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 continues its efforts to strengthen its capabilities in managing technology and information in order to be the world's leader in information technology. The President proposes to spend nearly $71 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 continuing to focus on results by applying the principles and methods of Earned Value Management (EVM) to achieve improved customer service levels and greater savings.

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;
- Securing our systems and data;
- Making better purchasing decisions; and
- Reducing duplication and related costs.

This Budget chapter and Table 9–1, "Effectiveness of Agency's IT Management and E-Gov Processes," fulfill the statutory reporting requirement of the Clinger-Cohen Act of 1996. Table 9–1 and other tables referenced in the text are available on-line at *www.budget.gov* or on the CD–ROM with printed versions provided by the Government Printing Office. Other management guidance provided to Federal departments and agencies is included in Table 9–2, "Management Guidance," which accompanies this chapter, and individual guidance memoranda are 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 (PMA), for 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 with performance being defined to deliver measurable results.

The Federal departments and agencies continue to improve in their efforts to guarantee success and results for the taxpayer. There were 585 major investments representing about $27 billion on the "Management Watch List (MWL)," i.e., those IT investment justifications needing improvement in performance measurement, earned value management or system security. Before the start of each fiscal year, agencies are directed to remediate the shortfalls identified prior to expending additional funds. The agencies work to remediate the weaknesses or put measures in place to monitor the progress of an IT investment, which could include multiple projects. If an investment is still on the MWL agencies must describe their plans to manage or mitigate risk before undertaking or continuing development activities related to that investment. As of December 31, 2007, 52 percent of the agencies (14 of 27) had acceptable 2008 business cases. Remaining on last year's MWL, there were 134 business cases valued in 2008 at $8.6 billion from thirteen agencies. Table 9–3, "Management Watch List for FY 08," provides a listing of the 134 business cases by department and agency. The IT projects associated with these investments have been moved to the High Risk List. Table 9–4, "High Risk IT Projects as of September 30, 2007," is a complete listing to date of all High Risk IT projects being monitored by the Office of Management and Budget (OMB) and/or the departments and agencies.

This year, 585 of the 810 2009 major IT investments are on the MWL as of December 31, 2007. See Table 9–5, "Agencies with IT Investments on the Management Watch List." In the evaluation of the departments' and agencies' business cases, the following criteria were used for placing investments on the MWL [Table 9–6, "FY 2009 Exhibit 300 Evaluation Criteria," provides the explanation for numeric evaluation for the business cases]:

- Overall Evaluation of 30 or less;
- Security Evaluation of 3 or less;
- If any other evaluation element has a rating of 2 or less;
- Project Manager Rating mismatched between Exhibit 53 and Exhibit 300;
- Project Manager identified has not been validated as qualified for the Investment as identified on the Exhibit 53;
- Agencies failing to receive a "satisfactory" or better evaluation by the agency IG in their annual Federal Information Security Management Act (FISMA) reports due to OMB on October 1, 2007 for the quality of their C&A process;
- Agencies failing to receive a "satisfactory" or better evaluation by the agency IG in their annual

FISMA reports due to OMB on October 1, 2007 for the quality of their PIA process and the investment requires a PIA;

- The agency is currently red for the Cost/Schedule Performance element of the PMA E-Gov Scorecard; and/or
- Overall Consistency Issue.

OMB will release investments remaining on the MWL in the spring of 2008 for the quarter ending March 31, 2008. Departments and agencies have been provided the specific information regarding the weaknesses for their investments. Many of the investments still need to address security, performance measures, implementation of earned value management and other issues prior to obligating funding in 2009. Table 9–7, "Comparison of the Management Watch List by Fiscal Year," illustrates the analysis of total portfolio including the number of projects on the High Risk List. Table 9–8, "Number of Recurring Investments on the Management Watch List," includes by department and agency the same investments on the MWL since inception.

