



# **STRATEGIC PLAN**

**FISCAL YEAR  
2001 – 2002**

Washington, D.C.  
OCTOBER 2000

## TABLE OF CONTENTS

<b>Foreword</b> .....	<b>1</b>
<b>Executive Summary</b> .....	<b>4</b>
<b>FY 2001 Strategic Goals:</b>	
1. All Citizens Connected to Products, Services, and Information of Their Government.....	<b>6</b>
2. Interoperable and Innovative Government-wide IT Initiatives.....	<b>16</b>
3. A Secure and Reliable Information Infrastructure That The Customer Can Access and Trust.....	<b>25</b>
4. IT Skills and Resources To Meet Mission Objectives.....	<b>37</b>
5. Collaborations Between the Public and Private Sectors Achieve Better Government.....	<b>44</b>
6. Investment Management Policies, Practices, and Tools That Enable Improved Delivery of Government Programs and Services.....	<b>49</b>
<b>Appendices:</b>	
Appendix A: Executive Order 13011.....	<b>57</b>
Appendix B: CIO Council Charter.....	<b>63</b>
Appendix C: CIO Council Structure.....	<b>66</b>
Appendix D: FY2001 Objectives and Initiatives With Lead and Contributor Committee Responsibilities.....	<b>67</b>
Appendix E: General Abbreviations.....	<b>72</b>

# CIO COUNCIL STRATEGIC PLAN

## FOREWORD

### The CIO Council

The citizens of the United States are rightfully expecting a more responsive and efficient Federal Government. Information technology (IT) is an essential component of the modern infrastructure of government, and has become a means for the shift towards a more citizen-centric government.

Within the Executive Office of the President (EOP), the Office of Management and Budget (OMB) has oversight over the implementation of the Federal budget and agency program management. A statutory office in OMB, the Office of Information and Regulatory Affairs, is given specific authorities from the Paperwork Reduction Act of 1995 and the Clinger-Cohen Act to oversee a variety of Federal IT activities. To support this function, Executive Order 13011 of July 16, 1996 established the Chief Information Officers (CIO) Council as a Government-wide body to address crosscutting IT issues. CIOs and Deputy CIOs of the 28 largest Federal agencies and two CIOs representing the smaller Federal agencies comprise the Council's membership, under the leadership of OMB's Deputy Director for Management.

The Council plays a key role in directing and leading the strategic management of Federal IT resources. It serves as a focal point for coordinating responses to Government-wide IT challenges and partners with other governmental councils to address issues that require multi-disciplinary and multi-level

solutions. The Council's Charter defines its responsibilities as follows:

- Develop recommendations for overall Federal information technology management policy, procedures, and standards;
- Share experiences, ideas, and promising practices, including work process redesign and the development of performance measures, to improve the management of information resources;
- Identify opportunities, make recommendations for, and sponsor co-operation in using information resources;
- Assess and address the hiring, training, classification, and professional development needs of the Federal Government with respect to information resources management;
- Make recommendations and provide advice to appropriate executive agencies and organizations, including advice to OMB on the Government-wide strategic plan required by the Paperwork Reduction Act; and seek the views of the Chief Financial Officers Council, the Information Technology Resources Board, the Procurement Executive Council, industry, academia, and Federal, Tribal, and

## CIO COUNCIL STRATEGIC PLAN

State and local governments on matters of concern to the Council, as appropriate.

### **The Strategic Plan**

Since January 1998, OMB and the CIO Council have jointly published a strategic plan to meet the requirements of the Paperwork Reduction Act of 1995 and Executive Order 13011 on Federal Information Technology. The goal of the strategic plan is to enhance the strategic focus of the Council, establish roadmaps for achieving the strategic vision, define measures to assist the Council in evaluating its progress toward meeting its challenges, and provide a basis for budget planning.

To this end, the Council has actively sought feedback from its stakeholders from within both the Government and the private sector regarding its strategic direction and tactical initiatives. The Council has created partnerships with other Councils such as the Chief Financial Officers Council, the Human Resources Development Council, and the Procurement Executive Council to work collaboratively on key issues such as security, privacy, workforce retention, and procurement.

This document sets forth the results of the Council's FY 2001 strategic planning. The plan continues to refine the Council's strategic planning process and perspectives. It reflects the Council's view of critical, cross-cutting IT issues that are affecting the Federal Government's ability to better serve its citizens. Some of these issues are long standing; others are emerging with rapidly changing technologies.

The plan is structured around a number of themes. The themes provide the focus for the Council's strategic goals. Each goal is expressed as a statement of an end state or desired environment. The goals are intended to be long term and stable. A set of objectives is associated with each goal. The objectives define the major actions to be undertaken, primarily by Federal agencies, in order to achieve the goal. The initiatives represent specific, concrete actions that the Council, in collaboration with other governmental and non-governmental organizations, will take to implement the objectives. This classic strategic planning approach provides a stable and repeatable framework for the Council to continue to address IT challenges.

As Federal agencies prepare for the transition to a new Administration, the Council too will be preparing transition papers on Federal IT to assist the new Administration. The Council, in its role as advisor to the Administration in Federal IT management policy, sponsoring promising IT solutions and initiatives and in implementing legislation, aims to position its recommendations and advice to the incoming Administration in the context of the Council's longer term strategic directions and initiatives. This plan provides that context. Later in the fall, the Council will publish a separate transition plan outlining more immediate issues.

### **Acknowledgement**

This plan could not have been produced without the commitment and hard work of all of the Council's members. Their

## **CIO COUNCIL STRATEGIC PLAN**

participation in the strategic planning process and the quality of their contributions indicate their dedication to the aims of the Council and their interest in improving government.

Signed:  
Sally Katzen  
Chair, CIO Council

Signed:  
Jim Flyzik  
Vice Chair, CIO Council

# CIO COUNCIL STRATEGIC PLAN

## EXECUTIVE SUMMARY

The Council's strategic plan reflects a consensus by the Federal Government's Chief Information Officers. This consensus developed as the Council considered its challenges and direction in the light of the business and technical environment in which the Government operates. E-business and the continuing need to meet existing demands for better service at lower cost are causing the revolution in business practices. The Council can not stand pat; it must evolve and grow to meet the technical and management issues of the beginning of the 21<sup>st</sup> century.

Given this context, the Council evaluated and reformulated its vision to specifically address the concept of a better government. The CIOs recognize that technology alone can not achieve better government. Technology is viewed as an enabler, albeit an important one given the productivity, quality of life, and other achievements that have resulted from the intelligent use of technology. Notwithstanding the importance of technology, technical solutions must work in concert with people, processes, and information to provide the services that government uses to work better. As shown below, the CIO Council's statement of its vision captures these important concepts and highlights that IT is an important element of the national infrastructure.

***"Better government through better use of information, people, processes and technology"***

The vision establishes the compass for the remainder of the Council's strategic plan. In effect, the vision encompasses six themes.

- **Connecting citizens** is a new focus for the Council. The globalization of IT and the impact of Internet-based technologies on business are influences that impact the Federal Government. The e-Government strategy has evolved to incorporate improving citizen access to Government services, improving the quality of services available through Government sites and addressing security, privacy, and accessibility for the disabled concerns. A fourth element is to remove barriers to citizen interactions with Government through eliminating reliance on paper-based transactions.
- **Interoperability and innovation** is a recurring theme for the Council whose significance has evolved due to the impact of e-Government and other factors. The seamless integration of services and infrastructure using innovative technologies and approaches are components of this theme.
- **Security and reliability** is another recurring theme whose importance has been enhanced under the impact of technological advances. The privacy of personal information and transactions, security of assets from cyber attacks, and risk management constitute the third theme.

## CIO COUNCIL STRATEGIC PLAN

- **Skills and resources** are an on-going concern for the Council. The need to improve the Government's ability to attract and retain a top-notch workforce and expand training and education opportunities are included in the fourth theme.
- **Collaboration and awareness** is another focus. The Council recognizes the need to develop close and effective partnerships with all levels of government and with other stakeholders.
- **Managed investments** indicates the Council's continuing focus on improving how IT investments are defined, evaluated, and managed.

Each of these themes is further developed in the subsequent pages of this FY 2001 CIO Council strategic plan.

**GOAL 1: ALL CITIZENS  
CONNECTED TO THE  
PRODUCTS, SERVICES, AND  
INFORMATION OF THEIR  
GOVERNMENT**

**CONNECTING CITIZENS**

**Background:**

The goal of connecting citizens to the products, services, and information of their Government reflects the impact of Internet-based technologies and solutions on the business of Government. The Council identified five major objectives that support the achievement of this goal.

The global trend towards making government information accessible to citizens and to facilitating interactions with citizens is notable. The increased use of Internet-based solutions to facilitate business-to-business and business-to-customer interactions has major implications for Federal Government IT initiatives that the Council wants to address. The Council has recognized the importance of this development and has already taken a number of actions to include establishing the e-Government Committee to provide a focus for Council actions in supporting e-Government initiatives. A key initiative that the Council is supporting is the development and implementation of FirstGov, as well as support for sector specific cross-agency portals like Access America.

- 1) Develop a single point-of-entry portal model to access Government services (the "entry" phase of the e-Government strategy).
- 2) Increase the customer-value of Government sites (the "quality of content" phase of the e-Government strategy).
- 3) Make transactions across all levels of Government seamless (the "integration" phase of the e-Government strategy).
- 4) Authenticate citizen transactions and interactions with Government agencies easily and properly (the "privacy safeguard" phase of the e-Government strategy).
- 5) Establish communities of practice and affinity groups through the use of collaborative tools (the "knowledge management" phase of the e-Government strategy)

The passage of the Government Paperwork Elimination Act (GPEA) with its requirement for the optional electronic maintenance, submission or disclosure of information, when practical, as a substitute for paper by FY 2003 poses a major managerial and technological challenge for Federal agencies. Legislation and other regulatory actions such as Section 508 of the Rehabilitation Act have been enacted that reinforce the importance of this theme.



## CIO COUNCIL STRATEGIC PLAN

### Accomplishments

#### **Funding/Participation in FirstGov -**

The Council actively participates on the FirstGov Board that oversees the development of a single port of entry to provide governments, citizens, businesses, and community groups with one-stop access to over 20,000 Federal Web sites.

#### **Inventory of Noteworthy Federal e-Gov. Programs/Projects -**

The Council coordinated the development of an inventory of approximately 200 Federal e-Government programs and projects. These projects were either nominated or won an award for the years 1996 through 2000 (e.g., Government Computer News, E-Gov, Innovation Award). The inventory provides the opportunity for Federal agencies to share best practices and learn from each other's successes.

**Promoting e-Government -** Council members have presented numerous presentations and speeches, participated in seminars, roundtables, and forums to both industry groups and Federal and State agencies. These efforts were aimed at promoting the Council's e-Government initiatives in all arenas. Conference and group participation included: Management of Change Conference, AFCEA's Virtual Government, Federal Office Systems Exposition (FOSE) Industry Advisory Council (IAC), E-Gov, Excellence in Government, Information Technology Association of America (ITAA), and Federal Sources. The Council sponsored a series of small, informal gatherings with senior IT leaders from the private sector who are working in and knowledgeable about the e-Business or digital government arena.

The e-Government promotion activities have served to increase awareness of e-Government aims and challenges, as well as assisting agencies to define e-Government strategies.

#### **E-Government Coordinating Group -**

The Administration's e-Government Coordinating Group was created for cross-coordination of e-Government groups under the CIO Council, the Chief Financial Officers (CFO) Council, and the Procurement Executive Council (PEC). Representatives explore ways to promote e-Government initiatives across several disciplines – financial management, Federal procurement, and information technology.

**Best Practices -** The Council initiated a joint effort with the IAC to research and publish "*Best IT Practices in the Federal Government – Volume III – Digital Government.*" Publication of the results is scheduled for early FY 2001.

