE

The Federal government continues to make progress by maximizing its, IT investments to deliver program results through the adoption of electronic government management principles and best practices. Departments and agencies continue to focus on:

- Improving service levels to citizens and government decision makers;
- Making better purchasing decisions;
- Securing our systems and data; and
- Reducing duplication and related costs.

This Budget chapter and Table 9–1, "Effectiveness of Agency's IT Management and E-Gov Processes," included on the CD–ROM, fulfill the statutory reporting requirement of the Clinger-Cohen Act of 1996. Other management guidance provided to Federal departments and agencies is included on Table 9–2, "Management Guidance," and is available at *www.whitehouse.gov/OMB/memoranda.*

Government Performance.—The Federal government has shown improvement over the last year in achieving the goals specifically included in the President's Management Agenda, the Expanded Electronic Government (E-Government) initiative. For example, each IT investment must have specific performance targets tied to a specific, significant, beneficial impact for our citizens. Performance functions must be defined, valued and deliver measurable results.

The Federal departments and agencies continue to improve in their efforts to guarantee the success and results for the taxpayer. There were 263 major investments representing about $10 billion on the "Management Watch List," i.e., those IT investment justifications needing improvement in performance measurement, earned value management or system security. Before the start of the fiscal year, agencies were directed to remediate the shortfalls identified prior to expending additional funds. The agencies have worked to remediate the weaknesses or have put measures in place to monitor the progress of the IT investment which could include multiple projects. If an investment is still on the "Management Watch List," agencies must describe their plans to manage or mitigate risk before undertaking or continuing activities related to that investment. As of December 31, 2006, 81 percent of the agencies (22 of 27) had all acceptable FY 2007 business cases. Thus, remaining on last year's Management Watch list, there were 84 business cases valued in FY 07 at $4.3 billion from five agencies. This year, 346 of the 840 FY 2008 major IT investments are on the "Management Watch List." These investments still need to address performance measures, implementation of earned value management, security or other issues before obligating funding in Fiscal Year 2008. See Table 9–3, "Agencies with IT Investments on the Management Watch List."

The Report on Information Technology (IT) Spending for the Federal Government (Exhibit 53) will be published in the spring of 2007 and is located at *www.whitehouse.gov/OMB.* It provides details of the Administration's proposed 2008 IT investments. Related documents on IT security and Electronic Government (E-Government) are also available at *www.whitehouse.gov/OMB.*

Fiscal Year 2008 proposed IT investments were analyzed for trends and potential duplications across government entities. At about $65 billion, the Fiscal Year 2008 Federal IT portfolio represents a 3 percent increase over Fiscal Year 2007 President's Budget. The following represents the highlights:

	FY 2006	FY 2007	FY 2008	Percent [1] Change
Major IT Investments	1,087	857	840	–2%
Not Well Planned and Managed	358	263	346	32%
Well Planned and Managed	682	594	494	–17%

[1] Change from FY 2007 to FY 2008.

The decreasing number of major IT investments is attributed to departments and agencies better managing their Capital Planning and Investment Control (CPIC) process in conformance with their enterprise architectures. The continued maturation of the CPIC processes provide for greater oversight and evaluation of the investments achieving and/or addressing intended results by departments' and agencies' Chief Information Officers. This oversight and understanding allows for changes in the IT portfolio to address mission

priorities, consolidation and elimination of redundant investments.

With the Administration's focus on achieving program results, the department and agencies partner with OMB to identify high-risk projects (those IT projects requiring special attention from oversight authorities and/or the highest level of agency management) and report on the agreed upon list of projects quarterly to OMB. As a result, oversight authorities and agency management now have available quarterly data on the progress of these projects to ensure improved execution and performance. OMB is working with departments and agencies to implement corrective action plans in cases where a project did not meet one or more of the four principle criteria. Additional information about high-risk projects including agency performance for FY07Q1 can be found at: *www.whitehouse.gov/omb/egov/b-1-information.html#io.*

When duplication across Federal agencies has been identified, the Administration has an ongoing process to bring together the appropriate agencies and help them to consider broad-based approaches to promote inter-agency data sharing and cooperation in building common solutions, rather than maintaining separate investments. Upon migration to common, government-wide solutions, agencies will shut down existing systems—which will not only save money but also free-up resources for agencies to better focus on achieving their missions. These inter-agency taskforces focus on the agency Lines of Business (LoB) rather than a specific technology or investment. The following are the current LoB initiatives underway:

- Case Management;
- Federal Health Architecture;
- Financial Management;
- Human Resources Management;
- Grants Management;
- Information System Security;
- Budget Formulation and Execution;
- IT Infrastructure; and
- Geospatial.