The "high risk list" approach is separate and distinct from the MWL since it presents oversight authorities with information differing in focus, timing and expected results. It is not designed to replace pre-existing oversight and internal agency processes, but rather to supplement and complement them. The objective of the analysis is to manage the risk associated with the IT projects each quarter to achieve the intended outcomes. Each quarter agencies evaluate and report to OMB on the performance of the high risk projects. These projects are considered *high*-risk, requiring special attention from the highest level of agency management and oversight authorities due to size, complexity, and/or nature of the risk of the project, but are not necessarily *at*-risk.

Unlike the MWL, the high risk list contains a mix of major and non-major systems, as well as discrete projects and programmatic activities. The criteria for inclusion on the high risk list include, but are not limited to: Major systems the agency or OMB deems to be high risk due to a variety of factors, such as:

- high cost;
- complexity;
- high profile political or citizen interest;
- cross-organizational or agency impact or interdependencies with other systems efforts;
- major systems on the MWL at the conclusion of the prior fiscal year and continuing to warrant heightened attention during project execution;
- major systems formally designated as an E-Government or Line of Business (LoB) Shared Service Provider;
- planned or underway E-Government initiative migration projects (which are removed upon completion);
- existing or legacy agency systems retiring once their functionality has been migrated to a common solution (also removed once retired); and

- Program or Program Management Office activities supporting government-wide common solutions.

OMB and agencies monitor the status of projects on the high risk list, and track their progress in establishing goals and performance against cost and schedule baselines.

The Report on Information Technology (IT) Spending for the Federal Government (Exhibit 53) located at *www.whitehouse.gov/OMB*, provides details of the Administration's proposed 2009 IT investments. Related documents on IT security and Electronic Government (E-Government) will also be available at *www.whitehouse.gov/OMB* and will be published in the spring of 2008.

The 2009 proposed IT investments were analyzed for trends and potential duplications across government entities. At about $71 billion, the 2009 Federal IT portfolio represents a 3.8 percent increase over the 2008 President's Budget. The following represents the highlights:

	FY 2007	FY 2008	FY 2009	Percent [1] Change
Major IT Investments	857	840	810	–4%
Not Well Planned and Managed	263	364	535	47%
Well Planned and Managed	594	494	275	–44%

[1] Change from 2008 to 2009.

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 line 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 IT Infrastructure (ITI) LoB puts in place a government-wide approach for measuring and optimizing agency infrastructures to enhance cost efficiency/service levels and better enable core agency missions and customer-centric services. The ITI LoB, with the assistance of industry experts, will provide tools and metrics for agencies to leverage in order to optimize their commodity infrastructure cost efficiency/service level metrics. The ITI

LoB will provide tools and metrics in the following areas:

- Desktop/Seat Management and Support;
- Data Centers; and
- Data Networks and Telecommunications.

Accomplishments of this LoB and the remaining LoB initiatives as well as the next steps are included in Table 9–9, "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. The SmartBUY Office located at the General Services Administration (GSA) continues to manage a total of twenty-five agreements within nine programs. In June 2007, SmartBUY awarded the 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. These agreements included the ability of the state, local and tribal governments to procure products leveraging the federal government's buying power and receiving reduced pricing to meet their needs. In October 2007, the Administration broadened the scope of the current SmartBUY agreements to offer cost savings to all U.S. Federal government agencies (including DoD) for volume purchases. This ensures optimal pricing and leverages federal purchasing power. To date, the Federal government has avoided and/or saved more than $600 million dollars ($133 million in 2007) through the use of this program.

In August 2006, OMB released Memorandum 06–22 (M–06–22), *Cost Savings Achieved Through E–Government and Line of Business Initiatives.* M–06–22 asked agencies to identify legacy investments impacted by agency use of an E-Gov or LoB initiative and develop baseline cost estimates for these investments. Going forward, it is expected agencies savings will be realized by the migration of functions from their legacy systems, which can be terminated, to government wide common solutions. Agencies were requested to measure actual costs for the identified investments on an ongoing basis to provide the basis for estimating these savings.