#### **Survey of e-Government Initiatives -**

The Council also initiated a survey, via a one-page questionnaire, to inventory all current Federal agency e-Government initiatives. The initiatives were classified according to channels (government to citizen, to government, to employee, and to business). This interactive database of information will be used in planning strategies for developing e-Government.

#### **National Association of State Information Resource Executives (NASIRE) -**

The Council held joint sessions with NASIRE to discuss Federal and state joint projects, coordinated initiatives, and integrated

## CIO COUNCIL STRATEGIC PLAN

delivery. Members of the Council are members of NASIRE.

**Authentication** - Working with the General Services Administration (GSA), the Council developed a strategy for encouraging more agencies (grouped by functionality) to participate in the Access Certificates for Electronic Services (ACES) Project. The main purpose of the strategy is to bring together agencies that have similar customer groups, such as the Internal Revenue Service (IRS), Social Security Administration (SSA), Department of Veterans Affairs (VA), Department of Education, and United States Postal Service (USPS), to work on more coordinated ways of using ACES certificates. The first 110,000 digital certificates were created under ACES. The certificates from AT&T Corp. and Digital Signature Trust Co. of Salt Lake City are among 500,000 that will be issued free. The initial set of certificates is scheduled for distribution to the VA and the Federal Emergency Management Agency (FEMA).

**E-Gov. Awards** - The Council supported the creation of a new awards program. The program, sponsored by IAC, the Council for Excellence in Government, and the E-Gov Journal, recognizes agencies that demonstrate major achievements in e-Government.

## CIO COUNCIL STRATEGIC PLAN

**Objective 1.1:**

***Develop a single point-of-entry portal model to access Government services.***

The new site, FirstGov.gov, will allow citizens to search all online resources offered by the Federal Government from a single Web site. Entry points to FirstGov.gov will be expanded through “certified partnerships”. A strategy for implementing functional portals at five agencies will be developed. This is considered the “entry” phase of the e-Government strategy.

The e-Government Committee will be responsible for the initiatives related to development of a single point-of-entry portal model.

Initiatives	Milestones
1. Support implementation of FirstGov.gov.	10/01/00
2. Promote an expanded number of entry points to FirstGov.gov through "certified partnerships".	01/01/01
3. Develop a strategy for implementing functional portals at five Government agencies.	03/31/01
4. Support development of functional portals (e.g., Students, Seniors, and Fed-Commons).	<ul style="list-style-type: none"> <li>● 6 by 03/01/01</li> <li>● 6 more by 09/01/01</li> </ul>
5. Propose alternative models to provide universal citizen access to Government information and services.	12/01/01

The performance measures are:

- Number of additional entry points to FirstGov.gov under the "certified partnership" program by 01/01/01
- Number of functional portals created by 09/01/01 with a target of twelve

**Objective 1.2:**

***Increase the customer-value of Government sites.***

Government sites will only be of true value to the citizens if they are user friendly and provide the citizen with the appropriate Government information and services. In general, this will be accomplished by following seven guiding principles that are outlined below.

Easy to use. Easy for all Government customers to utilize, and crossing Federal, State, local, and international Governments.

Available to everyone. Accessible to all Americans – at home, at work, in schools, and in their communities.

Private and secure. High standards for privacy, security, and authentication – generating trust – are required for e-Government to serve the public, to grow, and to thrive.

Innovative and results-oriented. Emphasizing speed and state-of-the-art technology, while embracing continuous improvement.

Cost-effective. Strategic investments and results that produce significant long term efficiencies and savings.

Collaborative. Within a framework of Government policy, standards, and accountability, solutions are developed collectively and openly among public, private, nonprofit, and research partners based on their experience and expertise.

## CIO COUNCIL STRATEGIC PLAN

Transformational. Harnessing technology to transform Government, rather than automating existing practices, through personal and organizational leadership.

Government services and information would be available 24 hours a day, seven days a week. Guidelines and recommended standards for electronic information and services on Federal sites will be developed. Fifty percent of all rule making, such as public comments, will be performed online. Increasingly, Government data will be available in geo-spatial form. This is the "quality of content" phase of the e-Government strategy.

The e-Government Committee will also be responsible for initiatives to increase the customer-value of Government Web sites.

Initiatives	Milestones
1. Promote work by agencies to modify their Web sites to support the functional portals.	06/01/01
2. Support the e-Gov awards program recognizing innovative Federal sites.	02/15/01 (issue first awards by that date)
3. Support the dissemination of industry and Government "best practices" for site content.	02/15/01
4. Develop Government-wide guidelines and best practices and recommend standards for electronic information and services on Federal sites.	09/01/01
5. Establish five moderated, open discussion groups for citizen interaction with agencies.	09/30/01
6. Assist Federal agencies in offering online rule making such that 50% are online.	10/01/02
7. Promote the transition of Federal data to geo-spatial form.	02/01/03
8. Support OMB in the smooth implementation of GPEA.	10/01/03

The performance measures are:

- e-Gov. awards recognizing innovative Federal sites issued by 02/15/01
- Number of Government-wide guidelines, best practice guides, and recommended standards, related to electronic information and services, issued by 09/01/01
- Percent of Federal rule making conducted online by 10/01/02 with a target of 50%
- Percent of Federal data in geo-spatial form by 02/02/03

## CIO COUNCIL STRATEGIC PLAN

**Objective 1.3:**

***Make transactions across all levels of Government seamless.***

The integration of information and services at the Federal, State, and local government levels is critical to permit citizens to interact effectively with all levels of government. The integration should be seamless and transparent to the citizen. To achieve this, the Council, in collaboration with groups such as NASIRE, the National Association of Counties (NACO) and the National League of Cities (NLC), will develop and issue a strategy for integrating electronic information and services. On the international side, the Council will hold two e-Gov Congresses to discuss and develop an inter-governmental and international strategy for integrating electronic information and services. This is the “integration” phase of the e-Government' strategy.

The e-Government Committee and the Outreach Committee will jointly support the initiatives related to the seamless integration of Government transactions.

Initiatives	Milestones
1. Develop and issue a strategy for integrating electronic information and services with State Governments.	03/01/01
2. Develop and issue a strategy for integrating electronic information and services with local Governments.	09/01/01
3. Plan, organize and hold an Inter-Governmental e-Congress.	12/01/01
4. Develop and issue a strategy for integrating electronic information and services in specific functional areas with five other countries.	01/01/03
5. Plan, organize, and hold an international e-Gov Congress.	06/01/03

The performance measures are:

- Inter-governmental and international strategy for integrating electronic information and services issued (one in 03/01/01; a second by 09/01/01, and a third by 01/01/03)
- Inter-governmental and international e-Congresses held (one by 12/01/01; the other by 06/01/03)

**Objective 1.4:**

***Citizen transactions and interactions with Government agencies are easily and properly authenticated.***

Citizen transactions and interactions with Government agencies must be authenticated easily and properly. This will increase the public's confidence in the Government's capability to safeguard personal information. The Council supports the development of private, secure, and effective communication across Federal agencies and with the public through the use of public key technology. The immediate goal is to meet the President's December 17, 1999 mandate to have 100,000 digital signatures by January 2000, with a follow-up goal of one million by January 2002. An action plan will be developed that will further enhance the creation of this critical mass of digital signature certificates and promote their use. Additionally, other initiatives are aimed at cross-certifying at least five vendor public key infrastructure (PKI) certifications and implementing five cross-agency digital signature approaches. This is the “privacy safeguard” phase of the e-Government strategy.

## CIO COUNCIL STRATEGIC PLAN

The e-Government Committee and the Security, Privacy, and Critical Infrastructure Committee, supported by the Enterprise Interoperability and Emerging IT Committee, will have responsibility for the initiatives related to the easy and reliable authentication of citizen transactions with Government agencies.

Initiatives	Milestone
1. Promote the use of digital signatures by citizens and businesses.	<ul style="list-style-type: none"> <li>● 100,000 by 01/01/01</li> <li>● 1,000,000 by 01/01/02.</li> </ul>
2. Cross-certify at least five vendor PKI certificates for Government use.	10/01/01
3. Develop five cross-agency digital signature approaches.	06/01/02

The performance measures are:

- Number of digital signatures in use by 01/01/02 with a target of 1,000,000
- Number of vendor PKI certificates cross-certified by 10/10/01 with a target of five
- Number of cross-agency digital signature approaches developed by 06/01/02 with a target of five

***Objective 1.5: Establish communities of practice and affinity groups through the use of collaborative tools.***

As common interest areas increasingly cross organizational boundaries, the Council will establish communities of practice and affinity groups through the use of knowledge management tools and practices. Collaborative software

will be developed for Government-wide use and developed around at least three specific communities of practice. These communities, concentrating on CIO issues, will be evaluated for their effectiveness in fostering interagency collaboration and service to the public. This is the "knowledge management" phase of the e-Government strategy.

The e-Government Committee will be responsible for the initiatives to establish communities of practice and affinity groups through the use of collaborative tools.

Initiatives	Milestone
1. Build collaborative software infrastructure to support communities of interest.	09/30/01
2. Develop at least three communities centered on CIO concerns.	11/01/01
3. Evaluate the effectiveness of communities of interest for interagency collaboration.	02/01/02

The performance measures are:

- Collaborative software infrastructure in place by 09/30/01
- Three communities of interests developed by 11/01/01

### **Schedule**

The charts that follow present the objectives, initiatives, and milestone dates for Goal 1.

## CIO COUNCIL STRATEGIC PLAN

FISCAL YEAR	2001				2002				2003				2004	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
<b>Goal: All Citizens Connected To The Products, Services, And Information Of Their Government</b>														
<p><b><u>Objective 1.1:</u></b>  <b><i>Develop a single point-of-entry portal model to access Government services.</i></b></p> <p>1. Support implementation of FirstGov.gov.</p> <p>2. Promote an expanded number of entry points to FirstGov.gov through "certified partnerships".</p> <p>3. Develop a strategy for implementing functional portals at five Government agencies.</p> <p>4. Support development of functional portals (e.g., Students, Seniors, and Fed-Commons).</p> <p>5. Propose alternative models to provide universal citizen access to Government information and services.</p> <p><b><u>Objective 1.2:</u></b>  <b><i>Increase the customer-value of Government sites.</i></b></p> <p>1. Promote work by agencies to modify their Web sites to support the functional portals.</p> <p>2. Support the e-Gov awards program recognizing innovative Federal sites.</p> <p>3. Support the dissemination of industry and Government "best practices" for site content.</p> <p>4. Develop Government-wide guidelines and best practices and recommend standards for electronic information and services on Federal sites.</p>	<p>◆ 10/01/00</p> <p>◆ 01/01/01</p> <p>◆ 03/31/01</p> <p>◆ 03/01/01</p> <p>◆ 09/01/01</p> <p>◆ 12/01/01</p>													

## CIO COUNCIL STRATEGIC PLAN

FISCAL YEAR	2001				2002				2003				2004	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
<b>Goal: All Citizens Connected To The Products, Services, And Information Of Their Government</b>														
<p><b><u>Objective 1.2:</u></b> <b><i>Increase the customer-value of Government sites. (con't)</i></b></p> <p>5. Establish five moderated, open discussion groups for citizen interaction with agencies.</p> <p>6. Assist Federal agencies in offering online rule making such that 50% are online.</p> <p>7. Promote the transition of Federal data to geo-spatial form.</p> <p>8. Support OMB in the smooth implementation of GPEA.</p>				◆ 09/30/01										
									◆ 10/01/02					
										◆ 02/01/03				
													◆ 10/01/03	
<p><b><u>Objective 1.3:</u></b> <b><i>Make transactions across all levels of Government seamless.</i></b></p> <p>1. Develop and issue a strategy for integrating electronic information and services with State Governments.</p> <p>2. Develop and issue a strategy for integrating electronic information and services with local Governments.</p> <p>3. Plan, organize and hold an Inter-Governmental e-Congress.</p> <p>4. Develop and issue a strategy for integrating electronic information and services in specific functional areas with five other countries.</p> <p>5. Plan, organize, and hold an international e-Gov Congress.</p>		◆ 03/01/01												
			◆ 09/01/01											
				◆ 12/01/01										
									◆ 01/01/03					
													◆ 06/01/03	



