

FEDERAL
CHIEF INFORMATION OFFICERS
COUNCIL
TRANSITION GUIDE



JANUARY 2009

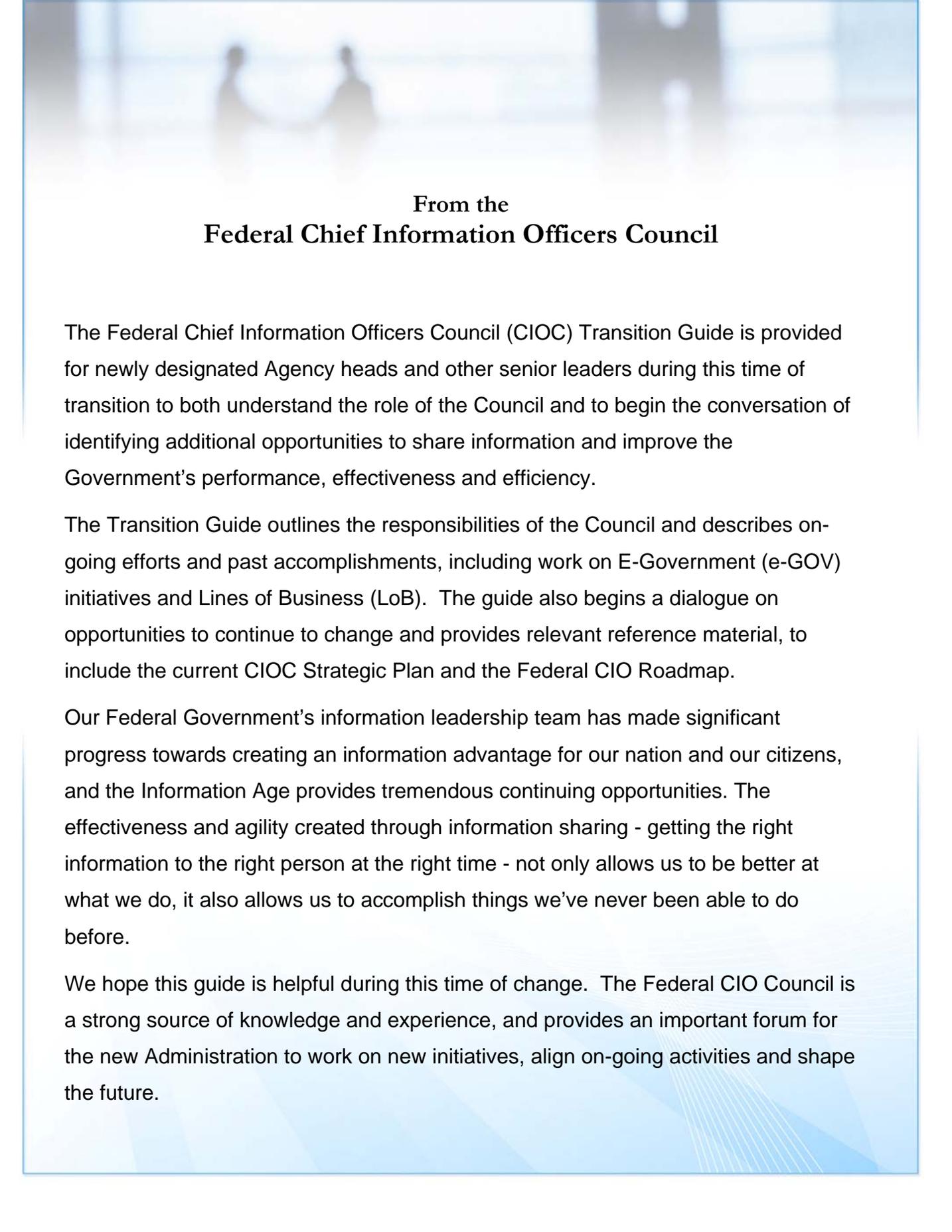
Federal Chief Information Officers Council – Transition Guide

Table of Contents

	<u>Page</u>
From the Federal Chief Information Officers Council.....	3
Introduction.....	4
Background.....	4
Role of the Federal CIO Council	4
E-Gov Initiatives and Lines of Business	6
Guiding Principles – Opportunities to Continue to Change.....	7
The Way Ahead.....	11

Appendices

Appendix A - Key Legislation.....	13
Appendix B - CIO Council Charter.....	15
Appendix C - Federal CIO Council Governance	19
Appendix D - Federal CIO Council Accomplishments.....	25
Appendix E - Federal CIO Council Strategic Plan.....	33
Appendix F - E-Gov and Lines of Business Initiatives	36
Appendix G - Federal CIO Roadmap	47



From the Federal Chief Information Officers Council

The Federal Chief Information Officers Council (CIOC) Transition Guide is provided for newly designated Agency heads and other senior leaders during this time of transition to both understand the role of the Council and to begin the conversation of identifying additional opportunities to share information and improve the Government's performance, effectiveness and efficiency.

The Transition Guide outlines the responsibilities of the Council and describes on-going efforts and past accomplishments, including work on E-Government (e-GOV) initiatives and Lines of Business (LoB). The guide also begins a dialogue on opportunities to continue to change and provides relevant reference material, to include the current CIOC Strategic Plan and the Federal CIO Roadmap.

Our Federal Government's information leadership team has made significant progress towards creating an information advantage for our nation and our citizens, and the Information Age provides tremendous continuing opportunities. The effectiveness and agility created through information sharing - getting the right information to the right person at the right time - not only allows us to be better at what we do, it also allows us to accomplish things we've never been able to do before.

We hope this guide is helpful during this time of change. The Federal CIO Council is a strong source of knowledge and experience, and provides an important forum for the new Administration to work on new initiatives, align on-going activities and shape the future.

Introduction

Today, we live in an information society – a world in which our ability to make decisions, our financial security and economic vitality, and our nation’s security are vitally dependent upon secure access to trusted information. Our ability to manage the nation’s information resources underpins all aspects of national life. Our government’s internal functions rely heavily upon seamless, trusted access to information. Information sharing must become the norm within individual agencies and across agency boundaries at the federal, state, and local levels. The citizens of the Nation look to their Government to provide electronic access to services and to use the power of information technology to operate effectively and efficiently.

The ever changing technological environment presents continuing opportunities for sweeping positive changes in how Federal Agencies can better serve the citizenry and the nation. The commercial world offers many new approaches with the potential to transform services and capabilities available to consumers. Unlike many solutions developed within the Government, these services have had their efficacy and responsiveness tested in the marketplace. These new technologies offer important potential for achieving a more citizen-centric Government if they are properly vetted and present a sound business case.

The Federal Chief Information Officers Council (CIOC) is focused on understanding the nature of this ever changing environment and harnessing the combined expertise that exists across the federal government to evaluate and implement new technologies. As a consequence, we will build and maintain a leadership position for our nation and our citizens in the information age. To transform the Federal government to one that is citizen-centered, results-oriented, and market-based, we are using a variety of initiatives, plans, policies, architectures, and assessments. This transition plan is provided to share information about our successes and to highlight issues that affect the power of information to safeguard American interests and improve Government’s performance, efficiency, and effectiveness.

Background

The CIO Council was established by Executive Order 13011, Federal Information Technology, on July 16, 1996 (now revoked), and then codified into law by Congress in the E-Government Act of 2002. The CIO Council serves as the principal interagency forum for improving practices in the design, modernization, use, sharing, and performance of Federal Government agency information resources. The Council's role includes developing recommendations for information technology and management policies, procedures, and standards; identifying opportunities to share information resources; and assessing and addressing the needs of the Federal Government's IT workforce. Appendix A provides a synopsis of key legislation governing the work of the CIO Council.

Role of the Federal CIO Council

The Federal CIO Council is charged with acting as the “... principal interagency forum for improving agency practices related to the design, acquisition, development, modernization, use, operation, sharing, and performance of Federal Government information resources.” In addition, the role of the Federal CIO Council is to improve government performance, effectiveness and

efficiency by proposing new ways to achieve the government's mission(s) by better use of enabling technology. More specifically, the Council is directed by the E-Government Act of 2002 [44 USC 3603(f)] to engage in seven activities:

- Develop recommendations for the Director of the Office of Management and Budget on Government information resources management policies and requirements
- Share experiences, ideas, best practices, and innovative approaches related to information resources management
- Assist the Administrator of the Office of Electronic Government in the identification, development, and coordination of multi-agency projects and other innovative initiatives to improve Government performance through the use of IT
- Promote the development and use of common performance measures for agency information resources management
- Work with the National Institute of Standards and Technology and the Administrator to develop recommendations on information technology standards
- Assess and address the hiring, training, classification, and professional development needs of the Government related to information resources management
- Work with the Archivist of the United States to assess how the Federal Records Act can be addressed effectively by Federal information resources management activities.

CIO Council Governance

The CIO Council serves as a focal point for coordinating challenges that cross agency boundaries and provides a number of opportunities for Federal CIOs to shape the Federal Government's information management and technology agenda. The Executive Chair of the CIO Council is the Deputy Director for Management for the Office of Management and Budget (OMB). The Director of the CIO Council is the Administrator, Office of eGovernment and Information Technology, Office of Management and Budget. The Vice Chair of the Council is elected by the CIO Council from its membership. Membership of the Council comprises the CIOs, Deputy CIOs and Chief Technology Officers (CTOs) from the Federal executive agencies as well as additional liaisons and ex officio members. A copy of the CIO Council Charter is provided in Appendix B.

The Council has a number of standing committees where CIOs and their staffs can work on important issues and initiatives. The governance structure has been designed to provide maximum flexibility to create committees as requirements and priorities change. Currently, the Council has five committees focused on the various functional priorities of information leaders:

- Architecture & Infrastructure
- Best Practices
- IT Workforce
- Privacy
- Information Security & Identity Management

Each of the committees has two co-chairs, selected from the Council membership. In addition to these five committees, there is also an Executive Committee, composed of the committee co-chairs and the Council's Director and Vice-Chair which focuses on the agenda for the Council and integrating and aligning the work of the various committees.

Additional details on the Council and its governance activities are provided in Appendix C. Highlights of CIOC accomplishments are provided in Appendix D.

Strategic Planning

The Council has an active strategic planning process, and is currently implementing its 2008-2009 CIOC Strategic Plan. The Plan documents a vision, mission, and goals (which are summarized below). For each goal, the plan provides a detailed description of the goal, defines relevant objectives, identifies major activities in pursuance of the goal along with associated timelines, specifies Key Performance Indicators, and identifies a relevant success story to provide a real-world context for the goal. The current plan was specifically timed to help sustain the Council through the transition to the new Administration and then provide the new Administration with the ability to begin work on new initiatives, goals, and objectives. A copy of the Federal CIO Council Strategic Plan is provided as Appendix E.

Strategic Plan Vision

A Federal Government that strategically, efficiently, and effectively uses IT to serve and protect our citizens.

Strategic Plan Mission

To foster the collaboration of Federal Government Chief Information Officers in strengthening Government-wide IT management practices.

Strategic Plan Goals

- A cadre of highly capable IT professionals with the mission-critical competencies needed to meet agency goals.
- Information securely, rapidly, and reliably delivered to our stakeholders.
- Interoperable IT solutions, identified, and used efficiently and effectively across the Federal Government.
- An integrated, accessible Federal infrastructure enabling interoperability across Federal, state, tribal, and local governments, as well as partners in the commercial and academic sectors.