The inter-agency taskforces have driven significant accomplishments for each LoB initiative. The Information System Security (ISS) LoB evaluated agency proposals to become shared service centers in the areas of security awareness training and Federal Information Security Management Act (FISMA) reporting. On the basis of the evaluation and recommendations, the following agencies were selected to be the initial shared service centers:

- Security Awareness Training:
  —Office of Personnel Management
  —Department of State/United States Agency for International Development
  —Department of Defense
- FISMA Reporting:
  —Environmental Protection Agency
  —Department of Justice

Accomplishments of this LoB and the remaining LoB initiatives as well as the next steps are included in Table 9–5, "Lines of Business (LoB) Update."

The Administration continues to leverage government buying power while reducing redundant purchases through the SmartBUY program. Launched in June 2003, the SmartBUY program continues to provide increased cost avoidance savings to federal agencies through new and existing agreements with commercial software providers. In FY 2006, the Federal Government has achieved cost avoidance of over $300 million for the Oracle agreement alone. The SmartBUY Office located at the General Services Administration (GSA) continues to manage a total of nine agreements. In December 2006, the Administration established an agreement with the first of several Antivirus software developers with projected cost avoidance of as much as $18 million annually compared with the current best pricing available on GSA schedule and projected agency buying patterns. SmartBUY will continue to identify and develop new agreements throughout the year. In particular, SmartBUY will pursue a multiple award agreement in support of OMB policy memorandum, M-06–16, "Protection of Sensitive Agency Information," which would include data at rest and remote access.

Government IT Workforce.—With rapid advances in IT, improved program performance is first and foremost driven by the Federal employees who manage the IT projects and portfolios. Qualified project managers and an IT workforce with the necessary skills and competencies help ensure agency investments are well planned and managed. In 2005, agencies submitted plans to OMB for closing critical IT skill and competency gaps. Progress against these plans is measured and included in the President's Management Agenda Human Capital Scorecard. As of September 30, 2006, out of the 26 scorecard agencies:

- 17 agencies (65 percent) have met all planned skill or competency gap closure milestones; and
- 15 agencies (58 percent) have met or are consistently meeting their IT hiring targets.

The table below provides a summary of agency progress toward hiring goals.

Job Area	Fiscal Year 2006—Total Number of Current Positions [1]	Number of Vacant Positions Agencies Planned to Fill by the End of Fiscal Year FY 2006
IT Project Management	4,619	600
IT Security	9,030	488
IT Architecture (Enterprise)	1,169	180
IT Architecture (Solutions)	942	148
Total	15,760	1,416

[1] As of date agencies reported to OMB.

Agencies have also made progress in assignment of project managers to major IT investments. As reported by agencies on their FY 2008 Exhibit 53 submissions, 83 percent of major IT investments have qualified project managers, an increase from approximately 70 percent in agency FY 2007 submissions.

Going forward, agencies are completing a new IT Workforce Assessment Survey developed and administered by the Chief Information Officers (CIO) Council. The survey collects information from Federal IT professionals about the types of work they perform, as well as their level of proficiency in competencies and skills. The survey also identifies top training needs; gathers information on the types of certifications owned by employees; and provides key demographic data. Using the survey results, agencies will prepare a gap analysis report and improvement plan. OMB will be working in conjunction with OPM and the CIO Council to review the survey results as well as the agency plans to address identified gaps.

Securing Government Systems.—The Federal government continues to improve information security performance; however, declines in a few agencies have resulted in a net decrease in overall performance in some areas. Additionally, aspects of IT security such as securing data on removable media remain under addressed government-wide. Departments and agencies progress against their corrective actions plans will be measured in the President's Management Agenda Expanded Electronic Government Scorecard. On balance, the majority of agencies continue to improve or sustain high performance. Agencies report quarterly on their efforts to address IT security weaknesses against key IT security performance measures.