Based on agency-reported estimated costs for 2007 as compared to agency-reported actual costs for the 2007, estimated gross cost savings is approximately $508 million.

2007 Baseline Cost Estimate—Investments Impacted by E-Gov	2007 Actual Costs	2007 Gross Cost Savings
$7,331M	$6,823M	$508M

OMB is continuing to work with agencies to identify additional legacy investments impacted by E-Gov and LoB initiatives.

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 2007, an IT Workforce Assessment Survey was developed and administered by the Chief Information Officers (CIO) Council. Using the survey results, agencies prepared a gap analysis report and improvement plan which identified competencies for improvement, staffing targets, and milestones with specific dates to successfully reach targets established. Agencies submitted plans to Office of Personnel Management (OPM) in June 2007. Progress against these plans is measured and included in the President's Management Agenda Human Capital Scorecard. As of September 1, 2007, 24 of 25 scorecard agencies have IT professionals on board have:

- met planned skill or competency gap closure milestones; and
- met or are consistently meeting their IT hiring targets.

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

	Current Number of Positions Filled	Number of Positions Filled on June 30, 2008
Enterprise Architecture	1,673	1,670
Solutions Architecture	1,457	1,472
IT Security	8,407	8,449
IT Project Management	6,248	6,061
Total	17,785	17,652

Agencies have also made progress in assignment of project managers to major IT investments. As reported by agencies on their 2009 Exhibit 53 submissions, 88 percent of major IT investments have qualified project managers, an increase from approximately 83 percent in agency 2008 submissions.

Going forward, agencies will continue to carry out the actions in their IT gap analysis and improvement plans. In June 2008, agencies will submit a measured results report to OPM comparing projected goals established in 2007 to actual outcomes in 2008.

Securing Government Systems.—The Federal government continues to improve information security performance relative to certification and accreditation rates and testing of security controls and contingency plans. In 2007, the percentage of certified and accredited systems rose from 88 percent to 92 percent. Even greater gains were reported in testing of security controls— from 88 percent of systems to 95 percent of systems— and for contingency plan testing—from 77 percent to 86 percent. Several larger agencies reported especially notable progress regarding these measures, including the National Aeronautics and Space Administration

(NASA), the Department of State, Treasury, and the Department of Defense.

Agencies have also maintained or improved performance relative to Inspector General qualitative assessments of IT security processes. Overall quality of the certification and accreditation processes as determined by agency Inspectors General (IG) increased compared to 2006, with 76 percent of agencies reporting "satisfactory" or better processes, up from 60 percent the prior year. 76 percent of agencies also demonstrated they have an effective process in place for identifying and correcting weaknesses using Plans of Action and Milestone (POA&M) management processes.

Departments and agencies progress against their corrective actions plans is measured in the President's Management Agenda Expanded Electronic Government Scorecard. Agencies report quarterly on their efforts to address IT security weaknesses against key IT security performance measures.

The overall security status and progress in percentage of systems, from 2002 to 2007, is as follows:

(In Fiscal Years)

	2002	2003	2004	2005	2006	2007
Effective Security and Privacy Controls (C&A)	47%	62%	77%	85%	88%	93%
Tested Contingency Plans	35%	48%	57%	61%	77%	86%
Tested Security Controls	60%	64%	76%	72%	88%	95%
Total Systems Reported	7,957	7,998	8,623	10,289	10,595	10,304

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

FY 2002	N/A (was not required in until FY 2003)
FY 2003	12
FY 2004	18
FY 2005	19
FY 2006	18
FY 2007	19

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, 2008 and will be made available on OMB's website.