E-Gov Initiatives and Lines of Business

Public law recognizes the value of the nation's information resources and assigns primary information management responsibility to the Office of Management and Budget (OMB) and Agency Chief Information Officers (CIOs). The Electronic Government (E-Gov) Act of 2002 [44 USC 3603(f)] stated that Government required strong leadership, better organization, improved interagency collaboration and more focused oversight to take full advantage of the improved performance achievable through Internet-based technology. It created two entities – the Office of Electronic Government in OMB and the Federal CIO Council – to achieve the goals of improving government performance and promote citizen-centric electronic government services and processes.

Electronic Government or “E-Gov” initiatives have been aligned to four key portfolios, Government to Citizen, Government to Business, Government to Government, and, Internal Efficiency and Effectiveness. E-Gov initiatives go through a process where they are assigned to managing partners, participating agencies are identified, policy and technical issues are resolved and progress is closely monitored. Over the past six years, many of the E-Gov initiatives have successfully completed this process – completed their initial implementation, have self-sustaining funding models and have implemented collaborative governance structures – and are now functioning as “business as usual” for the Federal Government. They include:

- GovBenefits.gov
- Recreation One-Stop
- IRS Free File
- GovLoans.gov
- USA Services
- E-Rulemaking
- Expanded Electronic Tax Products for Businesses
- Geo-Spatial One-Stop
- International Trade Process Streamlining
- SAFECOM
- Grants.gov
- Recruitment One Stop
- E-Records Management

In March 2004, OMB initiated a government-wide analysis of five (subsequently expanded to nine) Lines of Business (LoBs) supporting the President's Management Agenda goal to expand Electronic Government. Within each LoB, interagency taskforces examine business and information technology data and best practices. The goal of the effort is to identify opportunities to reduce the cost of government and improve services to citizens through business performance improvements. As in the case of the E-Gov initiatives, several of the LoBs have similarly reached a level of maturity where their efforts are now a part of normal operating procedures. They include:

- Financial Management
- Human Resources
- Grants Management
- Budget Formulation and Execution
- Geospatial
- IT Infrastructure

Detailed descriptions of E-Gov initiatives, implementation progress and performance results are provided to Congress in an annual report. The FY 2009 E-Gov Report to Congress will be completed in January 2009. Further descriptions of each of the E-Gov initiatives and Lines of Business can be found in Appendix F.

Guiding Principles – Opportunities to Continue to Change

The Federal CIO Council envisions a Federal Government that strategically, effectively and efficiently uses IT to serve and protect our citizens.

There are many significant opportunities to continue to use technology, information, and best practices to enhance our government’s ability to deliver services to the public in an efficient and responsive manner. These opportunities represent some guiding principles for the efforts of the Council and the Nation, and include:

- Empowering the Government through Information Sharing
- Protecting the Networks and Systems Required to Operate in the Information Age
- Tapping the Power of a Collaborative Citizenry
- Leveraging Scale-Economies and Combined Expertise to Achieve Best Practices and Act as an “Enterprise”
- Ensuring the Federal Government is an “Employer of Choice”
- Focusing on Environmental Responsibility

Empowering the Government through Information Sharing

The Information Age provides unprecedented opportunities to share knowledge across the world and make the intellectual capital of our organizations available to the people that need it, when they need it. CIOs across the federal government have been active in creating and encouraging an environment of sharing between agencies, trusted partners, industry, and citizens. The ability to share data is changing the way we execute our business processes:

- Sharing information has greatly enhanced situational awareness leading to better-informed decision makers at all levels of government.
- Facilitating an information-sharing culture fosters innovation and provides a forum for creative and collaborative work across the enterprise.
- Sharing across all levels of government allows for the elimination of unnecessary redundant systems and data, the adoption of best business practices and an engaged and informed citizenry.

Achieving an effective information-sharing environment requires many changes in the ways we do business, the ways we think about information and the ways we construct and configure our networks. We must be committed to fostering interagency interoperability that is a critical enabler to achieving an information sharing environment. Our challenge lies in developing incentives and mechanisms to accelerate the paradigm shift from protecting and guarding information to secure information sharing. Simultaneously addressing the needs for broader information accessibility, the privacy rights of citizens, and the security needs of the Nation will continue to be a challenge. It is clear though, that as organizations and individuals look at information opportunities first from a “need to share” rather than a “need to know” perspective, a more empowered and effective Government is achieved.

Protecting the Networks and Systems Required in the Information Age

Every day the nation’s economy and defense become more efficient as a result of the effective use of information technologies. However, this dependency also makes us increasingly more at risk in a world where the frequency and sophistication of attacks on our networks are ever growing – simultaneously attempting to deny our ability to use our information assets while placing sensitive information at risk.

Successfully ensuring information security has evolved as we move away from a world of local networks with security focused primarily on defending perimeters, to a world where access to the web is crucial. In the information age, our focus is now on maintaining the sustainability and

survivability of the Internet and global networks, while enabling people to find the knowledge they need, when they need it to get their job done.

The Council understands this growing concern and has established a committee of IT leaders to serve as a collaborative interagency executive level forum to improve the security of Federal networks and information. The Council does this by identifying high priority interagency information security and identity management initiatives that can be opportunities to develop recommendations for policies, procedures and standards to address these concerns, including:

- Ensuring the survivability, sustainability and resiliency of networks
- Implementing effective identity management
- Protecting the privacy of our people
- Focusing on “secure information sharing” where security controls ensure that individuals can gain access to the information that they need, when and where they need it – while also preventing unauthorized access to this information.

Tapping the Power of a Collaborative Citizenry

Web 2.0 technologies and services-oriented application approaches create rich media by integrating data sources and Internet-provided services. The interaction between the two enables organizations to create and manage business processes with greater flexibility and deliver new capabilities much more rapidly. Users can create enterprise “mashups” by collecting, assembling and sharing existing enterprise content to improve analysis, decision making, or transactional flows.

There's a fundamental change taking place, with a focus now on web services that can be rapidly developed and made available to the population. Over the past few years, we have increasingly leveraged shared services and Service Oriented Architecture (SOA). Instead of “pushing information out”, these approaches are creating an environment where users at any level can both “take what they need” and “contribute what they know.” This services-oriented environment can increase effectiveness and efficiency across Government, by giving all users access to the latest, most relevant and accurate information:

- Adopting web-based solutions for internal and outward-facing applications brings speed and agility to Government, and enables access to the right information at the right time, regardless of location, in order to accommodate unanticipated users, partners and events.
- Leveraging social network tools (such as MySpace, Facebook, YouTube, etc.) encourages collaboration across government agencies and with industry and citizens and significantly improves the Federal Government’s outreach efforts and ability to interact with the citizens of the nation.
- Providing citizens with greater transparency into government transactions and decision-making processes, creating confidence and ensuring a “voice of the customer” for Federal agencies.
- Migrating to the web provides for internal efficiencies for Government through collaborative service delivery, consolidations, shared service provisioning and the elimination of unnecessary duplication of effort.

Leveraging Scale-Economies and Combined Expertise to Achieve Best Practices and Act as an “Enterprise”

Over the last several years, great strides have been made in encouraging agencies to operate as a united Federal “enterprise.” As an example, efforts to exploit government purchasing power by using GSA-managed contracts (e.g., GWACs, Network Service contracts (i.e., Networx Universal, Networx Enterprise, Satcom II), SMARTBuy, Schedules 70 and 84), and other sourcing solutions have reduced costs, achieved more favorable licensing terms, and increased interoperability through greater standardization. There remain many untapped possibilities in leveraging the scale of the Federal Government enterprise. The effectiveness and efficiency gains of consolidating common functions, enables each agency to focus on their mission-unique requirements. The power of concepts such as performance-based contracting and managed services allow organizations to work more effectively with industry and non-traditional partners:

- Adopting cross-agency managed services solutions for enterprise IT infrastructure will ensure consistent and reliable services with a global reach as well as operational cost reduction. Moreover, these solutions provide better access to many data related capabilities.
- Providing massively scalable IT infrastructure for use by government agencies will enable the rapid delivery of new capabilities at dramatically reduced costs.
- Replacing individual agency large system acquisitions with enterprise services available to all reduces dependencies on proprietary solutions and increases incentives to provide capabilities to users across organizations.
- Expanding the use of pilots, prototypes and spiral development provides cost effective creation and deployment of new and unanticipated functions in response to dynamic mission environments.

Combining the expertise of industry and government will enable adopting best practices that:

- Leverage proven capabilities, such as cloud computing, to provide scalable, on-demand solutions for critical mission needs,
- Exploit best-in-class methods and approaches to improve efficiencies across the Federal government, and,
- Reward risk taking and innovation to generate and take advantage of new ideas and new ways of doing things; the end result being improved performance.

These efforts will require federal organizations to continue to work together in adopting common enterprise-wide solutions. Continued success will depend on strong leadership and establishing a climate of trust that will enable organizations to relinquish personal control and ownership of individual solutions.

Ensuring the Federal Government is an “Employer of Choice”

In order to facilitate change and create an information sharing culture, we must be positioned with the right mix of personnel with the skills necessary to meet both current and future mission requirements. Agencies will need to continue to provide continuous learning opportunities for current employees to gain new skills, while becoming an “employer of choice” for the “Net Generation” workforce. Agencies must embrace the use of Web 2.0 technologies to meet the expectations of the Net Generation. Future employees will not want to be relegated to consuming

web-based information, but rather will be accustomed to creating and producing content and then using and sharing it. In addition, the renewed emphasis on the importance of public service provides a golden opportunity to attract talented workers to find meaningful jobs within the federal service.

Focusing on Environmental Responsibility

Reducing our environmental footprint is an imperative both ecologically and financially. Green computing is synergistic with best practices such as cloud computing, consolidation of networks, collaboration, telework, etc. There is a tremendous opportunity for a positive environment impact through the more effective use of information technology.

“Gartner estimates that carbon dioxide emissions related to the operation of servers and PCs account for 0.75 percent of the annual global total, and that’s before factoring in emissions generated by cooling the boxes. Add to that the emissions generated by telecommunications networks, and IT’s contribution to the atmosphere’s greenhouse gas load is “probably in excess of 2 percent,” says Simon Mingay, research vice president with Gartner, adding that that’s “a big number for what is essentially a single device.” In fact, emissions tied to that device, the computer, are comparable to the level of greenhouse gasses being produced by all the world’s airplanes as they crisscross the skies above us.” (CIO Magazine - Why Green IT is Better IT, 28 March 07)

The Federal government can preserve the environment while improving service delivery by:

- Moving more rapidly towards cloud computing and virtual computing environments to consolidate and reduce hardware costs, optimize workloads, and increase IT flexibility and responsiveness.
- Advancing mobile computing and enhanced collaboration capabilities to enable teleworker contributions resulting in reduced emissions.
- Adopting energy efficient best practices to include benchmarking the environmental impacts and practices of other large organizations.

The Way Ahead

CIO Council Support of Agency CIO Transitions

One of the roles of the Federal CIO Council is to ensure that new federal CIOs quickly learn the challenges faced by information leaders in the federal government environment. The Council recognizes that the roles and responsibilities for Federal CIOs differ from those in the commercial sector. To address this need, the Council has implemented the Federal CIO Boot Camp for newly appointed CIOs and Deputy CIOs. The Boot Camp consists of a series of sessions addressing issues such as strategic planning, budget formulation and capital planning, program management and performance, security and privacy, information management, and working with Congress and OMB. The Boot Camp program also draws upon a network of senior information executives who have formerly served in senior government positions, to leverage their knowledge and expertise of government and technology management issues and share lessons learned. This networking experience also encourages team building and mentoring across the CIO community. A copy of the Federal CIO Roadmap which is distributed at the Boot Camp is provided as Appendix G.