## CIO COUNCIL STRATEGIC PLAN

FISCAL YEAR	2001				2002				2003				2004	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
<b>Goal: All Citizens Connected To The Products, Services, And Information Of Their Government</b>														
<p><b><u>Objective 1.4:</u></b>  <b><i>Citizen transactions and interactions with Government agencies are easily and properly authenticated.</i></b></p> <p>1. Promote the use of digital signatures by citizens and businesses.</p> <p>2. Cross-certify at least five vendor PKI certificates for Government use.</p> <p>3. Develop five cross-agency digital signature approaches.</p> <p><b><u>Objective 1.5: Establish communities of practice and affinity groups through the use of collaborative tools.</u></b></p> <p>1. Build collaborative software infrastructure to support communities of interest.</p> <p>2. Develop at least three communities centered on CIO concerns.</p> <p>3. Evaluate the effectiveness of communities of interest for interagency collaboration.</p>														
			01/01/01				01/01/02							
				10/01/01										
									06/01/02					
					09/30/01									
						11/01/01								
								02/01/02						

**GOAL 2: INTEROPERABLE AND INNOVATIVE GOVERNMENT-WIDE IT INITIATIVES**

**INTEROPERABILITY AND INNOVATION**

The goal of interoperable and innovative Government-wide IT initiatives reflects an on-going Council focus. The focus is on laying the foundation for Government business processes and systems to operate seamlessly. This has gained importance given the impact of e-Government. The Council identified five objectives to support the achievement of this goal.

- 1) Develop an interoperable Government-wide PKI based on sound policy guidance framework.
- 2) Establish the use of open, standards-based IT architectures.
- 3) Develop a formal Government-industry partnership to institute an IT accessibility test standard.
- 4) Foster sharing of best practices related to Federal IT applications.
- 5) Develop models of Knowledge Management Communities of Practice.

**Background:**

Although considerable work has been accomplished to address the narrow focus and lack of interoperability in today's systems, much remains to be done. The mandates of the Clinger-Cohen Act must be completely fulfilled. Agencies must now address how to fully implement their architectures and related standards. The Federal Enterprise Architecture Framework has been defined but needs to be fleshed out.

The rapid development of e-Government has also resulted in additional interoperability concerns. These include a Government-wide PKI to facilitate Government-wide transaction processing and information sharing. The Council recognizes the importance of security and privacy considerations in the context of the wider interoperability arena.

Two additional areas that the Council has identified for action are relatively recent. The first is the need for accessibility models and architectures to support the implementation of recent regulations and legislation (e.g., Section 508). The second is Knowledge Management (KM) with an emphasis on exploring ways of using this promising approach.

## CIO COUNCIL STRATEGIC PLAN

### Accomplishments:

**Federal PKI** - The Council oversaw the preparation of the charter for the Federal PKI Policy Authority, which will oversee the operation of the Federal Bridge Certification Authority (FBCA). The Council was instrumental in the design and architecture of the FBCA, in establishing a FBCA prototype and in conducting a large PKI interoperability test. The Council also published a report on Federal agency PKI efforts.

**Partnerships** - The Council developed and maintained close working relationships with the Governments of Canada and Australia, several states (New Jersey, Georgia, and Virginia), commercial vendors, and private companies. These partnerships were forged in relation to the Council's PKI, Knowledge Management, and other interoperability initiatives.

**Knowledge Management** - The Council recognized the importance of Knowledge Management and established a working group to focus on it. A KM primer has been published and mechanisms have been put in place to share KM strategies and best/first practices.

**Electronic Document Standards** - The Council supported and sponsored the Electronic Documents Conference, which provided a forum for identifying electronic document standard initiatives and issues in industry and Government. The Conference sought to prioritize the electronic document standards work needed in the year 2000-2005 time frame and to identify the standards bodies that would accomplish it.

**Architecture Alignment and Assessment** - The Council developed documents to assist Federal agencies in complying with OMB IT architecture guidance (under OMB A-130). The alignment and assessment process was piloted at two agencies. A guide was developed to encourage agencies to integrate the architecture assessment and alignment process with the capital planning process to support the full analysis of potential IT investments.

**Federal "White Pages"** - The Council continued to support the Federal "White Pages" initiative. Due in part to the Council's interest and support, the number of agencies contributing to the "White Pages" reached 20. The participating agencies have submitted over 420,000 entries.

## CIO COUNCIL STRATEGIC PLAN

**Objective 2.1:**

***Develop an interoperable Government-wide Public Key Infrastructure (PKI) based on a sound policy/guidance framework.***

The Council promotes the interoperability of products and protocols within a Government-wide PKI. Through this process the Council will: identify Federal Government PKI requirements; recommend policies, procedures, and standards development activities that support a FPKI; provide oversight of PKI activities in FPKI pilot projects; and make recommendations regarding establishment, demonstration, and operation of a FPKI.

The Enterprise Interoperability and Emerging IT Committee will have the lead responsibility for the initiatives related to the development of a Government-wide PKI. The Security, Privacy and Critical Infrastructure and e-Government Committees will support the initiatives.

Initiatives	Milestones
1. Implement the Federal Bridge Certification Authority, using at least four different Certification Authority products.	03/30/01
2. Interoperate with at least one foreign Government PKI and at least one State or local Government PKI.	03/30/02
3. Evolve the Federal White Pages Directory ("directory.gov") to support public certificates for the Government-wide PKI infrastructure.	09/30/02.
4. Recommend guidelines for the use of PKI in securing Government services.	05/31/01

The performance measures are:

- Implemented Federal Bridge Certification Authority using four

different Certification Authority products by 03/30/01

- Interoperability test successfully conducted with one foreign Government and one State by 03/30/02

**Objective 2.2:**

***Establish the use of open, standards-based architectures.***

One of the foundation components for interoperability is a Government-wide enterprise architecture that provides models and standards that identify and define the information services used throughout the Government. The Council will explore various approaches and models to develop a Federal IT architecture. The Council will provide the conceptual framework for a Federal IT architecture that will guide the further development of agency architectures; promulgate the use of IT standards that support a Federal enterprise information architecture; and develop strategies for the proliferation of beneficial technologies within the Federal architecture framework.

The initiatives related to the establishment of open, standards-based architectures will be supported by the Enterprise Interoperability and Emerging IT Committee.

## CIO COUNCIL STRATEGIC PLAN

Initiatives	Milestones
1. Create models for Federal architecture segments.	<ul style="list-style-type: none"> <li>● 2 by 09/30/01</li> <li>● an additional 3-5 by 09/30/02</li> </ul>
2. Promote common processes in specific functional areas across Government agencies.	12/01/01
3. Develop an online information resource (at xml.gov) defining and documenting an evolving strategy and a set of tasks for the effective and well-coordinated usage of eXtensible Markup Language (XML) to support governmental functions.	09/30/01.
4. Develop and promote a process for ensuring that architectural concepts incorporate emerging technologies.	09/30/02
5. Develop and promote a process that links IT Capital Planning and IT Architecture.	01/31/01

The performance measures are:

- Number of models for Federal architecture segments by 09/30/02 with a target of five to seven
- XML strategy and tasks published at xml.gov by 09/30/01
- Number of cross-agency processes developed by 09/30/02 with a target of at least two (one for linking Capital Planning and IT Architecture processes; the other for integrating new technologies into the development of Federal agency architectures)

### **Objective 2.3:**

***Promote the adoption of accessible technology and develop a formal partnership between the Government and industry to work toward the institution of an IT accessibility test standard.***

Accessibility by the disabled to IT services is emerging as a critical issue. The Council is promoting the adoption of accessible technologies. The Council is also supporting efforts to assist agencies in sharing best practices to conform to Access Board regulatory standards.

The Council will support the activities of the Access Board in the development and maintenance of accessibility requirements and standards for the Government. Additionally, the Council will provide a process to identify emerging technologies of potential benefit to individuals with special accessibility needs.

The Enterprise Interoperability and Emerging IT Committee will implement the initiatives related to the development of architectures to support accessibility.

Initiatives	Milestones
1. Develop a process to periodically review how innovative technologies contribute to achieving accessible IT architectures.	03/31/01
2. Design and implement a process to identify and prioritize near-term action and long-range research needs to address remaining Government-wide IT accessibility challenges.	03/31/01

## CIO COUNCIL STRATEGIC PLAN

The performance measure is:

- Development of the two processes (one for assessing the contribution of new technologies to improved accessibility; the other for prioritizing research needs) by 03/31/01

**Objective 2.4:**

***Foster collaboration and sharing of best practices related to Federal IT applications.***

Federal Government agencies have a wealth of knowledge and experience in the development and implementation of IT applications. Increasingly, agencies are recognizing the benefits of inter-agency collaboration for the development of IT applications meeting common requirements. The Council will support the development of affinity groups for the sharing of information related to the use of IT applications within the Federal Government. The particular focus will be system interoperability issues. The affinity groups will allow for the identification of opportunities for collaboration across agencies.

The Enterprise Interoperability and Emerging IT Committee will be responsible for the initiatives related to collaboration and sharing of best practices for Federal IT applications.

Initiatives	Milestones
1. Establish affinity groups for common business processes.	03/01/01
2. Define three to five opportunities for common systems across two or more agencies.	03/31/02

The performance measures are:

- Number of affinity groups established by 03/01/01
- Number of opportunities for use of common systems defined by 03/31/02 with a target of three to five

**Objective 2.5:**

***Develop models of Knowledge Management Communities of Practice.***

In the area of Knowledge Management (KM), the Council will sponsor the creation of Communities of Practice within the Federal Government. The Council will identify best practices in knowledge management within and beyond Federal agencies; encourage the dissemination of information related to the knowledge management discipline; and ensure the development of competency profiles for agency Chief Knowledge Officers.

The initiatives for the development of models of KM Communities of Practice are the responsibility of the Enterprise Interoperability and Emerging IT Committee.

Initiatives	Milestones
1. Establish virtual communities of practice through the knowledge management portal site ("www.km.gov").	06/30/01
2. Identify, collect, and disseminate best/first practices in knowledge management across the Federal Government.	07/31/01
3. Identify Chief Knowledge Officer competencies and establish Chief Knowledge Officer curriculum with academia and industry leaders in knowledge management.	08/31/01

## **CIO COUNCIL STRATEGIC PLAN**

The performance measures are:

- Number of virtual communities established by 06/30/01
- Knowledge Management best/first practices guide issued by 07/31/01

### **Schedule**

The following pages present the objectives, initiatives, and milestone dates for Goal 2.