Protecting Privacy.—In May 2006, the President signed an Executive Order creating the Federal Identity Theft Task Force. The Task Force issued its strategic plan which was submitted to the President. It is available at *http://www.idtheft.gov.* Several of the Task Force's 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 continued to issue 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. In 2007's annual FISMA report, agency IGs also provided a qualitative assessment of the quality of the agency's Privacy Impact Assessment process. The 2007 agency FISMA reports no overall percentage improvement in meeting several key privacy performance measures:

- *Privacy Impact Assessments (PIAs).* In 2007, 84 percent of applicable systems government-wide have publicly posted privacy impact assessments verses the goal of 90 percent.
- *System of Records Notices (SORNs).* In 2007, 83 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.
- *IG assessment of Quality of agency PIA process.* In 2007, 76 percent of IG's rated the agency's PIA process as satisfactory or better. (Two agencies did not complete the assessment due to time constraints, as this metric was added to the annual report requirements only 2 months prior to the report due date.)

Though the overall percent of systems with PIAs and SORNs for those systems require one stayed the same in 2007's annual FISMA report compared to the 2006 FISMA annual report, it is important to note agencies have increased the number of systems identified as requiring PIAs and SORNS significantly, collectively by more than 500 and 700 systems respectively. Thus to maintain the overall percentage of completion despite a sizable increase in the inventory is indicative of continued progress.

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 issued Homeland Security Presidential Directive 12 (HSPD–12) titled, "Policy for a Common Identification Standard for Federal Employees and Contractors," to address the recommenda-

tion of the 9–11 Commission to improve the security of our 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. In October 2006, agencies met the major milestone of their HSPD–12 implementation plans to begin issuance of compliant identification cards.

As of September 2007, departments and agencies had issued HSPD–12 identity credentials to 1 percent of the total workforce. OMB issued additional instructions to improve public reporting of the federal government's progress towards our milestones. As of December 31, 2007, with more accurate reporting from the departments and agencies, the required background investigations for 56 percent of federal employees and 43 percent for contractors have been completed. In accordance with their HSPD–12 implementation plans, by October 27, 2008, agencies are expected to complete background investigations for all existing employees and contractors and have their infrastructure and capabilities in place so they are issuing credentials as standard business practice.

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. Since the publication of OMB guidance in August 2005, agencies have been working toward the demonstration of capability to route IPv6 packets within their respective network backbones, to meet the June 2008 mandate. At the same time, the National Institute of Standards and Technology (NIST) has been working toward development of a technical profile and testing infrastructure for longer term product compliance.

The NIST will release a standards profile in March 2008 which will become effective 24 months following its publication date. The profile is a forward looking planning tool for Agencies, IPv6 equipment suppliers, testing laboratories, test equipment suppliers and Accreditation bodies. Since it is vital to protect critical US infrastructure, the technical profile includes sufficient security requirements, including a specification for Network Protection Devices as a first barrier against unauthorized access, and also effective deployment of the latest IP Security (IPsec) specifications, to provide integrity and authentication. In addition, the Federal Acquisition Regulation Council is finalizing language linking identifiable compliant IPv6 products with acquisition regulations.

Making Government Accessible to All.—Agency public websites continue to provide citizens timely information and services. For example, General Services Administration's (GSA's) Office of Citizen Services and Communications manages the operations of USA.gov, which serves as a consolidated gateway to all Federal websites and the information they publish.

Providing access to government information helps ensure a well-informed citizenry, and promotes public participation in agency activities. An example is Regulations.gov, a government-wide website for rulemaking which facilitates public participation in the Federal regulatory process. Regulations.gov allows citizens, business and other government entities to easily find, view, and comment on Federal regulatory action. The portal allows the public to communicate with a wide range of government agencies whose regulations may affect their daily lives. The site acts as a mechanism for the public to have a voice in influencing upcoming Federal regulations.

An E-Rulemaking analysis of Regulations.gov projects the initiative will save the Federal government more than $100 million over a five-year period since agencies will not need to deploy or maintain duplicative electronic comment management systems.