Charting the Course

Federal CIOs and other information leaders have made significant progress towards creating an information advantage for our nation and our citizens. Living in the Information Age provides us with tremendous opportunities. The agility created through information sharing - getting the right information to the right person at the right time - not only allows us to be better at what we do, it also allows us to accomplish things we've never been able to do before. These same capabilities create new challenges to our safety and security that must be managed creatively, while protecting us.

Mass collaboration and social networking tools of the Web 2.0 world are changing so many aspects of our lives. In a world of wikis, blogs and social networks, organizational boundaries become permeable and new ideas plant the seeds of innovation and creativity. Using commercially available solutions and adopting industry best practices allows us to rapidly and effectively adopt these new capabilities and meet our emerging information technology needs. We must not overlook the ingenuity of the private sector and its commitment to efficiency and a sound environment and capitalize on those abilities by maintaining an open dialogue with industry and the citizenry. Our success in embracing these changes in the market place, adopting the way in which the "net generation" workforce gets work done, will go a long way towards ensuring our technology future – making the federal government an employer of choice for today's young people.

This is an extraordinary responsibility and a significant opportunity for all of us. There are many success stories, but there are still numerous opportunities for change, as we learn to work together as a single team across the Federal Government. The Federal CIO Council is a strong source of knowledge and experience, and provides an important forum for the new Administration to work on additional efforts to sustain alignment and shape the future.

Appendices

Appendix A - Key Legislation

- E-Gov Act of 2002
- Federal Information Security Management Act of 2002 (FISMA)
- Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA)
- Government Paperwork Elimination Act of 1998 (GPEA)
- Clinger Cohen Act of 1996
- Freedom of Information Act of 1996 (FOIA)
- Paperwork Reduction Act of 1995 (PRA)
- Federal Acquisition Streamlining Act of 1994, Title V (FASA V)
- Government Performance Results Act of 1993 (GPRA)
- The Privacy Act of 1974
- Records Management by Federal Agencies (44 U.S.C. Ch.31)
- Federal Depository Library Program Laws (44 U.S.C. Ch.19)

Appendix B - CIO Council Charter

AUTHORITY:

Originally established by Executive Order 13011 (Federal Information Technology) and later codified by the E-Government Act of 2002, the Chief Information Officers Council (the CIO Council) is the principal interagency forum to improve agency practices for the management of information technology. The CIO Council is one element of an interagency support structure established to achieve information resource management (IRM) objectives delineated in legislation including the E-Government Act of 2002 (Public Law 107-347), Government Paperwork Elimination Act (GPEA), Paperwork Reduction Act (PRA), Government Performance and Results Act (GPRA), and the Information Technology Management Reform Act of 1996 (ITMRA). The CIO Council is a forum to improve agency practices related to the design, acquisition, development, modernization, use, sharing, and performance of federal government information resources. The CIO Council will communicate its findings to the Office of Management and Budget and to other executive agencies.

PURPOSE:

The CIO Council shall perform functions that include the following:

- Develop recommendations for the Office of Management and Budget (OMB) on federal government information resources management policies and requirements
- Share experiences, ideas, best practices, and innovative approaches related to information resources management
- Assist the Administrator of the Office of Electronic Government and Information Technology (OMB) in the identification, development, and coordination of multi-agency projects and other innovative initiatives to improve federal government performance through the use of information technology
- Promote the development and use of common performance measures for agency information resources management under Chapter 36 and Title II of the E-Government Act of 2002
- Work as appropriate with the National Institute of Standards and Technology and the Administrator of the Office of Electronic Government and Information Technology (OMB) to develop recommendations on information technology standards developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3) and promulgated under Section 11331 of Title 40, and maximize the use of commercial standards as appropriate, including the following:
 - Standards and guidelines for interconnectivity and interoperability as described under section 3504
 - Consistent with the process under section 207(d) of the E-Government Act of 2002, standards and guidelines for categorizing federal government electronic information to enable efficient use of technologies, such as through the use of extensible markup language

Appendix B - CIO Council Charter (Continued)

- Standards and guidelines for federal government computer system efficiency and security
- Work with the Office of Personnel Management to assess and address the hiring, training, classification, and professional development needs of the related to information resources management
- Work with the Archivist of the United States to assess how the Federal Records Act can be addressed effectively by Federal IRM activities
- Seek the views of the Chief Financial Officers Council, Federal Acquisition Council, Chief Human Capital Officers' Council, Budget Officers Advisory Council, and other key groups of federal management and program officials, as well as industry, academia, and federal, tribal, and state and local governments, on matters of concern to the Council as appropriate

The CIO Council vision is to be a resource to help the federal government work better and cost less by promoting the efficient and effective use of agency information resources. The CIO Council supports business process reengineering, continuous process improvement, and measurable increases in employee productivity in the performance of work related to the achievement of agency objectives.

RELATIONSHIPS:

The CIO Council may nominate members to serve on related councils, such as the Chief Financial Officers Council (CFO-C), the Federal Acquisition Council (FAC) and the Chief Human Resource Officers Council (CHCO).

The CIO Council will exchange information and perspectives with these boards and councils, and other governmental policy and standards bodies, such as the National Institute of Standards and Technology. The Council will serve as a filter to reflect agencies' views and the impacts of pending IRM policies and standards before they are promulgated.

MEMBERSHIP:

- The Deputy Director for Management (DDM) of the Office of Management and Budget, who shall act as executive chairperson of the Council
- The Administrator of E-Government and Information Technology, Office of Management and Budget, who shall act as director and lead the activities of the Council on behalf of the chairperson
- The Administrator of the Office of Information and Regulatory Affairs
- The Chief Information Officer, one Deputy Chief Information Officer, and the Chief Technology Officer (if one has been designated) of each agency described under section 901(b) of title 31
- The Chief Information Officer, one Deputy Chief Information Officer, and the Chief Technology Officer (if one has been designated) of the Intelligence community

Appendix B - CIO Council Charter (Continued)

- The Chief Information Office, one Deputy Chief Information Officer, and the Chief Technology Officer (if one has been designated) of the Department of Homeland Security
- The Chief Information Officer, one Deputy Chief Information Officer, and the Chief Technology Officer (if one has been designated) of the Department of the Army, the Department of the Navy, and the Department of the Air Force, if chief information officers have been designated for such departments under section 3506(a)(2)(B)
- Two small agency Council representatives, designated under the authority of the CIO Council
- Any other officer or employee of the United States designated by the CIO Council

EX OFFICIO:

- General Accounting Office (GAO) Representative
- Chief Financial Officers Council Representative
- Federal Acquisition Council representative
- Chief Human Capital Officer's Council representative
- Associate Administrator for Government-wide Policy, General Services Administration
- At least one state and local government representative
- Others designated by vote of the CIO Council

Voting agencies will get one vote per department or agency. The two representatives for small agencies will have one vote each. There is no minimum requirement to establish quorum at a meeting. The number of members required for a quorum will be the number of members at a meeting. The CIO and Deputy CIO may send their representative to a meeting, but only the CIO or Deputy may vote on behalf of their agency or department.

Ex-officio members are invited to contribute their particular skills and expertise to projects and work groups, but will not vote. At the option of the officers, and considering advice from the members, representatives of other organizations may be periodically invited to attend, observe, or contribute to meetings and activities.

OFFICERS:

The Administrator for the Office of E-Gov and Information Technology (of OMB) shall be the Director of the CIO Council and lead the activities of the CIO Council on behalf of the Deputy Director for Management.

The CIO Council from among its members shall select the Vice-Chairperson of the CIO Council. The Vice-Chairperson shall be an agency CIO, serve a two-year term (or two consecutive one-year terms under the current E-Government Act, pending technical amendment to the current statute, which provides for a one-year term), and may serve multiple terms.

Appendix B - CIO Council Charter (Continued)

PROCEDURES:

- The Council Chairperson will establish the procedures for promulgating Council decisions and resolutions.
- The General Services Administration will maintain an official archive of all minutes and Council documents and staff the CIO Council and Executive Committee
- An Executive Committee, chaired by the Vice-Chairperson and consisting of the chairpersons of the Council's standing committee, representatives from OMB, and the GSA executive secretariat, shall meet regularly to determine issues and agendas for the CIO Council.

COMMITTEES:

The CIO Council has the authority to establish standing committees and working groups as necessary to consider items of concern of the Council, such as committees to address: best practices, IT workforce, architecture and infrastructure, privacy and information security and identity management. The committees are co-chaired by agency CIOs or Deputy CIOs.

PROJECTS:

When it is necessary to establish ad-hoc task groups to address particular items, a Council member shall head each such task group.

STAFF SUPPORT:

The Administrator of General Services shall provide administrative and other support for the Council. The GSA staff will be given the title of executive secretariat. OMB and the Vice-Chair also will provide for staff support to the Council as needed.

Appendix C - Federal CIO Council Governance

Federal CIO Member Organizations

- Agency for International Development
- Department of Agriculture
- Department of the Army
- Department of Defense
- Department of Energy
- Department of Homeland Security
- Department of the Interior
- Department of Labor
- Department of State
- Department of the Treasury
- Environmental Protection Agency
- National Aeronautics and Space Administration
- Nuclear Regulatory Commission
- Small Business Administration
- Director of National Intelligence
- Department of the Air Force
- Department of Commerce
- Department of Education
- Department of Health and Human Services
- Department of Housing and Urban Development
- Department of Justice
- Department of the Navy
- Department of Transportation
- Department of Veterans Affairs
- General Services Administration
- National Science Foundation
- Office of Personnel Management
- Social Security Administration

Federal CIO Council Committees

The Council currently operates five functionally aligned committees, each co-chaired by two members of the Federal CIO Council.

1. Architecture & Infrastructure Committee
2. Best Practices Committee
3. IT Workforce Committee
4. Privacy Committee
5. Information Security & Identity Management Committee

Federal CIO Council Executive Committee

The Executive Committee sets the Council's direction and oversees and integrates the efforts of the other Committees. The Executive Committee is comprised of the following members: CIO Council Director, CIO Council Vice Chair, Ex-Officio Member (GSA), and the Co-Chairs for each of the five Federal CIO Council Committees (Information Security and Identity Management, Architecture and Infrastructure, IT Workforce, Best Practices and Privacy).

Council Liaisons

The CIO Council also maintains liaisons to and from the other Management Councils: These include:

Appendix C - Federal CIO Council Governance (Continued)

- Chief Acquisition Officers Council
- Chief Financial Officers Council
- Chief Human Capital Officers Council
- Small Agencies CIO Council
- National Association of State CIOs
- President's Council on Integrity & Efficiency (PCIE)

Federal CIO Council Committees

1. Architecture & Infrastructure Committee

The Architecture and Infrastructure Committee (AIC) develops policy, direction, and guidance in concert with the Federal Enterprise Architecture Program Management Office (FEA PMO) to drive business process improvement, investment management, and technical decisions. The partnership of the AIC and the FEA PMO is designed to further the development and implementation of the FEA. The purpose of the AIC is to support the CIO Council's mission for a Federal government that is transparent and responsive in servicing citizens and business needs and agile in meeting critical mission requirements. The AIC leads efforts to enable and support government agencies and their business partners to effectively architect, invest, and implement solutions to improve the performance of government.