## CIO COUNCIL STRATEGIC PLAN

FISCAL YEAR	2001				2002				2003				2004	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
<b>Goal: Interoperable And Innovative Government-Wide IT Initiatives</b>														
<p><b><i>Objective 2.1:</i></b>  <b><i>Develop an interoperable Government-wide Public Key Infrastructure (PKI) based on a sound policy/guidance framework</i></b></p> <p>1. Implement the Federal Bridge Certification Authority, using at least four different Certification Authority products.</p> <p>2. Interoperate with at least one foreign Government PKI and at least one State or local Government PKI.</p> <p>3. Evolve the Federal White Pages Directory ("directory.gov") to support public certificates for the Government-wide PKI infrastructure.</p> <p>4. Recommend guidelines for the use of PKI in securing government services.</p> <p><b><i>Objective 2.2:</i></b>  <b><i>Establish the use of open, standards-based architectures.</i></b></p> <p>1. Create models for Federal architecture segments.</p> <p>2. Promote common processes in specific functional areas across Government agencies.</p> <p>3. Develop an on-line information resource (at xml.gov) defining and documenting an evolving strategy and set of tasks for the effective and well-coordinated usage of the eXtensible Markup Language (XML) to support government functions.</p>			03/30/01											
						03/30/02								
								09/30/02						
		05/31/01												
				09/30/01				09/30/02						
					12/01/01									
				09/30/01										





## CIO COUNCIL STRATEGIC PLAN

FISCAL YEAR	2001				2002				2003				2004	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
<b>Goal: Interoperable And Innovative Government-Wide IT Initiatives</b>														
<p><b><u>Objective 2.4:</u></b>  <b><i>Foster collaboration and sharing of best practices related to Federal IT applications.</i></b></p> <p>1. Establish affinity groups for common business processes</p> <p>2. Define three to five opportunities for common systems across two or more agencies.</p>														
<p><b><u>Objective 2.5:</u></b>  <b><i>Develop models of Knowledge Management Communities of Practice.</i></b></p> <p>1. Establish virtual communities of practice through the knowledge management portal site ("www.km.gov").</p> <p>2. Identify, collect, and disseminate best/first practices in knowledge management across the Federal Government</p> <p>3. Identify Chief Knowledge Officer competencies and establish Chief Knowledge Officer curriculum with academia and industry leaders in knowledge management.</p>														

**GOAL 3: A SECURE AND RELIABLE INFORMATION INFRASTRUCTURE THAT THE CUSTOMER CAN ACCESS AND TRUST**

**SECURITY AND PRIVACY**

The rapid advances in technology, interconnectivity, and expanding use of the Internet have reinforced the priority on adequate security and privacy policies, processes and infrastructures. Federal agencies realize that they have a continuing and growing responsibility to ensure that systems and information are secure, that transactions and information are private and that critical infrastructure is protected. The Council identified eight objectives related to security and privacy.

- 1) Expand and operate a Security Best Practices repository.
- 2) Develop an initial Security Assessment Capability for Federal agencies.
- 3) Implement a Government-wide process to collect, analyze, and rapidly disseminate security incident and early warning information.
- 4) Develop a model security risk management program for use by Federal agencies.
- 5) Work to establish Critical Infrastructure guidelines and recommendations.
- 6) Protect personal privacy in Government electronic information systems.

- 7) Publish example security and privacy practices for common electronic services.
- 8) Recommend policies and guidelines to improve the protection of citizen and corporate information within Federal systems.

**Background**

The security and reliability of the Government's information infrastructure is a continuing focus for the Council. The Council wants to build on the work that it and its member agencies have accomplished to maintain the security of Federal systems, protect the privacy of citizen information, and safeguard the Government's critical infrastructure.

The Council continues to promote security and privacy best practices, tools, training, and model agency policies that are consistent with OMB Circular A-130 (Appendices I and III), NIST (National Institute of Standards and Technology) security guidance and the Privacy Act. In addition, the Council continues to work with agencies to support the implementation of Presidential Decision Directive (PDD) - 63, issued on May 28, 1998. This declared that "the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our

## CIO COUNCIL STRATEGIC PLAN

critical infrastructure including especially our cyber system".

Privacy requirements are another focus area for the Council. Recent incidents such as the use of "cookies" (a "cookie" is computer code that allows Internet companies to track who uses their sites) have resulted in new policies and strictures on agency systems and infrastructures. Agencies also need to comply with the requirements of the Children's OnLine Privacy Protection Act (COPPA).

### Accomplishments

#### **Information Technology Security**

**Assessment** - The Council has developed an Information Technology Security Assessment Framework that provides the means for Federal agencies to determine the current health of their security programs and, where necessary, to establish a target for improvement. Version 1 of this document will be published October 30, 2000. The Framework must be an integral component of an on-going security self-assessment by the agencies.

#### **Best Security Practices (BSPs)**

BSPs are essential components of sound security programs. Because no coordinated Government initiative has existed to put BSPs in the hands of Federal organizations, the Security Practices Subcommittee was formed to collect, document, and develop a Web-based repository for BSPs<sup>1</sup>. The repository is fully functional and is found

at [www.bsp.cio.gov](http://www.bsp.cio.gov).

**Privacy Requirements** - The Council endorsed the IRS's "Privacy Impact Assessment" as a best practice for evaluating privacy needs and risks on information systems, especially new or upgraded systems. The IRS model is particularly relevant since it is designed to evaluate privacy needs on information systems that contain personal and financial data on virtually every taxpaying resident with extremely rigorous privacy requirements.

#### **Computer Incident and Response**

The Council's Sample Policy Working Group has prepared a draft of a "Computer Incident Response and Handling" policy. Based on the Department of Energy's (DOE) policy implemented by the Computer Incident Advisory Center, this sample policy is intended to serve as a guideline for other agencies.

**e-Security** - As the Federal Government continues to create e-Government services - thus changing the way citizens and companies interact with government - a major issue is information security, including the validity, reliability, and privacy of stored and transmitted information. In light of this issue, the Council has partnered with the CFO Council and the ITAA to develop and identify security solutions that enable delivery of services while ensuring adequate security in a risk-balanced implementation. Version 1 of this document is expected in the fall of 2000.

#### **Partnership with R&D Universities**

The Council has identified the opportunity for agencies to submit proposals through the National Science Foundation to partner with R&D

---

<sup>1</sup> A best security practice is a method, proven by effective experience, that people use to perform a security-related task.

## CIO COUNCIL STRATEGIC PLAN

universities to address IT security and privacy challenges.

**Critical Infrastructure** - The Council has sponsored Critical Infrastructure Protection Day, Hacker Awareness Day, and has participated as a co-sponsor in other conferences, namely Defending Cyberspace '99 and the National Information Systems Security Conference. The Council has actively participated in the Critical Infrastructure Assurance Office (CIAO) sponsored Critical Infrastructure Working Group to discuss Critical Infrastructure Protection issues across government and industry.

## CIO COUNCIL STRATEGIC PLAN

**Objective 3.1:**  
***Expand and operate a Security Best Practices repository.***

The best practices will help Federal agencies implement and configure IT safeguards. The capabilities of the current CIO Council sponsored Best Security Practices Web repository (www.bsp.cio.gov) will be expanded to include an online, self guided, "how to" tutorial and over 200 BSPs.

The initiatives related to the security best practices repository are the responsibility of the Security, Privacy, and Critical Infrastructure Committee.

Initiatives	Milestones
1. Provide self-guided online "how to" security tutorial.	03/31/01
2. Provide users 200+ BSPs with a monthly turnover/refresh rate of 10%.	09/30/01

The performance measures are:

- On-line tutorial operational by 03/31/01
- Number of BSPs issued by 09/30/01 with a target of over 200

**Objective 3.2:**  
***Develop an initial Security Assessment Capability for Federal agencies.***

The Council has targeted the Information Technology Security Assessment Framework (ITSAF) for further development. The ITSAF will result in performance criteria based on implementing existing policy. Agencies will use the criteria to determine whether

they meet existing standards and to identify areas for improvement.

The Security, Privacy, and Critical Infrastructure Committee will continue to be responsible for the initiatives related to the development of an initial security assessment capability.

Initiatives	Milestones
1. Publish Version 1.0 of the Information Technology Security Assessment Framework.	10/30/00
2. Publish measures in support of Version 1.0 of the Information Technology Assessment Framework.	06/30/01

The performance measures are:

- Version 1.0 of ITSAF issued by 10/30/00
- Measures to support ITSAF published by 06/30/01

**Objective 3.3:**  
***Implement a Government-wide process to collect, analyze, and rapidly disseminate security incident and early warning information.***

The Council will be working with others to develop a top-level process description on how to use the Federal Computer Incident Response Capability (FedCIRC) as the focal point for sending out early warning information on security incidents. The Council will work with GSA and agency CIOs to demonstrate the process to ensure that it provides an operationally effective early warning mechanism and that it is effective for rapidly analyzing the impact of incidents.

The Security, Privacy, and Critical Infrastructure Committee will be responsible for the initiatives related to

## CIO COUNCIL STRATEGIC PLAN

the implementation of a Government-wide incident process.

Initiatives	Milestones
1. Identify and document roles and responsibilities to implement a Federal Government-wide incident handling and early warning system.	10/31/00
2. Demonstrate operational effectiveness of the early warning capability using an exercise.	07/31/01

The performance measure is:

- Exercise of an operational security incident early warning capability by 07/31/01

**Objective 3.4:**  
***Develop a model security risk management program for use by Federal agencies.***

The Council will work with NIST and other Federal agencies to develop better guidelines on how to perform risk management. The intent is to go beyond the risk assessment model and demonstrate how to manage the outcome.

The development of a model security risk management program will be the responsibility of the Security, Privacy, and Critical Infrastructure Committee.

Initiatives	Milestones
1. Work with key stakeholders to develop and publish a methodology to manage risk.	12/01/01

The performance measure is:

- Publication of a risk management methodology by 12/01/01

**Objective 3.5:**  
***Work to establish Critical Infrastructure guidelines and recommendations.***

The Council will work to establish Critical Infrastructure Protection (CIP) guidelines and recommendations for use by governmental organizations for funding, training, business case development and priority requirements. This work will be carried out in collaboration with a number of different groups such as CIAO, OMB, and NASIRE.

The Security, Privacy, and Critical Infrastructure Committee will be responsible for the initiatives to establish critical infrastructure guidelines and recommendations.

## CIO COUNCIL STRATEGIC PLAN

Initiatives	Milestones
1. Assist the National Coordinator, OMB and the CIAO in tracking progress in the implementation of PDD-63.	03/30/01
2. Work with the CIAO, GSA, OMB, and other governmental entities to explore and develop recommendations on funding mechanisms for agencies to use for implementing PDD-63.	03/01/02
3. In conjunction with OMB and CIAO, recommend guidelines for Tier Two agencies to use as a model in order to meet the requirements of PDD-63.	06/30/01
4. Publicize information assurance/information security competencies and develop a process for public and private training providers to map to the competencies.	09/30/02
5. Create a CIP primer, including a brief video, to emphasize the business case and priority requirements of CIP for Federal executives.	03/31/02
6. Sponsor a broad Federal CIP awareness campaign about cyber threats and employee responsibilities.	09/30/01
7. Explore ways to work with NASIRE in order to promote CIP awareness and processes with our system/infrastructure partners.	09/30/02

The performance measures are:

- Recommendations on PDD-63 implementation funding mechanisms developed by 03/01/02
- Guidelines issued for Tier Two agencies to use as a CIP model by 06/30/01
- CIP primer issued by 03/31/02
- Federal CIP awareness program in operation by 03/31/02

### **Objective 3.6:**

#### ***Protect personal privacy in Government electronic information systems.***

The highly personal and sensitive nature of data contained in Federal systems has to be protected. Concerns have been expressed in many quarters about the privacy of personal information and transactions with Federal agencies. The implementation of various measures to ensure that Federal agencies are protecting personal privacy in their information systems is the focus of this objective.

The Security, Privacy, and Critical Infrastructure Committee will be responsible for the initiatives to protect personal privacy in Federal electronic information systems.

Initiatives	Milestones
1. Promote the effective implementation of OMB guidance on Website privacy policies and assist agencies in reporting on their efforts to comply with such policies and on other privacy practices in the budget process.	12/01/00
2. Explore methods of ensuring privacy protection in Federal authentication systems.	06/01/01
3. Promote the development and appropriate use of privacy impact assessments in the development of new Government computer systems.	08/01/01
4. Develop and provide sample guidance to agencies on complying with the standards in COPPA.	05/01/01

The performance measures are:

- Sample guidance on complying with COPPA issued by 05/01/01



## CIO COUNCIL STRATEGIC PLAN

- Guidelines on how to integrate a privacy impact assessment into systems development processes issued by 08/01/01

**Objective 3.7:**

***Publish example security and privacy practices for common electronic services.***

Interoperability and security are closely linked. Security concerns and issues are key components of technology solutions that span several agencies. The Council is sponsoring an initiative with the CFO Council and the ITAA to learn about effective practices for information security and privacy for the delivery of Internet and Web-based capabilities by Federal agencies. As a starting point for this effort, the project group identified three specific service delivery categories in which Government and private industry can learn from each other regarding appropriate computer security and privacy solutions that can be implemented with confidence in the near term. The three categories selected for initial focus are:

- Web-based information sharing services
- Government and industry procurement
- Financial transactions with the public, e.g., applying and receiving benefits from Government agencies such as the Social Security Administration.