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 continues to be measured. The expanded availability of government information and the utilization of an increased percentage of transactions between the Federal government and citizens is being measure and made available on line at http://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 State

Virtual Presence Posts

State's Virtual Presence Posts (VPPs) are an innovative approach to extend the reach of State Department diplomatic services and consular information to cities and populations not served by physical embassies and consulates. The VPPs use information technology to deliver services cost-effectively, without the risks and challenges of staffing additional overseas posts. Currently, 41 VPPs are in operation in all regions of the world. These VPP web sites are designed to serve both

local country residents and US citizens. VPP sites connect Americans and foreign nationals at the government to government, government to foreign national, and American citizen to foreign national levels. They provide a variety of services tailored to local requirements by the country team. These services usually include consular information, web-based engagement (through web chats and online forums) and other limited services.

State regularly tracks the activities of VPP and tracks the number of visits to each of these sites. The VPPs are a highly leveraged and cost-effective mechanism for promoting US interests and engaging local populations around the world. The Department's Human Resources Bureau estimates to maintain a single US Foreign Service Officer costs at least $1 million annually, including $400,000 for employee costs. Establishing a Virtual Presence Post (VPP), costs approximately $10,000 for the website, $1,000 for annual hosting, and approximately $10,000 for Embassy visits to that city.

The VPPs using web technologies assist those with visual or mobility disabilities to access USG information. VPP websites are section 508 compliant and are easily accessible from anywhere internet access is available; homes, public locations such as American Corners, Binational Centers and internet cafes. This wide availability can be especially helpful to those who face difficulties in traveling to the nearest embassy or consulate. While The VPP program has been managed through State's capital planning as a minor investment it is following State department's processes and procedures to ensure the VPP's deliver their intended benefits to the communities.

Department of Housing and Urban Development

National Housing Locator Service

When disaster occurs, emergency response agencies and staff need flexible, innovative tools to quickly address basic human needs such as housing, food, and medical services. The Department of Housing and Urban Development (HUD), in support of FEMA, State and Local Housing Authorities, and other First Responders, launched the intergovernmental National Housing Locator Service (NHLS) website in January 2007. The NHLS is an accessible, searchable, web-based clearinghouse of over 200,000 rental housing vacancies available nationwide for emergency use.

In less than a year, the NHLS has come to represent a new model for quickly developing information applications to address HUD's strategic requirements and allows HUD to interoperate easily with other government organizations. Prior to this solution, government housing agencies and first responders would manually, over the course of weeks, collect, compile, and verify vacancy information from multiple agency legacy systems and on-line sources one by one. With NHLS, there is now one streamlined business process supported by state-of-the-art technology delivering quality data, day or night.

The move to the NHLS citizen-centric, one-stop portal is transforming the housing locator process and is realizing cost savings through the efficiencies achieved by reducing the housing locator process from weeks to seconds. This modern approach to application development allows HUD to invest incrementally in the program, in response to real-world requirements that evolve quickly in step with the nation's disaster-response capabilities.

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 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. Chapter 9, Table 9–10, "Status of the Presidential E-Government Initiatives," provides an update for each project.

CONTINUING TO ACHIEVE RESULTS

In 2009 and beyond, the Federal government will continue to identify IT opportunities for collaboration and consolidation while improving services. The Federal government has huge potential and opportunities for growth and to ensure program success and results through the effective use of information technology. In the coming year, each department and agency will leverage existing capabilities to the maximum potential while ensuring reliability, security, privacy and continuity of services. Key milestones will be achieved by the departments and agencies to strengthen their information resources programs. The deployment of the Federal Desktop Core Configuration in conjunction with IPv6, optimization of infrastructure in particular limiting external access points (Trusted Internet Connections initiative) with authorized access to physical and logical systems (HSPD–12 credentials) are all being realized in 2008. The institution of the management practices along with the strengthened infrastructure within each department and agency and throughout the government will ensure these results. GSA in conjunction with OMB will work with the Chief Information Officers (CIO) Council and individual departments' and agencies' CIOs to put into place a program to assess the policy uptake. This program will assist the CIO to ensure clear results are being demonstrated to achieve the outcome of improved information assurance, optimization of resources and performance levels. By completing these initiatives, the departments and agencies will be able to continue to improve their program and mission delivery and evolve their services into the next generation, Web 2.0 services.