The AIC supports the CIO Council mission and the AIC's goals by:

- Providing guidance to agencies on how they can align their enterprise architectures to the FEA;
- Facilitating cross-agency development and implementation of shared services through avenues such as the Chief Architects Forum (CAF) and CORE.Gov, the Shared Services Web Portal;
- Implementing and providing guidance on data management strategies; and
- Providing a mechanism that allows modifications to be made to the FEA reference models and the capital planning and investment control process to create greater synergy between technology push cycles and market pull cycles to support a performance-based framework

In pursuit of continuous improvement and rapidly achieving objectives; the Committee mobilized its' membership to:

- Promote the use and improvement of data and information sharing within and among communities of interests, both federal and intergovernmental.
- Accelerate maturation and discernment around emerging technologies
- Advance the federal enterprise architecture practice to enable agility in response to mission.
- Promote the shared services across the Federal government and its partners

Appendix C - Federal CIO Council Governance (Continued)

- Provide authoritative feedback on technology infrastructure questions to the OMB

The AIC has established four working subcommittees to execute its goals and objectives. These subcommittees are the Governance Subcommittee, the Services Subcommittee, the Data Architecture Subcommittee, and the Emerging Technology Subcommittee. The subcommittees of the AIC play a significant role in assisting the CIO Council with jointly achieving collaborative efforts between the CIO Council, Federal Agencies, and the Federal Enterprise Architecture Program Management Office (FEA PMO). The purpose of each of these subcommittees is described in the table below:

AIC Subcommittee	Description
Data Architecture Subcommittee	The purpose is to advance the management of Federal data as a valued national asset that supports the business of the Federal Government. This will be accomplished by stewardship of the Federal Enterprise Architecture (FEA) Data Reference Model (DRM), FEA DRM Management Strategy, and other emerging FEA DRM documents, promotion of the use and improvement of data and data standards across the Federal Government and; the facilitation of community collaboration and information sharing within and among communities of interests, both federal and intergovernmental.
Emerging Technology Subcommittee	The purpose is to develop processes and procedures that support the discovery and assessment of maturing technology offerings responsive to E-government goals. The goals are to: (1) create greater synergy between technology push cycles and market pull cycles in order to support a performance-based framework for innovation prototyping and adoption; and (2) provide a scalable, robust process to respond to the rapidly increasing number of proponent offerings, while accelerating the discovery, creation, validation, and maturation of FEA aligned technologies most likely to yield strategic contributions. The Subcommittee will employ mechanisms for interacting with industry that create value and mitigate risks for all parties.
Governance Subcommittee	Provides policy guidance, and advice and assistance in the definition, design and implementation of Enterprise Architecture (EA) discipline and practice throughout the Federal Government. The Subcommittee serves as a focal point for the development and coordination of Federal government-wide policy, guidance, including best practices for EA development and implementation. The Subcommittee establishes common terminology definitions, frameworks, and practical guidance for use by

AIC Subcommittee	Description
	Federal agencies to effectively implement and sustain EA.
Services Subcommittee	Will analyze the principles and patterns of Shared Services and Service Oriented Architecture, and develop communications collateral and architectural assets to advance the goal of resource rationalization across the Federal IT Portfolio by using shared services. The purpose of the Subcommittee is to understand the dynamics associated with designing and deploying Shared Solutions and Services and, in particular, composite applications using Service Oriented Architecture technologies and standards. In addition the Services Subcommittee will recommend solutions to the deployment, governance, performance, and program challenges involved with Shared Services, and will promote the sharing of reusable components through CORE.Gov.

The Chief Architects Forum (CAF) is an advisory body that supports the AIC. The Forum is a partnership with the AIC, where Chief Architects can collaborate, share lessons learned, and can request and give assistance to their colleagues with specific strategic, management and operational enterprise architecture (EA) challenges. The Forum serves as a formal mechanism for the voice of the Chief Architect community to be heard by the AIC leadership, CIO Council and Office of Management and Budget (OMB). The input from CAF also assists the AIC in providing policy guidance, and advice and assistance in the definition, design and implementation of the Enterprise Architecture (EA) discipline and practice throughout the Federal Government.

2. Best Practices Committee

The Best Practices Committee (BPC) was established by the CIO Council Charter to serve as a focal point for promoting information management/ information technology (IM/IT) best practices within the federal government. The BPC brings together a team of IT professionals committed to identifying the most successful of IM/IT practices being implemented in industry, government and academia; and sharing them with agency CIOs as best practices to be considered for emulation across the Federal Government.

Some efforts of the Best Practices Committee include:

- Special Issue Seminars:** In partnership with organizations such as the American Council for Technology (ACT) and the Council for Excellence in Government (CEG), the Federal CIO Council BPC sponsors a series of special seminars for Federal agency CIOs and their deputies. The seminars are opportunities for agency CIOs and their staffs to examine some of their most pressing IT issues in a not-for-attribution setting with leaders in the field.

Appendix C - Federal CIO Council Governance (Continued)

- **CIO Boot Camp:** The Federal CIO Council BPC offers an orientation for new Federal agency CIOs, Deputy CIOs, and CTOs. This two-day CIO Boot Camp provides new CIOs with insight and knowledge that can enhance their ability to achieve the missions and results of their agencies.

3. IT Workforce Committee

The IT Workforce Committee is government's advocate for strategies to help develop and maintain an effective IT workforce. Its broad agenda encompasses the full employment life cycle: workforce planning, recruitment and retention and career development. As the Federal government continues to streamline IT resources, resulting in more enterprise-wide programs, it must also ensure that the IT workforce is well versed in such areas as IT project management and trained to execute projects with minimum risk.

IT workforce issues continue to rank at the top of CIO critical issues lists. The Committee members, representing nearly every federal Department and agency, work in partnership with the HR community to develop, implement and communicate strategies to recruit, retain and manage a fully trained and qualified IT workforce, to meet current and future mission requirements.

Focus areas are as follows:

- **Recruitment and Retention:** Develop, implement and promote competitive compensation and workforce flexibilities that attract and retain top-level IT talent within the Federal Government, from entry-level to senior executive.
- **Critical Skill Areas:** IT Project Management and IT Security: Identify opportunities to strengthen and leverage critical skill areas such as IT project management and IT security skills in the Federal Government.
- **Professional Development:** Ensure that robust Federal IT professional development programs are offered that reflect current initiatives and the Federal Government's strategic direction.
- **Workforce Capability:** Improve IT workforce identification, assessment and reporting capabilities to support agency requirements and respond to overall Federal IT workforce trends.

4. Privacy Committee

The Privacy Committee of the CIO Council serves as the interagency coordination group for Senior Agency Officials for Privacy in the federal government to provide a focal point for the development and harmonization of privacy policy and protections. The Privacy Committee works to promote adherence to the letter and the spirit of laws advancing privacy, including the Privacy Act of 1974 and the E-Government Act of 2002, as well as widely accepted concepts of fair information principles and practices. Additionally, it looks

Appendix C - Federal CIO Council Governance (Continued)

to ensure widely available education and outreach efforts to create a culture of privacy and to enhance the respect for fair information principles across the federal government. These activities of the Privacy Committee help the Senior Agency Officials for Privacy ensure that their agency appropriately minimizes the impact on the individual's privacy, particularly the individual's personal information and dignity, in the design, development, and operation of agency collections of data.

5. Information Security & Identity Management Committee

The purpose of the Information Security and Identity Management Committee is to support the CIO Council as a collaborative interagency executive level forum that will improve the security of the Federal networks and information by identifying high priority interagency information security and identity management initiatives and by developing recommendations for policies, procedures and standards to address those initiatives. Specifically, the ISIMC works with issues associated with the Trusted internet connection (TIC), Information Assurance Certification and Accreditation Process (IACAP), Comprehensive National Cyber-Security Initiative (CNCI and the National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23),HSPD-12 and others. The ISIMC leverages the success and expertise of the Department of Homeland Security (DHS) Information Systems Security Line of Business (ISSLOB), the United States Computer Emergency Readiness Team Center (US-CERT), and Department of Defense cyber security organizations.

Appendix D - Federal CIO Council Accomplishments

Since its inception, the CIO Council has been focused on ensuring the continued improvement of government IT practices. When new federal wide IT issues arise, this organization has routinely stepped up to develop guidance and policy, and identify best practices. The CIO Council has several notable accomplishments and they are aligned to four major categories. The following pages list some of these accomplishments.

Supporting the IT Workforce

Net Generation Engagement and Exploration

Through the use of a wiki and other collaborative initiatives, the Council prepared a guide, “Connecting with the Net-Generation: Exploring Recruitment, Development, and Retention in the Federal Government,” for IT managers to assist them in employing the next generation of IT workers. Currently, over 67% of individuals in the major federal IT community fall within the Baby Boomer or older age groups. As more of these employees become retirement eligible in the next decade, there will be significant turnover within the Federal Government. In 2008, the Council partnered with general, a generational and innovation thought leader, to understand both the implications and opportunities of increasing employment of the youngest, digital-savvy “Net Generation” within the federal IT workplace. A special emphasis was placed on support of Gov 2.0. In addition the IT Workforce committee began roundtable discussions with the current membership to brainstorm potential high-impact pilot programs focused on IT recruiting across federal agencies, working in collaboration with other like-minded organizations.

Scholarship for Service

The Scholarship for Service program increased the national capacity for educating information technology (IT) specialists in information assurance (IA) disciplines and produced new entrants to the Federal IA workforce. The placement rate was over 90%. Since 2002, approximately 750 students have graduated and gone to work for over 130 different agencies and sub-agencies. In January 2008, the Annual Symposium and Job Placement Fair attracted approximately 200 students, who had the opportunity to network with recruitment representatives from over 40 Federal agencies. Approximately 150 students are currently in school (BA, MA, PhD). Seventy-seven students graduated in 2008 and only nine remain to be finally placed in agencies. The CIO Council’s IT Workforce Committee promoted the Scholarship for Service (SFS) Program to federal agencies. SFS, co-sponsored by the National Science Foundation (NSF) and the Department of Homeland Security- National Cyber Security Division (DHS-NCSD), provided scholarship money for a maximum of two years to outstanding cyber security undergraduate, graduate, and doctoral students in exchange for an equal amount of time spent in Federal government service after graduation.

Appendix D - Federal CIO Council Accomplishments (Continued)

Recruitment Video

The Recruitment Video highlights how diversity of people and diversity of ideas are valued by the federal government, and how federal IT careers open the door to world-class benefits, global opportunities and professional training. The IT Workforce Committee created the recruitment video that is available to be downloaded and used by anyone wishing to promote federal information technology careers. The video was first released on October 4, 2006 at the Federal IT Summit in Arlington, VA.

IT Security Qualifications Matrix

The IT Security Qualifications Matrix establishes qualification levels for all staff engaged in IT Security work based on skills and competencies. This guidance promotes general consistency across the Federal government in identifying the capabilities of qualified IT security staff to handle varying levels of complexity involved with completing cyber security initiatives. The Federal government can also leverage these scarce resources by identifying where they are located in the Federal government structure so they can be matched up to our highest priority initiatives.

CIO University

The CIOC awarded the coveted CIO University Certificate anchored in Clinger-Cohen Core Competencies to 180 people in the following Master's in Information Technology university programs: Syracuse, George Mason, George Washington, Carnegie Mellon, LaSalle and the University of Maryland-University College. With this graduating class, the program has now (since its inception in 1999) awarded certificates to 1,096 people, many of whom play key roles in government and industry Information Technology programs.