Current practices for the three selected categories of electronic services will be

identified and will be updated on a continuing basis. Additionally, there will be further development of security and privacy practices in other areas of electronic service delivery.

The Security, Privacy, and Critical Infrastructure Committee will be primarily responsible for the initiatives that support the example security and privacy practices. This Committee will coordinate its activities with the e-Government and Enterprise Interoperability and Emerging IT Committees.

Initiatives	Milestones
1. Identify example security and privacy solutions for Web-based information sites, financial transactions, and procurement transactions.	12/30/00
2. Update initial example solutions and expand coverage of electronic services.	09/30/01

The performance measure is:

- Number of example security and privacy solutions identified for Web-based information sites, financial or procurement transactions by 12/30/00

**Objective 3.8:**

***Recommend policies and guidelines to improve protection of citizen and corporate information within Federal systems.***

The protection of citizen and corporate information is of major concern as Federal applications and infrastructures become more interoperable. The Council will develop recommendations for specific policies or standards needed to support cross-Government initiatives in a secure manner and ensure privacy

## CIO COUNCIL STRATEGIC PLAN

protection. In the near term, the Council will define agencies' needs for the protection of proprietary information.

The Security, Privacy, and Critical Infrastructure Committee will be responsible for the initiatives that result in the recommended policies and guidelines to improve protection and corporate information within Federal systems.

Initiatives	Milestones
1. Work with OMB and NIST to develop three draft or sample policies for use by Federal agencies in the areas of privacy and security.	09/30/02

The performance measure is:

- Number of sample privacy or security policies developed by 09/30/02 with a target of three

### **Schedule**

The following pages present the objectives, initiatives, and milestone dates for Goal 3.

## CIO COUNCIL STRATEGIC PLAN

FISCAL YEAR	2001				2002				2003				2004	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
<b>Goal: A Secure And Reliable Information Infrastructure That The Customer Can Access And Trust</b>														
<p><b><u>Objective 3.1:</u></b>  <b><i>Expand and operate a Security Best Practices repository.</i></b></p> <p>1. Provide self-guided online "how to" security tutorial.</p> <p>2. Provide users 200+ BSPs with a monthly turnover/refresh rate of 10%.</p>			◆ 03/31/01											
<p><b><u>Objective 3.2:</u></b>  <b><i>Develop an initial Security Assessment Capability for Federal agencies.</i></b></p> <p>1. Publish Version 1.0 of the Information Technology Security Assessment Framework.</p> <p>2. Publish measures in support of Version 1.0 of the Information Technology Assessment Framework.</p>	◆ 10/30/00						◆ 06/30/01							
<p><b><u>Objective 3.3:</u></b>  <b><i>Implement a Government-wide process to collect, analyze, and rapidly disseminate security incident and early warning information.</i></b></p> <p>1. Identify and document roles and responsibilities to implement a Federal Government-wide incident handling and early warning system.</p> <p>2. Demonstrate operational effectiveness of the early warning capability using an exercise.</p>	◆ 10/31/00													

## CIO COUNCIL STRATEGIC PLAN

FISCAL YEAR	2001				2002				2003				2004	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
<b>Goal: A Secure And Reliable Information Infrastructure That The Customer Can Access And Trust</b>														
<p><b><u>Objective 3.4:</u></b>  <b><i>Develop a model security risk management program for use by Federal agencies.</i></b></p> <p>1. Work with key stakeholders to develop and publish a methodology to manage risk.</p>					12/01/01									
<p><b><u>Objective 3.5:</u></b>  <b><i>Work to establish Critical Infrastructure guidelines and recommendations.</i></b></p> <p>1. Assist the National Coordinator, OMB and the CIAO in tracking progress in the implementation of PDD-63.</p> <p>2. Work with the CIAO, GSA, OMB, and other governmental entities to explore and develop recommendations on funding mechanisms for agencies to use for implementing PDD-63.</p> <p>3. In conjunction with OMB and CIAO, recommend guidelines for Tier Two agencies to use as a model in order to meet the requirements of PDD-63.</p> <p>4. Publicize information assurance/information security competencies and develop a process for public and private training providers to map to the competencies.</p>		03/30/01				03/01/02								
			06/30/01											
									09/30/02					



## CIO COUNCIL STRATEGIC PLAN

FISCAL YEAR	2001				2002				2003				2004	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
<b>Goal: A Secure And Reliable Information Infrastructure That The Customer Can Access And Trust</b>														
<p><b><u>Objective 3.6:</u></b> <b><i>Protect personal privacy in Government electronic information systems. (con't)</i></b></p> <p>4. Develop and provide sample guidance to agencies on complying with the standards in COPPA.</p>				05/01/01										
<p><b><u>Objective 3.7:</u></b> <b><i>Publish example security and privacy practices for common electronic services.</i></b></p> <p>1. Identify example security and privacy solutions for Web-based information sites, financial transactions, and procurement transactions.</p> <p>2. Update initial example solutions and expand coverage of electronic services.</p>	12/31/00				09/30/01									
<p><b><u>Objective 3.8:</u></b> <b><i>Recommend policies and guidelines to improve protection of citizen and corporate information within Federal systems.</i></b></p> <p>1. Work with OMB and NIST to develop three draft or sample policies for use by Federal agencies in the areas of privacy and security.</p>													09/30/02	

**GOAL 4: IT SKILLS AND RESOURCES TO MEET MISSION OBJECTIVES**

**SKILLS AND RESOURCES**

Federal agencies continue to be faced with the reality that IT human resources are in short supply. The increasing need for qualified IT professionals puts the Government in competition with private sector organizations with radically different compensation structures and advancement opportunities. The Council has identified two objectives to achieve the goal.

- 1) Improve the Federal Government's ability to attract and retain a top-notch IT workforce.
- 2) Expand effective IT education and training opportunities for the existing Federal workforce.

**Background**

The issue of the Federal Government's ability to attract, retain, and train a qualified work force is the primary focus of the Council's activities related to IT workforce.

The Clinger-Cohen Act, the work of the National Partnership for Reinventing Government, the Government Performance and Results Act (GPRA) and the General Accounting Office (GAO) have provided guidance to Government agencies that support action to ensure that the Government's workforce has the skills to operate in today's work place. The Council continues to address this challenge.

The Council has already initiated several projects such as the "Federal IT Workforce Challenge" report issued in 1999 and the Strategic and Tactical Advocates for Results (STAR) Program. These projects are to be continued.

**Accomplishments**

**IT Occupational Pay Analysis** - The Council contracted with the National Academy of Public Administration (NAPA) to produce a report which provides an initial cost and benefit analysis of basic alternatives for an IT Occupational Pay System. The report also provides the basic principles to be included in such a system.

## CIO COUNCIL STRATEGIC PLAN

**Implementation of the "Federal IT Workforce Challenge" Report** - The Council monitored the implementation of the "Federal IT Workforce Challenge" report. Reports on the status of the implementation of the report's recommendations were produced.

**IT Executive Development** - The Council participated in an OPM Inter-Agency Working Group that is developing a new directive authorizing agencies to exchange their best and brightest IT executives for developmental assignments.

**Revised Classification and Qualification Standards** - The Council worked closely with the Office of Personnel Management (OPM) to provide input to OPM's revised classification and qualification standards for the Information Technology Management series.

**Core CIO Competencies** - The Council also revised the Clinger-Cohen Act Core Competencies.

**CIO University** - The Council continued to support the CIO University. Consequently, the CIO University graduated the first eighteen students (two from Government and sixteen from private industry) on July 12, 2000. Graduates received CIO University Certificates signed by Vice President Al Gore.

**STAR Program** - The Council also continued to support the STAR Program. The STAR Program is a graduate-level program designed to create an optimal learning environment for professionals. The STAR Program graduated its first two classes in December 1999 and in May 2000.

**Computer Competency Assessment Skills** - The Council completed a pilot project that tested a system for assessing basic computer competencies using Internet technologies.



## CIO COUNCIL STRATEGIC PLAN

***Objective 4.1:  
Improve the Federal Government's ability to attract and retain a top-notch IT workforce.***

The Federal Government faces tremendous challenges in employing and paying its civilian IT workforce. Chief among them are disparate pay levels and an inflexible and outdated occupational structure. The Council will work with OPM to restructure the IT occupational and associated pay categories. In addition, the Council will produce a report, prepared by NAPA, which provides an initial cost and benefit analysis of basic alternatives for an IT Occupational Pay System. The report will address the basic principles to be included in such a system. The report will propose solutions for the problems identified in today's system with due regard for individual requirements of each agency. The Council will work actively with OPM to define strategies for implementing the recommendations of the NAPA study on compensation and retention issues.

The Council will also encourage the full implementation of the recommendations of the "Federal IT Workforce Challenge" report. It will reinforce the use of hiring flexibilities available to Federal agencies to recruit and retain IT professionals. To expand the IT labor supply, the Council supports the development of programs to recruit women, minorities, and people with disabilities to fill IT vacancies.

The Federal Government needs to act now to interest more students in computer professions early in their educational careers. To help address the need to increase the talent pool for IT jobs, the Council will partner with the

private sector to develop an outreach program for high schools in the Washington, DC area. The purpose of this program is to provide information and opportunities to local high school students to become aware of IT careers in the Federal Government.

The IT Workforce Committee will be responsible for the following initiatives related to the evaluation of the Government's ability to attract and retain a top-notch IT workforce.

Initiatives	Milestones
1. Establish, in partnership with the private sector, an outreach program to local high schools to develop interest in pursuing IT careers in the Federal Government.	09/30/01
2. Support full implementation of recommendations from the "Federal IT Workforce Challenge" report.	09/30/02
3. Support the implementation of the recommendations from the NAPA study of compensation and retention issues.	09/30/02

The performance objectives are:

- Outreach program targeting Washington, D.C. high school students established by 09/30/01
- Number of recommendations from the NAPA and the "Federal It Workforce Challenge" report implemented by 09/30/02

## CIO COUNCIL STRATEGIC PLAN

**Objective 4.2:**

***Expand effective IT education and training opportunities for the existing Federal workforce.***

The Council supports the continuing development of managers, staff, and IT professionals in functional training areas such as security and capital planning. The Clinger-Cohen Core Competencies serve as a tool to determine IT skills, knowledge, and education requirements. The associated learning objectives provide a level of definition and explanation of the competencies to assist Federal agencies and training institutions in developing courses and curricula to address the competency requirement. With the identification of the learning objectives associated with the CIO Core Competencies, it is imperative to develop effective methods for Federal workers to attain proficiency in one or more of these competencies in order for them to realize their career goals and maximize their value to the American taxpayer. The determination of the knowledge, skills, and abilities required for Federal workers to meet the learning objectives is the focus of the “road maps” initiative.

The Council will assist OPM in establishing an Executive Exchange Program (EEP) that will allow top managers in business and government to participate in developmental assignments to enhance their executive competencies and their effectiveness as leaders. In addition, a program for CIO Council Committee Co-Chairs to mentor proteges, who in turn could help carry out the work of the various working groups of the Council, will be established. CIOs would serve as role models and structure a mentor-protégé relationship around the professional

development needs of the individual and the specific needs of the Council.