The 2006 agency FISMA reports reveal continued progress in the area of system certification and accreditation. In FY 2006, the percentage of certified and accredited systems rose from 85 percent to 88 percent, despite a 3 percent increase in the total system inventory to 10,600 operational systems. A few larger agencies made exceptional progress in closing the gap on certification and accreditation and testing of security controls and contingency plans. The State Department and Department of Homeland security both more than doubled their percentage of secured systems. Several departments achieved impressive increases in the percentage of systems with tested security controls and/or contingency plans, most notably Homeland Security, the Department of Housing and Urban Development, the Department of Defense, Department of Energy, Education, and the General Services Administration.

Overall quality of the certification and accreditation processes as determined by agency Inspectors General (IG) decreased slightly compared to 2005, with 60 percent of agencies reporting "satisfactory" or better processes. Over 72 percent of agencies can demonstrate they have an effective process in place for identifying and correcting weaknesses, a slight decrease from 2005.

The overall security status and progress in percentage of systems, from FY 2002 to FY 2006, is as follows:

(In Fiscal Years)

	2002	2003	2004	2005	2006
Effective Security and Privacy Controls (C&A)	47%	62%	77%	85%	88%
Tested Contingency Plans	35%	48%	57%	61%	88%
Tested Security Controls	60%	64%	76%	72%	77%
Total Systems Reported	7,957	7,998	8,623	10,289	10,600

The number of agencies where the IG has verified the process exists to remediate IT security weaknesses (Plan of Actions & Milestones):

FY 2002	N/A (was not required in until FY 2003)
FY 2003	12
FY 2004	18
FY 2005	19
FY 2006	18

Government-wide, incremental progress in resolving fundamental IT security weaknesses has been made in many aspects of information security; however departments and agencies must continually assess the risks associated with technological developments and service offerings. Thus, each year brings new challenges and approaches, and potentially new measures for performance. Additional information and detail concerning the Federal Government's IT security program and agency IT security performance can be found in OMB's Annual Report to Congress on IT Security. The next such report will be issued by March 1, 2007, and will be made available on OMB's website.

Protecting Privacy.—In 2006, several agencies experienced high profile data security breaches involving personal information. Most notable of these was the Department of Veterans Affairs, but significant problems also exist at other departments and agencies. Virtually all of these incidents resulted from "internal" problems within agencies and not external attacks on agency systems.

To help address this issue, in May 2006, the President signed an Executive Order creating the Federal Identity Theft Task Force. Several of the Task Force's interim recommendations address the need to improve data security in the government, improve the agencies' ability to respond to data breaches, and reduce the risk to personally identifiable information.

In this context, OMB has issued four security and privacy policy and advisory memoranda. These memoranda reemphasize agency responsibilities under law and policy regarding protection and safeguard of sensitive personally identifiable information, including information accessed through removable media, and incident reporting. They are included in Table 9–2, "Management Guidance," and are available at: *www.whitehouse.gov/OMB/memoranda.*

To help ensure safeguard of personally identifiable information, agencies are required to report on several performance metrics related to information privacy. Additionally, this year agencies were also required to provide quantitative performance measures to assess the privacy of agencies' personally identifiable information. The FY 2006 agency FISMA reports reveal modest suc-

cess in meeting several key privacy performance measures:

- *Program Oversight.* In 2006, the majority of agencies report having appropriate oversight over their privacy programs in place. All agencies report having a privacy official who participates in privacy compliance activities, however, 84 percent report coordinated oversight coordination with the Office of the Inspector General (OIG). Most agencies report privacy training for Federal employees and contractors, with 92 percent reporting general privacy training and 84 percent reporting job-specific privacy training.
- *Privacy Impact Assessments.* In 2006, 82 percent of applicable systems government-wide have publicly posted privacy impact assessments verses the goal of 90 percent.
- *System of Records Notices (SORNs).* In 2006, 82 percent of systems government-wide with personally identifiable information contained in a system of records covered by the Privacy Act have developed, published, and maintained current systems of records notices verses the goal of 90 percent.