Clinger Cohen Core Competencies

The Clinger Cohen Core Competencies update introduces new learning objectives that the federal government deems necessary for prospective CIOs. Every two years the CIO Council's IT Workforce Committee updates the Clinger-Cohen Core Competencies and learning objectives which are used by many institutions of higher learning to develop curriculum for Master's in Information Technology degrees. At the end of calendar year 2008 the newest update will be published after working with subject matter experts to review comments and suggestions from federal CIOs, academics, CIO University Partners and representatives from industry. The current version can be found at: <http://www.cio.gov/documents/2006ClingerCohenCCLearningObj.pdf>

Appendix D - Federal CIO Council Accomplishments (Continued)

IT Quarterly Forums

IT Quarterly Forum information sharing helps the government strengthen its cadre of highly capable IT professionals with mission critical competencies to meet agency goals. The CIO Council's IT Workforce Committee hosted two free quarterly forums (in addition to the annual fall IT Summit) featuring key government experts to share information. At the IT forums this year, more than 350 people from government and industry attended sessions on the IT Infrastructure Line of Business and Section 508 of the Rehabilitation Act. 85% of attendees surveyed rated the forums as very good or excellent, and 95% responded that they learned something that would help them do their jobs.

Student Outreach

Student Outreach provided an opportunity for high school students to learn about the federal IT work world. The Federal CIO Council in partnership with the Association for Federal Information Resources Management (AFFIRM) and Junior Achievement implemented another very successful Information Technology (IT) Job Shadow Day for high school students.

- 2007- 26 agencies and 27 high schools participated in IT Job Shadow Day hosting 280 high students, almost a 200% increase in participation as compared to previous years.
- 2008 - 37 agencies, 31 high schools and 378 students participated in the event, a 26% increase over 2007.

2210 Series Management Activities

OPM and the Federal CIO Council have improved the process of matching applicant qualifications to job announcements by updating the 2210 Qualification Standards. This is an ongoing FY2008 initiative and is in the final review stage. Additionally, The Office of Personnel Management (OPM), working at the behest of the Council, and in consultation with Council members, academia and private industry, established a new specialty classification for Enterprise Architecture which was published in the fall of 2008. The new guidance will support job classification and tracking for this skill area which is critically important to the federal IT community. The IT Management Specialist community, with over 67,000 individuals, is the largest segment of the federal IT workforce, and is employed by all Cabinet-level agencies and most medium-sized and small independent agencies.

Federal IT Summit and the Federal Privacy Summit

The Federal IT Summit and the Federal Privacy Summit assisted federal workers to become better able to provide citizen-centered, customer-focused government to the American public. The CIO Council's IT Workforce Committee organized the Federal IT and the Federal Privacy Summits. The events were attended by 875 federal IT professionals from 95 different agencies and bureaus, and were co-sponsored by OMB's Office of Electronic Government and the Federal CIOC.

Appendix D - Federal CIO Council Accomplishments (Continued)

IT Project Management Matrix and ITPM Training Directory

The IT Project Management Matrix establishes qualification levels for all staff engaged in IT Project Management work based on standardized training, skills and competencies. A companion directory of available ITPM training courses located at www.cio.gov/itprojectmanagement, averages over 100 visitors a month from individuals looking for ITPM training sources. OMB uses the matrix to create universally understood standards and metrics for scoring the qualifications of IT systems project managers managing major IT systems. The matrix has improved the quality of project managers and helped to decrease the number of at-risk IT projects within the Federal Government.

IT Career Development Roadmap

The web-based IT Roadmap career planning tool includes cross-Government competencies and supporting data for critical IT functions within the Federal Government and supports career management and professional development for over 67,000 personnel within the IT Management Specialist 2210. This tool provides employees with the competency recommendations for the parenthetical titles associated with the 2210 IT Management series. It provides opportunities for individual proficiency assessments; identification of competency gaps and career progression planning. This results in more effective career management by employees.

Promoting Information Sharing

Federal Enterprise Architecture

The Federal Enterprise Architecture initiative has provided opportunities to simplify processes and unify work across Federal agencies and within the lines of business of the Federal government. The outcome of this effort was a more citizen-centered, customer-focused government that maximizes technology investments to better achieve mission outcomes. This initiative developed and implemented an effective Reference Model Maintenance Process (RMMP) to assist with the maintenance, revision, and implementation of the Federal Enterprise Architecture (FEA) reference models. Additionally, it has supported the development and coordinated feedback on the Data Reference Model (DRM) v2.0 (including Testing and Management Strategy) and provided sponsorship and support for over 50 “Collaborative Expedition Workshops” focused on topics such as multiple taxonomies, software components development, reuse, and management, intelligent information use in manufacturing, and semantic technology tools and applications.

Appendix D - Federal CIO Council Accomplishments (Continued)

Trusted Internet Connection (TIC)

The TIC initiative has improved the federal government's security posture and incident response capability through the reduction and consolidation of external internet connections and provides a centralized gateway monitoring at a select group of TIC Access Providers (TICAPs). To date, Agencies have indicated a significant reduction and consolidation of existing external connections from more than 4,300 in January 2008 to 2,758 (39%) as of May 2008.

Information Sharing Efforts with the Program Manager for the Information Sharing Environment (PM-ISE)

The improved ISE is founded on trusted partnerships among Federal, state, local, and tribal governments, the private sector, and our foreign allies – partnerships based on a shared commitment to detect, prevent, disrupt, preempt, and mitigate the effects of terrorism against the United States. The architectural approach defines processes for connecting information resources among the Federal, state, and local governments in addition to the private sector. The Information Sharing Environment (ISE) Profile will be used to implement the Information Sharing Environment, consistent with OMB FEA Framework guidelines. The Information Sharing Architecture Framework v.1 facilitates information sharing using a Service Oriented Architecture approach.

Adoption of Federal Controlled Unclassified Information (CUI) Framework Initiative for Information Sharing

The CUI Framework established a Federal-level common vocabulary and associated set of business rules that enable functional capabilities across the various Communities of Interest to apply consistent logic, encoding standards, and security policy in the development of data and services capabilities for tagging and sharing sensitive information within the Federal Government. A new policy and implementation framework was prepared to replace current Sensitive But Unclassified (SBU) markings and processes with a standardized set of Controlled Unclassified Information (CUI) markings, safeguards, and dissemination controls. The initiative was completed by the interagency Sensitive But Unclassified Coordinating Committee, led by the Program Manager, Information Sharing Environment (PM-ISE). Policy and framework were developed in response to the Presidential Guideline 3 requirement in a memorandum issued by the President in December 2005 to the heads of all Executive Departments and Agencies entitled: "Guidelines and Requirements in Support of the Information Sharing Environment."

Practical Guide for Service Oriented Architecture

The Practical Guide for Service Oriented Architecture supports enhanced information sharing, providing an effective and efficient approach to implementing reusable data exchanges. It was developed and released to describe how to simplify delivery of enhanced government services by enabling collaboration and access to services across organizational boundaries.

Appendix D - Federal CIO Council Accomplishments (Continued)

Universal Core (uCore)

The uCore initiative focuses on improving national readiness and international security by developing a common technical approach and vocabulary that enable information sharing between Federal, state, regional, and local governments, along with civil and non-governmental organizations, and U. S. coalition partners and allies. An XML schema was defined containing agreed-upon representations for the most commonly shared and universally understood concepts of who, what, when, and where in order to promote Federal information sharing. To date, 22 independent Communities of Interest, programs, and teams from across the Federal Government have participated in the uCore initiative.

Maritime Domain Awareness (MDA)

The MDA data sharing capability is now used regularly by analysts in the maritime awareness community. With the shared data now available, the people protecting our ships and ports have greatly enhanced data upon which they can make more intelligent decisions on their courses of action. With the vast number of ships afloat, MDA allows individuals involved to be aware of potential problem ships and affords our government the opportunity to take appropriate action. The Maritime Domain Awareness (MDA) pilot employed a community-based approach together with a common technological approach to improve cross-organizational maritime awareness and the sharing of maritime awareness data. The central problem addressed by the initial pilot was to enable unanticipated users to discover and subscribe to Automatic Identification System (AIS) information. AIS data producers and consumers (Navy, Coast Guard, and Department of Transportation) worked collaboratively to: develop a common, community-defined vocabulary and schema to support information exchanges; agree to a common business process and standardize the information exchange vocabulary that described it; and leverage and reuse existing capabilities of DoD's Net-Centric Enterprise Services (NCEs) program Early Capability Baseline (ECB). ECB provided data search, security and messaging services, and a common SOA framework, allowing AIS producers to make their data visible, accessible, and understandable to authorized consumers. Within eight months, the MDA data sharing community of interest demonstrated that shared data could be discovered, accessed, understood and used to provide situational awareness and drive decisions.

Federal Data Quality Framework

The Federal Data Quality Framework provides the ability for government agencies to be able to certify the quality level of their data. The Framework assists federal agencies in detecting faulty data, establishing data quality benchmarks, statistically measuring quality and continuously monitoring quality compliance.

Appendix D - Federal CIO Council Accomplishments (Continued)

Federal Segment Architecture Methodology

The Federal Segment Architecture Methodology facilitates the development of successful segment architecture government wide and was based on best practices compiled from cross-government collaboration.

Protecting Our IT Infrastructure and Privacy

HSPD-12

The CIO Council's Security and Identity Management Committee developed a process for agencies to accept and trust a card issued by another agency for facility visit requests. The government-wide smart card, introduced by Homeland Security Presidential Directive 12 (HSPD-12) provided a common process to assure identity authentication and is a first step toward promoting trust and information sharing among agencies. It aimed to raise the bar on physical and eventually logical security government-wide.

Data at Rest (DAR)

The SmartBUY and ESI teams worked together to establish Blanket Purchase Agreements (BPAs) for data at rest (DAR) encryption products and services. This ground-breaking work is the first enterprise buying initiative to be made available to all US Federal, State, Local, and Tribal governments.

Federal Desktop Core Configuration (FDCC)

The Federal Desktop Core Configuration provides desktop standard security configurations for two operating systems, Microsoft Windows XP and Microsoft Windows Vista. This standardization enables pre-configured, pre-installed, and pre-tested configurations, thereby reducing the cost and time required to deploy the new operating system. To date, 27 Federal agencies are meeting their OMB mandated Federal Desktop Core Configuration (FDCC) reporting requirement using Security Content Automation Protocol (SCAP) validated software tools.

IPv6 Documentation: IPv6 Standards Profile and Executive Guide

The Executive Guide assists Federal CIOs in deploying secure IPv6-based network services and capabilities. The IPv6 Standards Profile defines IPv6 capabilities, identifies configuration options to enhance security, and provides the technical basis upon which agencies' can define future IT policies.

Appendix D - Federal CIO Council Accomplishments (Continued)

Leveraging our Investments

Networkx Cost Benefit Analysis

The Networkx program assisted agencies in meeting the requirements of OMB M-08-05, Implementation of Trusted Internet Connections, which required agencies to optimize individual external connections, including internet points of presence currently in use by the federal government. This improved the federal government's incident response capability through the reduction of external connections. The Networkx program, managed by GSA, replaced the federal government-wide FTS2001 program (and its associated Crossover contract) for telecommunications services. The DoD CIO was asked by the Federal CIO Council Chair to conduct a Cost Benefit Analysis (CBA) to evaluate potential broad Federal benefit from use of the Networkx contract for IT services as the basis for a mandatory use decision. Based on the favorable results of the CBA, the OMB Administrator for E-Gov and Information Technology issued a memorandum to all federal CIOs directing that agencies use the Networkx contract.