The Council will take action to enhance the competencies and skills of agency leaders through the refinement and delivery of the STAR Program. STAR focuses on tomorrow’s government workplace - the highly strategic environment where operational functions are outsourced and agency business objectives and outcomes are key. STAR emphasizes Clinger-Cohen results-based management as well as “information technology as a strategic resource”.

The IT Workforce Committee will be responsible for the following initiatives related to the expansion of IT education and training opportunities for the existing workforce.

Initiatives	Milestones
1. Review and revise CIO Core Competencies and associated learning objectives on a biennial basis.	09/30/00 09/30/02
2. Develop “road maps” for meeting the core competency training needs of staff.	12/31/01
3. Establish the CIO Executive Exchange program in collaboration with OPM.	01/31/01
4. Establish the CIO Council Mentoring Program.	04/30/01
5. Refine and enhance the STAR Program and deliver two pilot seminars.	08/31/01

The performance objectives are:

- Updated CIO Core Competencies issued on a biennial basis
- "Road map" components to meet competency training needs developed by 12/31/01

## CIO COUNCIL STRATEGIC PLAN

- CIO Exchange Program established by 01/31/01
- CIO Council Mentoring Program established by 04/30/01
- Number of STAR seminars given by 08/31/01 with a target of two



### **Schedule**

The following pages present the objectives, initiatives, and milestone dates for Goal 4.

## CIO COUNCIL STRATEGIC PLAN

FISCAL YEAR	2001				2002				2003				2004	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
<b>Goal: IT Skills And Resources To Meet Mission Objectives</b>														
<p><b><u>Objective 4.1:</u></b> <b><i>Improve the Federal Government's ability to attract and retain a top-notch - workforce.</i></b></p> <p>1. Establish, in partnership with the private sector, an outreach program to local high schools to develop interest in pursuing IT careers in the Federal Government.</p> <p>2. Support full implementation of recommendations from the "Federal IT Workforce Challenge" report.</p> <p>3. Support the implementation of the recommendations from the NAPA study of compensation and retention issues.</p>				◆ 09/30/01										
										◆ 09/30/02				
										◆ 09/30/02				
<p><b><u>Objective 4.2:</u></b> <b><i>Expand effective IT education and training opportunities for the existing Federal workforce.</i></b></p> <p>1. Review and revise CIO Core Competencies and associated learning objectives on a biennial basis.</p> <p>2. Develop "road maps" for meeting the core competency training needs of staff.</p> <p>3. Establish the CIO Executive Exchange program in collaboration with OPM.</p>	◆ 09/30/00									◆ 09/30/02				
														◆ 12/31/01
			◆ 01/31/01											

## CIO COUNCIL STRATEGIC PLAN

FISCAL YEAR	2001				2002				2003				2004	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
<b>Goal: IT Skills And Resources To Meet Mission Objectives</b>														
<p><b><u>Objective 4.2:</u></b>  <b><i>Expand effective IT education and training opportunities for the existing Federal workforce. (con't)</i></b></p> <p>4. Establish the CIO Council Mentoring Program.</p> <p>5. Refine and enhance the STAR Program and deliver two pilot seminars.</p>				04/30/01										
					08/31/01									

**GOAL 5: COLLABORATIONS BETWEEN THE PUBLIC AND PRIVATE SECTORS ACHIEVE BETTER GOVERNMENT**

**COLLABORATION AND AWARENESS**

The development of effective collaborations between the public and private sectors is critical to the achievement of the Council's strategic vision and goals. The Council has established three objectives for achieving the collaborations.

- 1) Promote inter-governmental collaboration with representatives from all levels of government.
- 2) Establish stronger and more productive collaborative relationships between the leadership in the Federal sector and that in other sectors.
- 3) Significantly raise the level of awareness and acceptance among key stakeholders and decision-makers of the CIO Council's efforts and accomplishments.

**Background**

Outreach is an important component of the Council's activities. The focus of external outreach activities is on building partnerships and promoting collaboration with a large diverse community to include Congress, State and local governments, industry, academia, and the media. The internal focus is on transmitting the Council's positions and ideas to the CIO community and key technical staff in the agencies.

The Council will continue to undertake actions to reach its external and internal stakeholders. These activities represent a follow on to those outreach programs that the Council has already initiated.

**Accomplishments**

**Best Practices** -The Council enhanced the understanding of national security issues with the release of "Best Practices in the Federal Government, Volume II" at the Executive Leadership Conference '99. Six thousand copies of this document, which focuses on national security and emergency preparedness success stories, were distributed to public and private sector organizations.

**Promulgation Of Council Messages** - Council messages in the form of numerous news commentaries and articles by CIOs were distributed. News sources used were the *Federal*

## CIO COUNCIL STRATEGIC PLAN

*Times, Government Computer News, Federal Computer Week, E-Gov Journal, and Government Executive.* The Council completed an agreement with Post-Newsweek for an exclusive Council insert on strategic plans and goals.

**Partnerships** - The Council's visibility and partnership with international, State, and local governments to address issues of common interest were reinforced. Examples of connected communities include the International Council for Information Technology, NASIRE, and Washington, D.C. area governments.

**Common Ground Meetings** - Common Ground Meetings were designed as a new communications format to facilitate Council exchange with major organizations and associations. Two are currently scheduled and staffed: the NASIRE Conference and the Executive Leadership Conference.

**Presentation of Council Positions** - The Council's interests and positions were conveyed at three major conferences: AFCEA's Virtual Government, GSA's Interagency Resources Management Conference (IRMCO) and Post-Newsweek's FOSE. The Council participated in several other forums including Excellence in Government 2000, e-Gov, Executive Leadership Conference, and Government Technology Leadership Institute '99.

**Objective 5.1:**  
***Promote inter-governmental collaboration with representatives from all levels of Government.***

External links with Federal, State, local, and international organizations will be used to identify joint initiatives, create new partnerships, and leverage resources. Primary opportunities for these forums will include various conferences (such as NASIRE, FOSE, IRMCO, etc.). The use of the Common Ground Forums will be expanded.

The initiatives related to the promotion of inter-governmental collaboration with representatives from all levels of Government will be the responsibility of the Outreach Committee.

Initiatives	Milestones
1. Develop and conduct a number of Common Ground Forums, comprised of Federal, State, and local agencies.	09/30/02
2. Develop and conduct Congressional Common Ground Forums.	09/30/01
3. Identify inter-governmental initiatives to be completed jointly with NASIRE.	09/30/01

The performance measure is:

- Number of Common Ground Forums with Federal, State, and local agencies conducted by 09/30/02

**Objective 5.2:**  
***Establish stronger and more productive collaborative relationships between the leadership in the Federal sector and that in other sectors.***

## CIO COUNCIL STRATEGIC PLAN

The inter-Governmental partnerships are one component of the community that the Council impacts. Other sectors such as industry and academia need to be advised on the Council's positions and projects. This will be achieved using Common Ground Forums.

The initiative related to establishment of stronger and more productive collaborations between the government and other sectors will be the responsibility of the Outreach Committee.

Initiatives	Milestones
1. Develop and conduct Common Ground Forums, comprised of government, academic and industry participants, at various conferences (such as Virtual Government Conferences, IAC/ELC, FOSE, etc.)	09/30/02
2. Facilitate an ongoing exchange of ideas and information between industry leaders and the Capitol Hill community.	09/30/02

The performance objective is:

- Number of Common Ground Forums conducted with the leadership of academia and industry by 09/30/02

**Objective 5.3:**  
***Significantly raise the level of awareness and acceptance among key stakeholders and decision-makers of the CIO Council's efforts and accomplishments.***

The visibility of the Council's work and its results are another important component in its continuing efforts to build effective partnerships with stakeholders and decision-makers. The visibility will be enhanced through the

use of publications, attendance at conferences, and the use of newer technologies such as Webcast.

The initiatives related to this objective will be the responsibility of the Outreach Committee.

Initiatives	Milestones
1. Deliver the Council's transition message in a special <i>Government Computer News</i> (GCN) supplement.	11/30/00
2. Webcast a full CIO Council meeting.	11/30/00
3. Create a Council presence at major conferences (e.g., FOSE, Virtual Government, IRMCO, and TechNet).	09/30/02
4. Coordinate CIO Council coverage with major trade and national publications (e.g., <i>Federal Times</i> , <i>Government Computer News</i> , <i>Federal Computer Week</i> , <i>Government Executive</i> , <i>Wall Street Journal</i> , and the <i>Washington Post</i> ).	09/30/02

The performance measures are:

- Number of major conferences with a significant Council presence (e.g.; speech given, paper presented) by 09/30/02
- Number of CIO Council news articles or publications appearing in major trade and national publications by 09/30/02

### **Schedule**

The following pages present the objectives, initiatives, and milestone dates for Goal 5.





## CIO COUNCIL STRATEGIC PLAN

FISCAL YEAR	2001				2002				2003				2004	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
<b>Goal: Collaborations Between The Public And Private Sectors Achieve Better Government</b>														
<p><b><u>Objective 5.3:</u></b>  <b><i>Significantly raise the level of awareness and acceptance among key stakeholders and decision-makers of the CIO Council's efforts and accomplishments.</i></b></p> <p>1. Deliver the Council's transition message in a special <i>Government Computer News</i> (GCN) supplement.</p> <p>2. Webcast a full CIO Council meeting.</p> <p>3. Create a Council presence at major conferences (e.g., FOSE, Virtual Government, IRMCO, and TechNet).</p> <p>4. Coordinate CIO Council coverage with major trade and national publications (e.g., <i>Federal Times</i>, <i>Government Computer News</i>, <i>Federal Computer Week</i>, <i>Government Executive</i>, <i>Wall Street Journal</i>, and <i>the Washington Post</i>).</p>	◆	11/30/00												
	◆	11/30/00												
									◆	09/30/02				
									◆	09/30/02				

**GOAL 6: INVESTMENT MANAGEMENT POLICIES, PRACTICES, AND TOOLS THAT ENABLE IMPROVED DELIVERY OF GOVERNMENT PROGRAMS AND SERVICES**

**MANAGED INVESTMENTS**

Background

Federal agencies are required to manage IT projects as business as opposed to technical investments. IT projects have to demonstrate that they have a business value and payoff. Moreover, opportunities exist to improve the way Federal agencies acquire and manage IT. The Council has defined five major objectives that support the achievement of this goal.

Federal agencies are faced with major managerial and technical challenges as they identify, select and control IT investments. Reform legislation such as the Paperwork Reduction Act of 1995, the Federal Acquisition Streamlining Act of 1994 (FASA) and the Clinger-Cohen Act have placed requirements on how agencies manage IT investments.

- 1) Foster better integration of planning, budgeting, acquisition, and program management communities and processes.
- 2) Achieve consistent application of investment management measures, methodologies, and policies.
- 3) Seamlessly integrate Federal statutory requirements into the investment management process.
- 4) Improve the quality, accuracy, consistency, and currency of data used to support investment decision-making and meaningful reporting.
- 5) Improve information technology acquisition strategies.

The Council continues to identify and support initiatives to reinforce agencies' investment management practices. The integration of the disparate investment management processes, covering budgeting, planning, selection, evaluation, and control is an emerging issue that the Council views as important. The ongoing development of tools to help agencies manage their investment portfolios and to measure the effectiveness of their investment management processes are to be addressed.

Accomplishments

**Collaboration and Information**

**Sharing** - The Council used meetings as a forum for discussion and exchange of ideas among Federal capital planning community members and with groups with related responsibilities such as the Government Accounting Office (GAO) and CIO Council Security sub-Committee.

**Reporting Improvements** - The Council provided feedback and

## CIO COUNCIL STRATEGIC PLAN

assistance to OMB in revising OMB Circular A-11 (Exhibits 53 and 300B) to make the exhibits more user-friendly and more useful tools for OMB and the agencies.

### **Information Technology Investment Portfolio System (I-TIPS) Modification**

- The Council provided funding for modification of I-TIPS to produce OMB Exhibits 300B, 53 and 52. The Council provided funding to revise the Architecture module developed by the Department of Energy and integrate it into I-TIPS Version 3.0.