Initiative to Secure Federal Information Systems and Facilities.—Inconsistent agency approaches to facility security and computer security are inefficient and costly, and increase risks to the Federal government. On August 27, 2004, the President signed Homeland Security Presidential Directive (HSPD) 12, "Policy for a Common Identification Standard for Federal Employees and Contractors," which requires agencies to implement a mandatory, government-wide standard for secure and reliable forms of identification for Federal employees and contractors. In October 2006, agencies met the major milestone of their HSPD-12 implementation plans which was to begin issuance of compliant identification cards. During FY2007—FY2008, agencies are required to complete issuance of these IDs to all applicable employees and contractors and install infrastructure to use them.

Initiative for Improving Government Networking Capabilities.—In order for the departments and agencies to overcome technical limitations arising from this need to interoperate and support emerging requirements and technologies, the Administration set June 2008 as the date by which all agencies' infrastructure (network backbones) must be IPv6-capable. In August 2005, OMB issued guidance to agencies to ensure an orderly and secure transition from Internet Protocol Version 4 (IPv4) to Version 6 (IPv6). Since the Internet Protocol is core to an agency's IT infrastructure, in February 2006, the Administration began using the Enterprise Architecture (EA) Assessment Framework to evaluate agency IPv6 transition planning and progress. The agencies are responsible for a series of actions by specific dates. For instance, by June 30, 2006, agencies were to complete:

—an inventory of existing routers, switches, and hardware firewalls; and

—an impact analysis of fiscal and operational impacts and risks.

Agencies are required to submit status reports with their quarterly EA submissions showing progress against the agency-specific milestones detailed in their IPv6 transition plans.

To avoid unnecessary costs in the future, agencies are also required to the maximum extent practicable, to ensure all new IT procurements are IPv6 compliant. Any exceptions to the use of IPv6 require the agency's CIO to give advance, written approval. In support of this requirement, the National Institute of Standards and Technology (NIST) will release a standards profile. The profile will be released for public comment in January 2007.

Additionally, the President's National Strategy to Secure Cyberspace directed the Secretary of Commerce to form a task force to examine the most recent iteration of the Internet Protocol, IP version 6 (IPv6). The President charged the task force with considering a variety of IPv6-related issues, "including the appropriate role of government, international interoperability, security in transition, and costs and benefits." The task force, co-chaired by the Administrator of the National Telecommunications and Information Administration (NTIA) and the Director of the NIST, prepared a report discussing the benefits and impacts of IPv6. This report was published in January 2006.

Making Government Accessible to All.—The efficient, effective, and appropriately consistent use of Federal agency public websites is important to promote a more citizen centered government. Federal agency public websites are information resources funded in whole or in part by the Federal government and operated by an agency, contractor, or other organization on behalf of the agency. They present government information or provide services to the public or a specific non-Federal user group and support the proper performance of an agency function.

GSA's Office of Citizen Services and Communications manages the operations of FirstGov.gov and recently upgraded their search capability and changed its name to USA.gov in order to improve public access to Federal government information.

An interagency "web content" working group, sponsored by GSA, regularly hosts training for Federal agency webmasters and public affairs officers. Recent courses provided instructions for making agency websites more effective and relevant to popular search engines. Additionally, a web content working group maintains *www.webcontent.gov,* conducts interagency meetings to assist agencies in managing their websites, and exchanges best practices among other agencies. These activities support agency efforts to provide access to and dissemination of government information to the public. GSA plans to complete the online tutorial by April 2007. This service will complement other services at USA.gov and elsewhere to aid the public in locating government information.

SUCCESSFULLY USING ELECTRONIC GOVERNMENT

The departments and agencies continue to leverage information technologies to make government services available to citizens while ensuring security of those systems, the privacy of the citizen information and the prudent use of taxpayer money. E-Government is about providing direct and measurable results supporting departments' and agencies' mission and goals. For departments and agencies, the benefits will far outweigh the cost of implementation. Increased agency adoption and customer utilization will become the primary measures of success. The expanded availability of government information and the utilization of an increased percentage of transactions between the Federal government and citizens will be measured, where appropriate and made available on line at *www.egov.gov*.