SmartBUY

SmartBUY is a federal government procurement vehicle designed to promote effective enterprise level software management. By leveraging the government's immense buying power, SmartBUY has saved taxpayers millions of dollars through government wide aggregate buying of Commercial off the shelf (COTS) software products. To date, (FY06 - FY08), approximately \$398 Million SmartBUY cost avoidance savings have been realized. SmartBUY and ESI awarded 12 BPAs in June 2007 for DAR encryption products and services. The agreements support OMB and DoD's mandate to implement data-at-rest encryption on all mobile computing devices and removable storage. This interagency task force has yielded \$84 million in savings and the sale of nearly 1.4 million data-at-rest (DAR) encryption licenses. To date, federal, state and local governments have purchased essentially \$103 million worth of products at an actual cost of \$19.2 million. Besides providing reduced prices and more favorable terms/conditions, the SmartBUY program assisted agencies to achieve greater standardization, improved configuration management, and more robust IT security. Over 60 large cabinet level agencies, States, and Local governments have ordered off of the DAR BPAs. Additionally, in April 2008 the SmartBUY program, in support of OMB, established a contract, on an expedited basis, for Security Content Automation Protocol (SCAP) validated software tools for Federal Desktop Core Configuration (FDCC) reporting. This short-term fast track solution assists agencies with meeting the OMB requirements to test, assess, monitor, and report on FDCC compliance by incorporating SCAP validated tools into their risk management practice.

Appendix D - Federal CIO Council Accomplishments (Continued)

Earned Value Management

The implementation of the Earned Value Management System (EVMS) ensured that cost, schedule, and technical aspects of a contract are integrated and estimated, and actual progress of the project can be identified. OMB requires the use of an EVMS compliant with the guidelines in ANSI/EIA Standard 748 for all major IT investments with development work. Earned Value Management (EVM) is a project management control tool allowing visibility into technical, cost and schedule planning, performance and progress for major IT projects. EVM not only encourages contractors to use effective internal cost and schedule management control systems, but also provides the manager with timely and consistent cost, schedule and progress data. The CIO Council has provided guidance on the effective use of EVM.

Federal CIO Council Boot Camp

One of the roles of the Federal CIO Council is to ensure that new federal CIOs quickly learn the challenges faced by information leaders in the federal government environment. The Council recognizes that the roles and responsibilities for Federal CIOs differ from those in the commercial sector. To address this need, the Council has implemented the Federal CIO Boot Camp for newly appointed CIOs and deputy CIOs. The Boot Camp consists of a series of sessions addressing issues such as strategic planning, budget formulation and capital planning, program management and performance, security and privacy, information management, and working with Congress and OMB. The Boot Camp program also draws upon a network of senior information executives who have formerly served in senior government positions, to leverage their knowledge and expertise of government and technology management issues and share lessons learned. This networking experience also encourages team building and mentoring across the CIO community.

Agency E-Gov Implementation Plans

For FY 2008: 28 of 28 agencies had mutually accepted Plans and 87% of milestones (or 1041) were successfully met.

IT Workforce Assessment Survey

The IT Workforce Assessment Survey, jointly conducted by OPM and the CIOC provides, collects information from Federal IT professionals about the types of work they perform, as well as their level of proficiency in competencies and skills. It also identifies top training needs; gathers information on certifications held; and provided key demographic data.

Based on a review of the most recent IT Workforce Assessment Survey results which was administered between September 20, 2006 and November 15, 2006, the following lists the percentage breakdown of competencies targeted by agencies for closure:

Appendix D - Federal CIO Council Accomplishments (Continued)

Job Area	Percent of Agencies
IT Project Management	33 percent
IT Security/Information Assurance	26 percent
Solutions Architecture	21 percent
Enterprise Architecture	20 percent

The most frequently targeted competency and skill gaps by area are as follows:

	# of Agencies Identifying Gap for Closure
Enterprise Architecture	
Business Process Reengineering	8
Information Technology Architecture	6
Solutions Architecture	
Information Technology Architecture	6
Requirements Analysis	5
IT Project Management	
Project Management	16
Capital Planning and Investment Assessment	7
Risk Management	7
IT Security	
Information Assurance	9
Information Systems Security Certification	8
Information Systems/Network Security	7
Risk Management	6

Appendix E - Federal CIO Council Strategic Plan

(provided separately)

Appendix F - E-Gov and Lines of Business Initiatives

E-Government Initiatives

(Excerpted from *REPORT TO CONGRESS ON THE BENEFITS OF THE PRESIDENT'S E-GOVERNMENT INITIATIVES*, February 2008)

The Federal government is delivering results through expansion and adoption of electronic government principles and best practices in managing information technology (IT). Through the implementation of these principles, the government is increasingly providing timely and accurate information to the citizens and government decision makers while ensuring security and privacy.

In the fall of 2001, the Office of Management and Budget (OMB) and Federal agencies identified 24 E-Government (E-Gov) Initiatives which were approved by the President's Management Council. Operated, managed and supported by agencies, these Initiatives provide high-quality, common solutions such as citizen tax filing, Federal rulemaking, and electronic training. Beneficiaries include citizens, businesses, and Federal and state government employees.

In the spring of 2004, OMB announced the formation of five Line of Business (LoB) task forces. Additional LoBs were established in 2005 and 2006, bringing the total number of LoBs to nine. The LoBs were identified through a comprehensive analysis of agencies' enterprise architecture data seeking to determine common solutions and methodologies in order to improve service delivery to agencies, increase operational efficiencies, and decrease unnecessary duplication in common administrative areas.

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 requested 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 \$508M.

Selected examples of how citizens and Federal employees are benefiting through the use of the Presidential E-Government Initiatives include:

- **Recruitment One-Stop** – USAJobs.gov, the Federal online recruitment service, receives over 300,000 visits daily from job seekers looking for information regarding career opportunities with the Federal government. This is an increase of 25% over last year.

Appendix F - E-Gov and Lines of Business Initiatives (Continued)

- **IRS Free File** – For the 2007 filing season, as of October 2007, by the use of IRS Free File, the government has already saved more than \$9 million. In the 2006 filing season, 78% of those who used Free File reported “very” high satisfaction with Free File. And, of those who use Free File in 2006, 95% indicated they plan on using it for 2007.
- **E-Travel** – The Treasury Department’s participation in the E-Travel initiative allowed the Department to save \$402,000 in travel management fees in FY 2007.
- **USA Services (USA.gov)** – Recently, Time magazine named USA.gov, the official web portal for the U.S. government, as one of “25 Sites We Can’t Live Without.” USA.gov joins the notable ranks of other websites featured on the “Can’t Live Without” list such as Amazon, eBay, Google, WebMD and Yahoo.com.
- **E-Rulemaking (Regulations.gov)** – Below is an excerpt from Susan Dudley, the Administrator for OMB’s Office of Information and Regulatory Affairs at Regulations.gov 5th Anniversary Ceremony: To find out information on a rule, we used to have to go to an agency’s docket room – deep in the bowels of a government building – and make copies of relevant information (at 5 cents a page). That meant only those sophisticated in the ways of Washington were able to influence rulemaking. The Administration’s e-Rulemaking initiative changes this by providing all American citizens a greater voice in the regulatory decision-making process. We don’t have to go back 25 years to see significant changes. Over the last five years e-Rulemaking has transformed access to the federal government rulemaking process.
 - Regulations.gov has brought government wide-information together, and made it searchable, so a rule watcher doesn’t need to know what agency is issuing a specific rule.
 - A visitor to Regulations.gov can find regulations on a particular subject, determine whether they are open for comment, access important supporting documents, file comments on proposals, and even read comments filed by others.
 - And it has adopted features that – 5 years ago – we didn’t consider important to the rulemaking process, such as RSS feed, book marking etc.

Another E-Rulemaking advancement is the online publication of the Unified Agenda and Regulatory Plan. For the first time last month, they became available in an electronic format that offers users an enhanced ability to obtain and search for information on upcoming US regulations. The shift from paper to the Internet will help save Federal regulatory agencies an estimated \$800,000 per year, and allow the public to search current regulatory information and, within the next few months, historical content.

- **GovBenefits.gov** – GovBenefits.gov provides a single point of access for citizens to locate information and determine potential eligibility for government benefits and services. In FY 2007, GovBenefits.gov received over 250,000 visits per month by citizens and, provided over 400,000 referrals to benefit programs each month.

Appendix F - E-Gov and Lines of Business Initiatives (Continued)

Many more examples of successful e-Government initiatives can be found in the *REPORT TO CONGRESS ON THE BENEFITS OF THE PRESIDENT'S E-GOVERNMENT INITIATIVES*, February 2008 on the Federal CIO Council web site (www.cioc.gov).

Lines of Business

In the spring of 2004, OMB announced the formation of five Line of Business task forces. These five Initiatives were identified by a thorough review of agency enterprise architecture data. The task forces are analyzing this data to identify ways in which services commonly found in numerous agencies can be provided in a more efficient manner.

In the spring of 2005, OMB kicked off the Information Technology (IT) Security Line of Business task force. This task force is working toward identifying problems and proposing solutions to strengthen the ability of all agencies to identify and manage information security risks, as well as implementing improved, consistent, and measurable information security processes and controls across government. The task force is also looking for opportunities for savings or cost-avoidance through reduced duplication and economies of scale.

There are currently nine LoB initiatives:

- Case Management
- Financial Management
- Grants Management
- Human Resource Management
- Federal Health Architecture,
- Information Systems Management
- Budget Formulation and Execution
- Geospatial
- IT Infrastructure

More information for each LoB initiative is provided in the table below.

LoB Initiative:	Case Management
Lead Agency:	Department of Justice
Description:	Utilizing common solutions and data standards (www.niem.gov), case management information is easily and appropriately shared within and between Federal and local agencies
Goals:	<ul style="list-style-type: none"> • Enable case management data to be shared efficiently within and across agencies • Improve effectiveness and efficiency of law enforcement, investigation, and civil and criminal litigation case management business processes • Identify common case management processes across components and agencies that will drive system and function consolidation • Address immediate and long term case management needs and opportunities at the Department of Justice and sister agencies