**Best Practices** - The Council worked with IAC to produce a “Smart Practices” document, identifying IT capital planning smart practices from industry and Federal agencies.

### **IT Capital Planning Self Assessment**

**Tool** - The Council developed a self-assessment tool to allow Federal organizations to assess their IT capital planning strengths and weaknesses.

**IT Performance Measures** - The Council established a sub-committee to provide a forum for identifying, defining, and promulgating IT performance measures.

## CIO COUNCIL STRATEGIC PLAN

**Objective 6.1:**

***Foster better integration of planning, budgeting, acquisition, and program management communities and processes.***

There are currently a number of Federal Councils involved in the capital planning process: the Procurement Executive Council (acquisition), the CFO Council with its Budget Officer's Advisory Council (BOAC), and the CIO Council, including the Federal Architecture Working Group. The Councils have counterpart committees that need to communicate and collaborate with each other. Investment management can serve as the focal point for collaboration and for developing requirements to improve and better integrate the processes.

The initiatives related to fostering better integration of the communities and processes for investment management are the responsibility of the Capital Planning and IT Management Committee.

Initiatives	Milestones
1. Develop a framework and agreements for working relationships and collaboration with the CFO Council and the PEC through Information Sharing Forums.	11/30/00
2. Bring in strategic planning representation to the Information Sharing Forums.	02/28/01

The performance measure is:

- Number of Information Sharing Forums (ISFs) established by 11/30/00 with a target of at least two (one with CFO Council; the other with PEC)

**Objective 6.2:**

***Achieve consistent application of investment management measures, methodologies, and policies.***

Performance measurement for IT has been a weak point for many agencies. The Council can provide tools to support agencies as they develop performance measures.

The initiatives related to achieving consistent application of investment management measures, methodologies, and policies are the responsibility of the Capital Planning and IT Management Committee.

Initiatives	Milestones
1. Develop criteria for agencies to evaluate the performance measures for their major IT investments.	06/30/01
2. Conduct pilot demonstrations at a volunteer agency to evaluate methodologies that measure the contribution of IT to mission results.	05/01/01
3. Ask agencies to conduct a self-evaluation using the criteria on their FY 2001-FY 2002 investment portfolio.	09/30/01

The performance measures are:

- Criteria for investment management performance evaluation issued by 06/30/01
- Pilot demonstration accomplished by 05/01/01
- Number of agencies using the criteria for an agency investment portfolio and process performance self-evaluation by 09/30/01

## CIO COUNCIL STRATEGIC PLAN

**Objective 6.3:**  
***Seamlessly integrate Federal statutory requirements into the investment management process.***

Existing statutory requirements that impact investment management are found in statutes such as the Clinger Cohen Act, Section 508, GPEA, GPRA, and FASA. Other requirements are coming from OMB and agencies as they consider emerging issues such as security and privacy. The Council recognizes the need to link the requirements and to incorporate them into agency investment management processes.

The initiatives related to integrating Federal statutory requirements into the investment management process are the responsibility of the Capital Planning and IT Management Committee.

Initiatives	Milestones
1. Develop a framework and agreements for working relationships and collaboration with the other CIO Council committees.	11/30/00
2. Develop guidelines and framework for linking requirements.	08/31/01

The performance measure is:

- Guidelines and framework for integrating Federal statutory requirements into the investment management process issued by 08/31/01

**Objective 6.4:**  
***Improve the quality, accuracy, consistency, and currency of data used to support investment decision-making and meaningful reporting.***

There are common elements for cost data, such as for total cost of ownership (TCO), which need to be explored, including a need to tie cost data to a particular project to improve accuracy. Additionally, risk adjusted cost data is required.

The initiative related to improving investment management data is the responsibility of the Capital Planning and IT Management Committee.

Initiatives	Milestones
1. Develop cost models, cost report capturing processes and formats for reporting; integrate with I-TIPS.	06/30/01

The performance measure is:

- I-TIPS with an integrated cost reporting module by 06/30/01

**Objective 6.5:**  
***Improve information technology acquisition strategies.***

Changes in IT acquisition approaches and strategies are necessary to allow Federal agencies to acquire the infrastructure and human resources that are necessary to accomplish their IT plans.

The initiatives related to improving IT acquisition strategies are the responsibility of the Capital Planning and IT Management Committee.

## CIO COUNCIL STRATEGIC PLAN

Initiatives	Milestones
1. Assess the viability of the Seat Management approach to acquiring information technology.	09/30/01
2. Evaluate contractual ways of assuring that highly qualified IT professionals are available to Federal agencies and share the findings with the agencies.	03/31/02

The performance measures are:

- Issue report with the definition of options to the Seat Management approach by 09/30/01
- Issue report on the contractual approaches to obtaining IT professional services by 03/31/02

### **Schedule**

The following pages present the objectives, initiatives, and milestone dates for Goal 6.

## CIO COUNCIL STRATEGIC PLAN


FISCAL YEAR	2001				2002				2003				2004	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
<b>Goal: Investment Management Policies, Practices, And Tools That Enable Improved Delivery Of Government Programs And Services</b>														
<p><b><u>Objective 6.1:</u></b>  <b><i>Foster better integration of planning, budgeting, acquisition, and program management communities and processes.</i></b></p> <p>1. Develop a framework and agreements for working relationships and collaboration with the CFO Council and the PEC through Information Sharing Forums.</p> <p>2. Bring in strategic planning representation to the Information Sharing Forums.</p> <p><b><u>Objective 6.2:</u></b>  <b><i>Achieve consistent application of investment management measures, methodologies, and policies.</i></b></p> <p>1. Develop criteria for agencies to evaluate the performance measures for their major IT investments.</p> <p>2. Conduct pilot demonstrations at a volunteer agency to evaluate methodologies that measure the contribution of IT to mission results.</p> <p>3. Ask agencies to conduct a self-evaluation using the criteria on their FY 2001-FY 2002 investment portfolio.</p>	◆	◆	◆	◆										
		11/30/00												
			02/28/01											
				06/30/01										
			05/01/01											
				09/30/01										



## CIO COUNCIL STRATEGIC PLAN

FISCAL YEAR	2001				2002				2003				2004	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
<b>Goal: Investment Management Policies, Practices, And Tools That Enable Improved Delivery Of Government Programs And Services</b>														
<p><b><i>Objective 6.3:</i></b>  <b><i>Seamlessly integrate Federal statutory requirements into the investment management process.</i></b></p> <p>1. Develop a framework and agreements for working relationships and collaboration with the other CIO Council committees.</p> <p>2. Develop guidelines and framework for linking .</p>														
<p><b><i>Objective 6.4:</i></b>  <b><i>Improve the quality, accuracy, consistency, and currency of data used to support investment decision-making and meaningful reporting</i></b></p> <p>1. Develop cost models, cost report capturing processes and formats for reporting; integrate with I-TIPS.</p>														
<p><b><i>Objective 6.5:</i></b>  <b><i>Improve information technology acquisition strategies.</i></b></p> <p>1. Assess the viability of the Seat Management approach to acquiring information technology.</p>														

## CIO COUNCIL STRATEGIC PLAN

FISCAL YEAR	2001				2002				2003				2004	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
<b>Goal: Investment Management Policies, Practices, And Tools That Enable Improved Delivery Of Government Programs And Services</b>														
<p><b><i>Objective 6.5:</i></b>  <b><i>Improve information technology acquisition strategies. (con't)</i></b></p> <p>2. Evaluate contractual ways of assuring that highly qualified IT professionals are available to Federal agencies and share the findings with the agencies.</p>						 03/31/02								

# CIO COUNCIL STRATEGIC PLAN

## APPENDIX A: EXECUTIVE ORDER 13011

### EXECUTIVE ORDER 13011 OF JULY 16, 1996 FEDERAL INFORMATION TECHNOLOGY

A Government that works better and costs less requires efficient and effective information systems. The Paperwork Reduction Act of 1995 and the Information Technology Management Reform Act of 1996 provide the opportunity to improve significantly the way the Federal Government acquires and manages information technology. Agencies now have the clear authority and responsibility to make measurable improvements in mission performance and service delivery to the public through the strategic application of information technology. A coordinated approach that builds on existing structures and successful practices is needed to provide maximum benefit across the Federal Government from this technology.

Accordingly, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

#### **Section 1. Policy.**

It shall be the policy of the United States Government that executive agencies shall:

- (a) significantly improve the management of their information systems, including the acquisition of information technology, by implementing the relevant provisions of the Paperwork Reduction Act of 1995 (Public Law 104-13), the Information Technology Management Reform Act of 1996 (Division E of Public Law 104-106) ("Information Technology Act"), and the Government Performance and Results Act of 1993 (Public Law 103-62);
- (b) refocus information technology management to support directly their strategic missions, implement an investment review process that drives budget formulation and execution for information systems, and rethink and restructure the way they perform their functions before investing in information technology to support that work;
- (c) establish clear accountability for information resources management activities by creating agency Chief Information Officers (CIOs) with the visibility and management responsibilities necessary to advise the agency head on the design, development, and implementation of those information systems. These responsibilities include: (1) participating in the investment review process for information systems, (2) monitoring and evaluating the performance of those information systems on the basis of applicable performance measures, and, (3) as necessary advising the agency head to modify or terminate those systems;
- (d) cooperate in the use of information technology to improve the productivity of Federal programs and to promote a coordinated, interoperable, secure, and shared government-wide infrastructure that is provided and supported by a diversity of private-sector supplies and a well-trained corps of information technology professionals; and
- (e) establish an interagency support structure that builds on existing successful interagency efforts and shall provide expertise and advice to agencies; expand the skill and career development opportunities of information technology professionals; improve the management and use of information technology within and among agencies by developing information technology procedures and standards and by identifying and sharing experiences, ideas, and promising practices; and provided innovative, multi-disciplinary, project-specific support to agencies to enhance interoperability, minimize unnecessary duplication of effort, and capitalize on agency successes.

#### **Section 2. Responsibilities of Agency Heads.**

The head of each executive agency shall:

- (a) effectively use information technology to improve mission performance and service to the public;

## CIO COUNCIL STRATEGIC PLAN

(b) strengthen the quality of decision about the employment of information resources to meet mission needs through integrated analysis, planning, budgeting, and evaluation processes, including:

(1) determining, before making investments in new information systems, whether the Government should be performing the function, if the private sector or another agency should support the function, and if the function needs to be or has been appropriately redesigned to improve its efficiency;

(2) establishing mission-based performance measures for information systems investments, aligned with agency performance plans prepared pursuant to the Government Performance and Results Act of 1993 (Public Law 103-62);

(3) establishing agency-wide and project-level management structures and processes responsible and accountable for managing, selecting, controlling, and evaluating investments in information systems, with authority for terminating information systems when appropriate;

(4) supporting appropriate training of personnel; and

(5) seeking the advice of, participating in, and supporting the interagency support structure set forth in this order;

(c) select CIOs with the experience and skills necessary to accomplish the duties set out in law and policy, including this order and involve the CIO at the highest level of the agency in the processes and decisions set out in this section;

(d) ensure that the information security policies, procedures, and practices of the executive agency are adequate;

(e) where appropriate, and in accordance with the Federal Acquisition Regulation and guidance to be issued by the Office of Management and Budget (OMB), structure major information systems investments into manageable projects as narrow in scope and brief in duration as practicable, consistent with the Information Technology Act, to reduce risk, promote flexibility and interoperability, increase accountability, and better correlate mission need with current technology and market conditions; and

(f) to the extent permitted by law, enter into a contract that provides for multi-agency acquisitions of information technology as an executive agent for the Government, if and in the manner that the Director of OMB considers it advantageous to do so.