Examples of how the tenets of E-Government are helping to deliver services to the citizen and make the government more effective include:

Department of Commerce. The Online Positioning User Service (OPUS) transforms how users of global positioning systems obtain highly accurate geographic coordinates and elevation data (see: *www.ngs.noaa.gov/OPUS/*). The system allows users, such as professional surveyors, to electronically submit geospatial information via the Internet to the Department, where data are processed to determine corresponding three-dimensional positional coordinates. As a result, the Department is able to provide access to and disseminate more accurate and quality geospatial information to the public. For example, construction, transportation, and mapping industries reduce surveying time and costs (estimated $270 million cost savings to the public) of creating specific maps and other products needed to operate their business to a fraction of those previously reported.

User forums and workshops to obtain feedback are held regularly across the country, and usage of the system has grown from 1,000 data submissions per month in 2002, to over 13,000 per month in 2006. Extensive interaction between the National Oceanic and Atmospheric Administration (NOAA) and system users takes place during these sessions, and NOAA is currently identifying and surveying representatives from individual counties to ensure their diverse needs are being met. Additionally, users can complete an online survey to provide the Department comments and suggestions on how to improve the system and related positioning products and services. OPUS users include more than 175 organizations, including other Federal agencies, state and local governments, universities, the private sector, foreign governments, and others who share the goal of making more accurate positioning available worldwide. Users without Internet access and those with disabilities can mail their GPS observations to NOAA on a compact disk and receive the results back via the same mechanism on a prearranged basis.

U.S. Department of Agriculture. The Animal and Plant Health Inspection Service (APHIS) launched its new electronic permitting system (ePermits) on April 3, 2006. The system allows customers to apply for a permit, check its status, and view it online. The ability to submit applications and receive permits via the Internet and in some cases the ability to pay applicable permit application fees online, saves customers and APHIS the time and effort associated with the paper-based process. Additional information on system features can be found on the Web site at *www.aphis.usda.gov/permits/*.

To successfully implement the system, USDA demonstrated a desire to team with customers, state officials, and peer agencies by facilitating outreach sessions and customer tests. USDA continues to maintain ongoing dialogue with system developers, users, partners, and stakeholders to plan and implement additional features. Customers without Internet access at their facility can still use the paper permit application process and USDA developed the system to be compliant with Section 508 of The Rehabilitation Act of 1998.

Previously, the permit processing workload was growing to become unmanageable with current staff and resources. By eliminating the cost of processing paper and automating the system, more efficiency will result, with benefits to the Federal Government, state governments, and the general public estimated at $1.2 million per year in the first full year of operating the system. APHIS estimated that when the system is fully deployed it will cut in half the time it takes to process applications to import enterable plants and timber when the applications are entered online. In addition, the system will make it more difficult to tamper with a permit because the system provides immediate access to information relating to applications and permits

The Administration continues the focus of the department and agency specific services movement to citizen-centered services. Overall funding for the President's E-Government initiatives has reduced annually since Fiscal Year 2004 as the initiatives have met their milestones and have become incorporated into the daily operations of Federal departments and agencies. This reduction has come as result of moving the initiatives to fee-for-service models where appropriate, thereby eliminating the need for agency contributions. Table 9–4, "Status of the Presidential E-Government Initiatives," included on the CD–ROM, provides an update for each project.

CONTINUING TO ACHIEVE RESULTS

The Administration will continue to use the Federal Enterprise Architecture data for business analysis to focus our efforts to direct information technology investments to improve service delivery to citizens and other

entities. The Administration will continue to improve performance and achieve results by continuing our efforts in linking IT investments to program performance as demonstrated by the analytical tool called the Program Assessment Rating Tool (PART).

In 2008 and beyond, the Federal government will continue to identify IT opportunities for collaboration and consolidation while improving services. Although the Federal government continues to improve, much more work is needed to better serve the citizen. Through the PMA, the Clinger-Cohen Act, the E-Government Act, FISMA, budget guidance and other management tools, the Federal government has the ability to be the best manager, innovator and user of information, services and information systems in the world. The Federal Government has huge potential and opportunities for growth and to ensure program success and results through the effective use of information technology. Each department and agency will leverage existing capabilities to the maximum potential while ensuring reliability, security, privacy and continuity of services. The institution of the management practices within each department and agency and throughout the government will ensure these results.