	<ul style="list-style-type: none"> • Provide guidance for future case management investments across the federal government
LoB Initiative:	Financial Management
Lead Agency:	General Services Administration
Description:	To improve the cost, quality, and performance of financial management (FM) reducing non-compliance systems by leveraging common standards, shared service solutions and implementing other government-wide reforms that foster efficiencies in Federal financial operations.
Goals:	<p>Federal agencies are implementing financial systems that:</p> <ul style="list-style-type: none"> • Provide timely and accurate data available for decision making; • Facilitate stronger internal controls that ensure integrity in accounting and other stewardship activities; • Increase the numbers of agency financial management operations without material weaknesses, with clean audit positions and in compliance with FFMIA; • Reduce costs by providing a competitive alternative for agencies to acquire, develop, implement, and operate financial management systems through shared service solutions; • Standardize systems, business processes and data elements; and • Provide for seamless data exchange from feeder systems and between Federal agencies by implementing a common language and structure for financial information and system interfaces
LoB Initiative:	Grants Management
Lead Agency:	National Science Foundation and Department of Health and Human Services
Description:	A common solution to support end-to-end grants management activities that promote citizen access, customer service, and agency financial and technical stewardship.
Goals:	<ul style="list-style-type: none"> • Reduce cost • Improve customer service • Increase standardization/streamlining of business processes and technologies
LoB Initiative:	Human Resource Management
Lead Agency:	Office of Personnel Management
Description:	Government-wide, modern, cost effective, standardized, and interoperable Human Resource (HR) solutions providing common core functionality to support the strategic management of Human Capital.
Goals:	<ul style="list-style-type: none"> • Improve strategic management of human capital • Achieve operational efficiencies • Increase cost savings/avoidance • Improve customer service
LoB Initiative:	Federal Health Architecture
Lead Agency:	Department of Health and Human Services
Description:	To provide federal agencies the tools and solutions to support the development

	and exchange of interoperable health information within the federal government and with the tribal, state, local and private sector, thereby supporting the President’s national health IT agenda, enabling better care, increased efficiency, and improved population health.
Goals:	<p>Input into the Process: FHA identifies and organizes collective federal health IT needs to advance agency business priorities and the national agenda. Federal health IT expertise and experience are leveraged through participation in defining hit needs, coordination across federal agencies and leveraging of federal health IT investments.</p> <p>Implementation of interoperable solutions within the Federal Government: The President’s health IT plan is implemented in the federal agencies, in alignment with the Federal Enterprise Architecture, through adoption of standards, certified applications, secure and timely exchange of interoperable health information and the protection of patient privacy.</p> <p>Measure Accountability: Federal agencies coordinate effective capital planning activities, and invest in and implement interoperable health IT.</p>
LoB Initiative:	Information Systems Security
Lead Agency:	Department of Homeland Security
Description:	The Federal Government’s information systems security program enables agencies’ mission objectives through a comprehensive and consistently implemented set of risk-based, cost-effective controls and measures that adequately protects information contained in Federal Government information systems.
Goals:	<ul style="list-style-type: none"> • Identify problems and propose solutions to strengthen the ability of all agencies to identify and manage information security risks • Improved, consistent, and measurable information security processes and controls across government • Achieve savings or cost-avoidance through reduced duplication and economies of scale • Obtain NIST validated SCAP (Security Content Automation Protocol) tools with the ability to audit and assess a system to determine its compliance with the Federal Desktop Core Configuration (FDCC) requirements.
LoB Initiative:	Budget Formulation and Execution
Lead Agency:	Department of Education
Description:	Modern, interoperable, flexible, cost effective, and optimized solutions supporting all phases of the formulation and execution of the Federal Budget and linking budget formulation, execution, planning, performance, and financial information.
Goals:	<ul style="list-style-type: none"> • Improve the efficiency and effectiveness of agency & central processes for formulating and executing the Federal Budget • Improve the integration and standardized exchange of budget formulation, execution, planning, performance measurement, and financial management information and activities across government • Improve capabilities for analyzing budget, execution, planning, performance,

	<p>and financial information in support of decision making</p> <ul style="list-style-type: none"> • Enhance capabilities for aligning programs and their outputs and outcomes with budget levels and actual costs to institutionalize budget and performance integration • Enhance the effectiveness of the Federal budgeting workforce
LoB Initiative:	Geospatial
Lead Agency:	Department of Interior
Description:	<p>The Nation’s interests are served, and the core missions of Federal agencies and their partners are met, through the effective and efficient development, provision, and interoperability of geospatial data and services.</p> <p>To further refine the opportunities for optimizing and consolidating Federal geospatial-related investments to reduce the cost of government and, at the same time, improve services to citizens. Cross-agency coordination of geospatial activities can identify, consolidate, and reduce or eliminate redundant geospatial investments. Developing the Geospatial Line of Business (LoB) will result in a more coordinated approach to producing, maintaining, and using geospatial data, and will ensure sustainable participation from Federal partners to establish a collaborative model for geospatial-related activities and investments.</p>
Goals:	<p>Begin implementation by executing the tasks identified in the FY09 Joint Business Case including:</p> <ul style="list-style-type: none"> • Develop communications and outreach materials • Define and establish geospatial data steward life cycle responsibilities and performance measures for A-16 Framework data themes and Nationally Significant Data Themes • Expand smart-buy efforts for geospatial data and technologies and consider shared licenses • Develop requirements and make recommendations to ensure Federal-wide support for the technology and telecommunication infrastructure required to deliver geospatial services • Explore a broker service for data searching among agencies (peer to peer, service to service) which will build on and improve existing systems • Productive intergovernmental collaboration for geospatial-related activities and investments across all sectors and levels of government • Optimized and standardized common geospatial functions, services, and processes which are responsive to customers • Cost efficient acquisition, processing, and access to geospatial data and information • Completion and analysis of a Budget Data Request detailing federal geospatial investments • Reporting and analysis of plans for completion of OMB Circular A-16 data layers • Completion of Program Management Plan for the LoB initiative • Identification of National Geospatial Advisory Committee
LoB Initiative:	IT Infrastructure

Lead Agency:	OMB
Description:	Promotes and enables collaborative infrastructure planning, design, optimization, & systems lifecycle management through communities of practice dedicated to common government-wide performance metrics, Federal Enterprise Architecture/Infrastructure Segment Architectures and Infrastructure Asset Management (including acquisition), and by leading the development of agency five-year infrastructure optimization plans for more cohesive, cost-effective, & secure Federal technology infrastructure.
Goals:	<ul style="list-style-type: none"> • Infrastructure enables interoperability of functions across agencies and programs. • Optimize the infrastructure to enable collaboration within and across agencies, sectors, and government levels. • Efficiencies realized from infrastructure investments will be recapitalized in support of agency mission. • Infrastructure investment governed to achieve agency mission and government-wide goals.

Current Status and Disposition of E-Gov Initiative and Lines of Business

Several months ago, the Federal CIO Council reviewed the status of all E-Gov initiatives and Lines of Business efforts. A number of these efforts have met their initial goals, demonstrated their business case, have self-sustaining funding strategies in place and include an effective, collaborative governance structure. These efforts are shown in the first column of the table below, titled “Initiative/Effort Implemented.” Some of the efforts have demonstrated success but are still in the process of implementation and require continued involvement of the CIO Council. These efforts are shown in the second column, titled “Initiative/Effort Progressing.” A few of the efforts have been subsumed into other on-going initiatives or only require follow-on activity by a single agency. These efforts are shown in the third column, titled “Initiative/Effort Subsumed”.

(see next page)

Appendix F - E-Gov and Lines of Business Initiatives (Continued)

	Initiative/Effort Implemented	Initiative/Effort Progressing	Initiative/Effort Subsumed
E Gov Initiative	GovBenefits.gov	Federal Asset Sales	Business Gateway
	Recreation One-Stop	E-Clearance	Consolidated Health
	IRS Free File	Enterprise HR Integration	Informatics
	GovLoans.gov	E-Payroll	E-Vital
	USA Services	E-Travel	E-Authentication
	E-Rulemaking	Integrated Acquisition Environment	
	Expanding Electronic Tax Products for Businesses		
	Geo-Spatial One-Stop		
	International Trade		
	Process Streamlining		
	SAFECOM		
	Grants.gov		
	E-Training		
	Recruitment One-Stop		
	E-Records Management		
Lines of Business (LoBs)	Financial Management	Information Systems Security	Case Management
	Human Resources		Federal Health Architecture
	Grants Management		
	Budget Formulation and Execution		
	IT Infrastructure		
	Geospatial		

Appendix F - E-Gov and Lines of Business Initiatives (Continued)

The following is a brief description of each initiative.

Gov benefits.gov

Provides a single point of access for citizens to locate and determine potential eligibility for government benefits and services.

Recreation One-Stop

The Recreation One-Stop initiative will make it easier for citizens to plan a vacation (or a brief recreational break during a business trip), and make a reservation for a campsite, cabin, or tour at Federal recreation sites.

IRS Free file

Creates a single point of access to free on-line preparation and electronic tax filing services provided by Industry Partners to reduce burden and costs to taxpayers.

GovLoans.gov

Creates a single point of access for citizens to locate information on federal loan programs, and improves back-office loan functions.

USA Services

USA Services provides leadership in researching and promoting best practices in citizen services among all levels of government in the United States and with other countries.

E-Rulemaking

Allows the public to easily access and participate in the rulemaking process. Improves the access to, and quality of, the rulemaking process for individuals, businesses, and other government entities while streamlining and increasing the efficiency of internal agency processes.

Expanding Electronic Tax Products For Businesses

Reduces the tax-reporting burden on businesses while improving the efficiency and effectiveness of government operations, provides timely and accurate tax information to businesses, increases the availability of electronic tax filing, and models simplified federal and state tax employment laws.

Geo-Spatial One-Stop

Provides Federal and state agencies with single a point of access to map-related data enabling the sharing of existing data to maximize geospatial investments to leverage resources and reduce redundancies.

International Trade Process Streamlining

Export.gov makes it easy for Small and Medium Enterprises (SMEs) to obtain the information and documents needed to conduct business abroad.

Appendix F - E-Gov and Lines of Business Initiatives (Continued)

SAFECOM

SAFECOM functions as the key Federal coordinator for promoting and providing support to local, tribal, state, and Federal public safety agencies for the improvement of public safety response through more effective and efficient interoperable wireless communications.

Grants.gov

Grants.gov is the Federal Government's single site for the federal grant agencies to post and the public to access competitive, discretionary federal grant opportunities.

E-Training

The vision of this government-wide initiative is the creation of a premier e-Training environment that supports the development of the Federal workforce and advances the accomplishment of agency missions through simplified and one-stop access to e-Training products and services.

Recruitment One-Stop

Recruitment One-Stop provides state-of-the-art online recruitment services to Federal job seekers that include online job posting, intuitive job searching, resume warehousing, online application submission, automated eligibility and status feedback, applicant data mining and integration with sophisticated automated assessment tools.

E-Records Management

The E-Records Management initiative provides policy guidance to help agencies better manage their electronic records, so that records information can be effectively used to support timely and effective decision making, enhance service delivery, and ensure accountability.

Federal Asset Sales

GovSales.gov is a one-stop, on-line network for Federal agencies to post property for sale and for the public to locate for purchase. Federal Asset Sales' (eFAS) vision is to maximize value to the citizen, business, and government when selling real and personal property to the general public.

E-Clearance

The E-Clearance initiative streamlines and improves the quality of the current security clearance process through the deployment of automation and common systems and policies to manage the security clearance process.

Enhanced Human Resource Integration

The Enhanced Human Resource Integration (EHRI) initiative is developing policies and tools to streamline and automate the electronic exchange of standardized HR data needed for creation of an official employee record across the Executive Branch.

E-Payroll

The E-Payroll Initiative is consolidating 26 Executive branch Federal payroll providers, standardizing payroll policies and procedures, and simplifying and better integrating payroll, human resources, and finance functions.

Appendix F - E-Gov and Lines of Business Initiatives (Continued)

E-Travel

A government-wide, web-based service that applies world-class travel management practices to consolidate federal travel, minimize cost and produce superior customer satisfaction.

Integrated Acquisition Environment

The Integrated Acquisition Environment (IAE) is a Presidential E-Gov initiative managed by GSA that consists of 9 government-wide integrated systems facilitating, unifying, and streamlining each phase of the federal acquisition process.

Consolidated Health Informatics

Adopts a portfolio of existing health information interoperability standards (health vocabulary and messaging) enabling all agencies in the federal health enterprise to “speak the same language” based on common enterprise-wide business and information technology architectures.

E-Vital

Promotes automating how deaths are registered with the states (Electronic Death Registration (EDR)).

E-Authentication

Minimizes the burden on businesses, public and government when obtaining services on-line by providing a secure infrastructure for on-line transactions, eliminating the need for separate processes for the verification of identity and electronic signatures.



Appendix G - Federal CIO Roadmap

FEDERAL CIO ROADMAP

The Federal CIO Roadmap provides a high level look at areas of responsibility for Federal CIOs. Specific detailed CIO responsibilities are specified in law, regulation, and OMB circulars and guidance.

Strategic Planning

IRM/IT Strategic Planning: The Agency CIO is responsible for the development and annual maintenance of a strategic information resources management (IRM) plan describing information and technology management functions and activities. To use IT effectively it is recommended that CIOs develop a comprehensive IT/IRM strategic plan that aligns to the agency business strategy and ensures IT investments are funded only where they have the greatest impact on business results.

Federal IT Workforce: Agency CIOs are required to assess the information resources management skills needed for agency personnel and to evaluate and rectify deficiencies identified in meeting the agency performance goals. CIOs are further required to develop strategies and specific plans for the hiring, training and professional development that is needed. Agencies work with OMB and the CIO Council to identify needed competencies and to fill skill gaps. Agencies are also required to assign a qualified project manager to each project and to examine and document the qualifications of these individuals.

Enterprise Architecture (EA)

Federal laws and guidance direct agency CIOs to develop and maintain EAs as blueprints to guide IT modernization in support of agency missions. EA is carried out as a part of a Performance Improvement Lifecycle (PIL) consisting of three phases: Architect, Invest, and Implement.

The PIF is linked to the agency's budget development and submission process. In September, OMB issues FEA guidance, containing any cross-agency initiatives and the EA assessment framework for the fiscal year. An agency develops its EA and works with its business areas to develop segment architectures to further the agency's missions. Assessments are conducted in March with immediate feedback. An agency then uses its architectures to guide and inform its capital investment process, and submits its budget to OMB in September. OMB verifies that each agency's budget reflects its target architecture. For clear and consistent information for cross-agency IT initiative adoption, OMB has developed the Federal Transition Framework catalog aligned with the FEA reference models.

Annual EA Assessment: OMB conducts an annual assessment of an agency's EA program in three capability areas:

1. Completion of an agency's EA and related artifacts in support of the agency mission and cross-agency initiatives.
2. Use of an agency's EA to drive improved decision-making, and
3. Results achieved from EA use in terms of effectiveness and efficiency

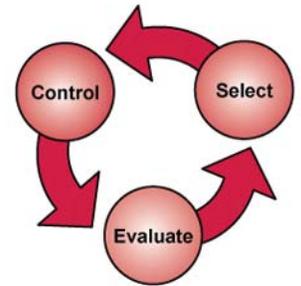
Agencies receive an average score for each capability area. Annual results are reflected in the Status measure for E-Government within the President's Management Agenda (PMA) Scorecard.

Quarterly EA Performance Review: An agency submits quarterly progress reports to OMB on the status of achieving transition strategy milestones. Results are reflected in the Progress measure for E-Government within the PMA Scorecard.

Budget Formulation and Capital Planning & Investment Control (CPIC)

The Capital Planning and Investment Control process is an integral part of agency budget formulation and execution. To maximize the value of invested taxpayer dollars, CIOs are required to monitor and evaluate the performance of information resource investments through a CPIC process and advise the agency head on whether to continue, modify, or terminate a program or project. Agency CIOs may use the CPIC process to manage IT investments on an individual basis as well as in the context of the entire IT portfolio. An effective capital planning process requires long-range planning and a disciplined budget process as the basis for managing a portfolio of capital assets. A sound capital planning process defines how an agency:

- **Selects** capital investments for funding each year;
- **Controls** and manages capital investments to achieve intended cost, schedule and performance outcomes;
- **Evaluates** performance to maintain a positive return on investment.



E-Government and IT Implementation

E-Gov Implementation and Alignment: To ensure the Federal Government achieves results for E-Government, Lines of Business (LoB), and SmartBUY initiatives, OMB measures agency participation and adoption of initiative outputs against a set of established milestones agreed to by the agency and OMB.

Agency Requirements: Agencies are required to submit quarterly progress reports on the status of their E-Gov implementation milestones. For any missed milestones, CIOs are required to provide a rationale and expected date of completion. In addition, as initiatives progress and new requirements are identified, CIOs are required to update their implementation plans and milestones.

Standards for Success: Agencies must demonstrate completion of all E-Gov implementation plan milestones scheduled for that quarter or risk being downgraded in *Progress* on their E-Gov PMA scorecard. In addition, Agencies that miss a major milestone will be downgraded in *Status* on their E-Gov PMA scorecard. If an agency misses a milestone due to circumstances outside its control, its *Progress* and *Status* scores will not be downgraded.

Lines of Business Initiative: Building upon the efforts of the Federal Enterprise Architecture Program to expand E-Government, OMB and designated cross-agency task forces launched the Line of Business (LoB) Initiative for nine lines of business.

- Case Management
- Federal Health Architecture
- Financial Management
- IT Infrastructure Optimization
- Geospatial
- Budget Formulation and Execution
- Grants Management
- HR Management
- Information System Security

An LoB initiative is a cross-agency effort to define, design, implement, and monitor a set of common solutions for a government-wide business function or service of the Federal Government. The scope of a Line of Business effort is to:

- Define processes and business rules associated with government-wide business functions;
- Shape existing or inform future policy by making recommendations to the appropriate policy authority associated with the business function;
- Provide implementation guidance to agency IT projects or systems to come into alignment with the LoB initiatives.

SmartBUY: SmartBUY is a Federal government-wide enterprise software licensing initiative designed to streamline the acquisition process and provide the best priced, standards-compliant IT. Agencies are required to maximize the use of SmartBUY leveraging government buying power to reduce software licenses expenses and avoid redundant purchases.

Program Management and Performance

When managed effectively, IT investments can have a dramatic impact on an organization's performance. If not, however, they can result in wasteful spending and lost opportunities for improving delivery of services to citizens.

Earned Value Management (EVM): EVM is a project management tool that effectively integrates the scope of work with schedule and cost elements for optimum investment planning and control. EVM allows for the development of a performance measurement baseline against which accomplishments may be measured in an independently verifiable basis. As a result, decision-makers have consistent, quantifiable indicators of performance to determine if a project is progressing as planned.

Standards for Success: Agency CIOs are required to assign a qualified project manager to each project. In addition, agencies are expected to achieve, on average, 90% of cost, schedule, and performance goals for all major and non-major projects. OMB evaluates agencies' actual performance of major IT investments on the PMA E-Gov Scorecard as follows:

-  Has demonstrated appropriate planning, execution, and management of major IT investments, using EVM or operational analysis, and have IT portfolio performance operating within 10% of cost, schedule, and performance goals.
-  Has demonstrated appropriate planning, execution, and management of major IT investments, using EVM or operational analysis, and have IT portfolio performance operating within 30% of cost, schedule, and performance goals.
-  Has cost and schedule overruns, and performance shortfalls, that average 30% or more.

In evaluating whether an agency has achieved the "green" standard for success for cost, schedule, and performance, OMB looks for:

1. Documented agency policy.
2. Established cost, schedule and performance baselines.
3. Examples of how the agency uses data and analysis to make decisions.
4. Contract language requiring the use of EVMS that meets the ANSI/EIA-STD 748
5. Current cumulative EVM data and variance analyses, and corrective action plans.

Security and Privacy

Security Considerations: The Federal Information Security Management Act (FISMA) provides the framework for securing the Federal Government's information technology including both unclassified and national security systems. All agencies must implement the requirements of FISMA and report annually to the Office of Management and Budget (OMB) on the effectiveness of their security programs. OMB uses the results of the reports to develop its annual security report to Congress. In addition, as part of the PMA scorecard process, agencies are required to submit quarterly reports demonstrating progress addressing security weaknesses on their Plan of Action and Milestones (POA&M).

Privacy Considerations: The Privacy Act of 1974 requires Federal agencies to develop systems of record for any information in their possession that identifies an individual by name, number, or any identifying particular assigned to that person. In addition, a notice of the existence and character of the system of records must be published in the Federal Register. Furthermore, agencies are required to:

- Provide notice to the individual of the system of record;
- Permit the individual access to that record;
- Disclose the routine uses of the information and gain consent prior to using the information beyond its original intent;
- Establish the appropriate safeguards to ensure the security and confidentiality of records.

The E-Government Act of 2002 directs agencies to conduct reviews of how information about individuals is handled within their agency when they use IT to collect new information, or when agencies develop or buy new IT systems to handle collections of personally identifiable information. In summary, Agencies are required to:

1. Conduct privacy impact assessments for electronic information systems and collections.
2. Make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.
3. Translate privacy policies into a standardized machine-readable format.
4. Report annually to OMB on compliance with section 208 of the E-Government Act of 2002.

GAO's Summary of CIO's Information Management & Technology Responsibilities

IT/IRM Strategic Planning - The agency CIO is responsible for strategic planning for all information and technology management functions - thus, the term information resources management (IRM) strategic planning. 44 U.S.C. 3506(b)(2).

IT/IRM Workforce Planning - CIOs have responsibilities for helping the agency meet its IT/IRM workforce or human capital needs. 44 U.S.C. 3506(b) and 40 U.S.C. 11315(c).

Capital Planning and Investment Management - Federal laws and guidance direct agencies to develop and implement processes for IT capital planning and investment management. 44 U.S.C. 3506(h) and 40 U.S.C. 11312 & 11313.

Systems Acquisition, Development, and Integration - GAO found that a critical element of successful IT management is effective control of systems acquisition, development, and integration.

Major Electronic Government (E-Gov) Initiatives - Various laws and guidance have directed agencies to undertake a variety of e-gov initiatives relating to using IT to improve government services to the public, as well as operations within the government.

Enterprise Architecture (EA) - Federal laws and guidance direct agencies to develop and maintain enterprise architectures as blueprints to guide IT modernization.

Information Security - The agency CIO is responsible for protecting information and systems. 44 U.S.C. 3506(g) and 3544(a)(3).

Privacy - The agency CIO is responsible for compliance with the Privacy Act and related laws. 44 U.S.C. 3506(g).

Information Collection/Paperwork Reduction - The agency CIO is responsible for overseeing a process to review agency information collection proposals in order to maximize the utility and minimize the public "paperwork" burdens associated with the agency's collection of information. 44 U.S.C. 3506(c).

Records Management - The agency CIO is responsible for ensuring that the agency implements and enforces records management policies and procedures. 44 U.S.C. 3506(f).

Information Dissemination - The agency CIO is responsible for ensuring that the agency's information dissemination activities meet policy goals, such as timely and equitable public access to information. 44 U.S.C. 3506(d).

Information Disclosure/Freedom of Information Act (FOIA) - The agency CIO is responsible for information access requirements, such as those of the FOIA and related laws. 44 U.S.C. 3506(g).

Statistical Policy and Coordination - The agency CIO is responsible for the agency's statistical policy and coordination functions. 44 U.S.C. 3506(e).

Source: GAO-04-823, *Federal Chief Information Officers Responsibilities, Reporting Relationships, Tenure, and Challenges*

Key Legislation

The E-Government Act of 2002

Federal Information Security Management Act of 2002 (FISMA)

Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA)

Government Paperwork Elimination Act of 1998 (GPEA)

Clinger Cohen Act of 1996

Freedom of Information Act of 1996 (FOIA)

Paperwork Reduction Act of 1995 (PRA)

Federal Acquisition Streamlining Act of 1994, Title V (FASA V)

Government Performance Results Act of 1993 (GPRA)

The Privacy Act of 1974

Records Management by Federal Agencies (44 U.S.C. Ch.31)

Federal Depository Library Program Laws (44 U.S.C. Ch.19)

Please refer to the OMB website (<http://www.whitehouse.gov/omb/inforeg/infopoltech.html>) for specific memos, circulars, and other IT related guidance.