### **Section 3. Chief Information Officers Council.**

(a) Purpose and Functions. A Chief Information Officers Council ("CIO Council") is established as the principal interagency forum to improve agency practices on such matters as the design, modernization, use, sharing, and performance of agency information resources. The Council shall:

(1) Develop recommendations for overall Federal information technology management policy, procedures, and standards;

(2) share experiences, ideas, and promising practices, including work process redesign and the development of performance measures, to improve the management of information resources;

(3) identify opportunities, make recommendations for, and sponsor cooperation in using information resources;

(4) assess and address the hiring, training, classification, and professional development needs of the Federal Government with respect to information resources management;

(5) make recommendations and provided advice to appropriate executive agencies and organizations, including advice to OMB on the government-wide strategic plan required by the Paperwork Reduction Act of 1995; and

## CIO COUNCIL STRATEGIC PLAN

(6) Seek the views of the Chief Financial Officers Council, Government Information Technology Services Board, Information Technology Resources Board, Federal Procurement Council, industry, academia, and State and local governments on matters of concern to the Council as appropriate.

(b) Membership. The CIO Council shall be composed of the CIOs and Deputy CIOs of the following executive agencies plus two representatives from other agencies:

1. Department of State;
2. Department of the Treasury;
3. Department of Defense;
4. Department of Justice;
5. Department of the Interior;
6. Department of Agriculture;
7. Department of Commerce;
8. Department of Labor;
9. Department of Health and Human Services;
10. Department of Housing and Urban Development;
11. Department of Transportation;
12. Department of Energy;
13. Department of Education;
14. Department of Veterans Affairs;
15. Environmental Protection Agency;
16. Federal Emergency Management Agency;
17. Central Intelligence Agency;
18. Small Business Administration;
19. Social Security Administration;
20. Department of the Army;
21. Department of the Navy;
22. Department of the Air Force;
23. National Aeronautics and Space Administration;
24. Agency for International Development;
25. General Services Administration;
26. National Science Foundation;
27. Nuclear Regulatory Commission; and
28. Office of Personnel Management.

The Administrator of the Office of Information and Regulatory Affairs of OMB, the Controller of the Office of Federal Financial Management of OMB, the Administrator of the Office of Federal Procurement Policy of OMB, a Senior Representative of the Office of Science and Technology Policy, the Chair of the Government Information Technology Services Board, and the Chair of the Information Technology Resources Board shall also be members. The CIO Council shall be chaired by the Deputy Director for Management of OMB. The Vice Chair, elected by the CIO Council on a rotating basis, shall be an agency CIO.

### **Section 4. Government Information Technology Services Board.**

(a) Purpose and Functions. A Government Information Technology Services Board ("Services Board") is established to ensure continued implementation of the information technology recommendations of the National Performance Review and to identify and promote the development of innovative technologies, standards, and practices among agencies and state and local governments and the private sector. It shall seek the views of experts from industry, academia, and state and local governments on matters of concern to the Services Board as appropriate. The Services Board shall also make recommendations to the agencies, the CIO Council, OMB, and others as appropriate, and assist in the following:

- (1) creating opportunities for cross-agency cooperation and intergovernmental approaches in using information resources to support common operational areas and to develop and provide shared government-wide infrastructure services;
- (2) developing shared government-wide information infrastructure services to be used for innovative, multi-agency information technology projects;

## CIO COUNCIL STRATEGIC PLAN

(3) creating and utilizing affinity groups for particular business or technology areas; and

(4) developing with the National Institute of Standards and Technology and with established standards bodies, standards and guidelines pertaining to Federal information systems, consistent with the limitations contained in the Computer Security Act of 1987 (40 U.S.C. 759 note), as amended by the Information Technology Act.

(b) Membership. The Services Board shall be composed of individuals from agencies based on their proven expertise or accomplishments in fields necessary to achieve its goals. Major government mission areas such as electronic benefits, electronic commerce, law enforcement, environmental protection, national defense, and health care may be represented on the Services Board to provide a program operations perspective. Initial selection of members will be made OMB in consultation with other agencies as appropriate. The CIO Council may nominate two members. The Services Board shall recommend new members to OMB for consideration. The Chair will be elected by the Services Board.

### **Section 5. Information Technology Resources Board.**

(a) Purpose and Functions. An Information Technology Resources Board ("Resource Board") is established to provide independent assessments to assist in the development, acquisition, and management of selected major information systems and to provide recommendations to agency heads and OMB as appropriated. The Resources Board shall:

(1) review, at the request of an agency and OMB, specific information systems proposed or under development and make recommendations to the agency and OMB regarding the status of systems or next steps;

(2) publicize lessons learned and promising practices based on information systems reviewed by the Board; and

(3) seek the views of experts from industry, academia, and state and local governments on matters of concern to the Resources Board, as appropriate.

(b) Membership. The Resources Board shall be composed of individuals from executive branch agencies based on their knowledge of information technology, program, or acquisition management within Federal agencies. Selection of members shall be made by OMB in consultation with other agencies as appropriate. The Chair will be elected by the Resources Board. The Resources Board may call upon the department or agency whose project is being reviewed, or any other department or agency to provide knowledgeable representation(s) to the Board whose guidance and expertise will assist in focusing on the primary issue(s) presented by a specific system.

### **Section 6. Office of Management and Budget.** The Director of OMB shall:

(1) evaluate agency information resources management practice and, as part of the budget process, analyze, track and evaluate the risks and results of all major capital investments for information systems;

(2) notify an agency if it believes that a major information system requires outside assistance;

(3) provide guidance on the implementation of this order and on the management of information resources to the executive agencies and to the Boards established by this order; and

(4) evaluate the effectiveness of the management structure set out in this order after 3 years and make recommendations for any appropriate changes.

### **Section 7. General Services Administration.** Under the direction of OMB, the Administrator of General Services shall:

(1) continue to manage the FTS2000 program and coordinate the follow-on to that program, on behalf of and with the advice of customer agencies;

## CIO COUNCIL STRATEGIC PLAN

- (2) develop, maintain, and disseminate for the use of the Federal community, as requested by OMB or the agencies, recommended methods and strategies for the development and acquisition of information technology;
- (3) conduct and manage outreach programs in cooperation with agency managers;
- (4) be a focal point for liaison on information resources management, including Federal information technology, with state and local governments, and with non-governmental international organizations subject to prior consultation with the Secretary of State to ensure such liaison would be consistent with and support overall United States foreign policy objectives;
- (5) support the activities of the Secretary of State for liaison, consultation, and negotiation with intergovernmental organizations in information resources management matters;
- (6) assist OMB, as requested, in evaluating agencies' performance-based management tracking systems and agencies' achievement of cost, schedule, and performance goals; and
- (7) provide support and assistance to the interagency groups established in this order.

**Section 8. Department of Commerce.** The Secretary of Commerce shall carry out the standards responsibilities under the Computer Security Act of 1987, as amended by the Information Technology Act, taking into consideration the recommendations of the agencies, the CIO Council, and the Services Board.

### **Section 9. Department of State.**

- (a) The Secretary of State shall be responsible for liaison, consultation, and negotiation with foreign governments and intergovernmental organizations on all matters related to information resources management, including Federal information technology. The Secretary shall further ensure, in consultation with the Secretary of Commerce, that the United States is represented in the development of international standards and recommendations affecting information technology. In the exercise of these responsibilities, the Secretary shall consult, as appropriate, with affected domestic agencies, organizations, and other members of the public.
- (b) The Secretary of State shall advise the Director on the development of United States positions and policies on international information policy and technology issues affecting Federal Government activities and the development or international information technology standards.

### **Section 10. Definitions.**

- (a) "Executive agency" has the meaning given to that term in section 4(1) of the Office of Federal Procurement Policy Act (41 U.S.C. 403 (1)).
- (b) "Information Technology" has the meaning given that term in section 5002 of the Information Technology Act.
- (c) "Information resources" has the meaning given that term in section 3502(6) of title 44, United States Code.
- (d) "Information resources management" has the meaning given that term in section 3502(7) of title 44, United States Code.
- (e) "Information system" has the meaning given that term in section 3502(8) of title 44, United States Code.
- (f) "Affinity group" means any interagency group focused on a business or technology area with common information technology or customer requirements. The functions of an affinity group can include identifying common program goals and requirements; identifying opportunities for sharing information to improve quality and effectiveness; reducing costs and burden on the public; and recommending protocols and other standards, including security standards, to the National Institute of Standards and Technology for government-wide applicability, for action in accordance with the Computer Security Act of 1987, as amended by the Information Technology Act.'
- (g) "National security system" means any telecommunications or information system operated by the United

## CIO COUNCIL STRATEGIC PLAN

States Government, the function, operation, or use of which (1) involves intelligence activities; (2) involves cryptologic activities related to national security; (3) involves command and control of military forces; (4) involves equipment that is an integral part of a weapon or weapons system; or (5) is critical to the direct fulfillment of military or intelligence missions, but excluding any system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

**Section 11. Applicability to National Security Systems.** The heads of executive agencies shall apply the policies and procedures established in this order to national security systems in a manner consistent with the applicability and related limitations regarding such systems set out in the Information Technology Act.

**Section 12. Judicial Review.** Nothing in this Executive order shall affect any otherwise available judicial review of agency action. This Executive order is intended only to improve the internal management of the executive branch and does not create any right or benefit, substantive or procedure, enforceable at law or equity by a party against the United States, its agencies or instrumentalities, its officers or employees, or any other person.

**WILLIAM J. CLINTON**



# CIO COUNCIL STRATEGIC PLAN

## APPENDIX B: CIO COUNCIL CHARTER

### AUTHORITY:

Executive Order 13011, *Federal Information Technology*, establishes a Chief Information Officers Council (the CIO Council) as 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 IRM objectives delineated in the Government Performance and Results Act, the Paperwork Reduction Act of 1995 (PRA), and the Information Technology Management Reform Act of 1996 (ITMRA). The CIO Council is a forum to improve agency practices on such matters as the design, modernization, use, sharing, and performance of agency 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 serves as the principal forum for executive agency CIOs to:

- develop recommendations for overall federal information technology management policy, procedures, and standards;
- share experiences, ideas, and promising practices, including work process redesign and the development of performance measures, to improve the management of information resources;
- identify opportunities, make recommendations for, and sponsor co-operation in using information resources;
- assess and address the hiring, training, classification, and professional development needs of the Federal Government with respect to information resources management;
- make recommendations and provide advice to appropriate executive agencies and organizations, including advice to OMB on the Government-wide strategic plan required by the Paperwork Reduction Act; and
- seek the views of the Chief Financial Officers Council, the Government Information Technology Services Board, the Information Technology Resources Board, Federal Procurement Council, 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 which will help the Government to 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 Presidential Commission on Management Improvement (PCMI) and the Government Information Technology Services Board (GITSB).

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.

## CIO COUNCIL STRATEGIC PLAN

### **MEMBERSHIP:**

Chair, Deputy Director of Management, OMB

Vice-Chair

CIOs and Deputy CIOs from agencies listed in the Executive Order

Administrator, Office of Federal Procurement Policy, OMB

Administrator, Office of Information and Regulatory Affairs, OMB

Controller, Office of Federal Financial Management, OMB

Senior Representative of the Office of Science and Technology Policy

Chair of the Government Information Technology Services Board

Chair of the Information Technology Resources Board

Two Small Agency Council representatives

### **Ex officio:**

General Accounting Office (GAO) Representative

Chief Financial Officers Council Representative

Others designated by vote of the CIO Council

Voting Agencies listed in E.O. 13011 will get one vote per Department or Agency. In accordance with E.O. 13011 the two representatives for small agencies will have one vote each. 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:**

By Executive Order the Chairperson shall be the Deputy Director for Management of the Office of Management and Budget. Elected officers of the Council are:

Vice-Chair

Secretary/Treasurer

Officer at Large (as needed)

The Vice-Chair shall be an agency CIO. The Vice-Chair term is two years.

## **CIO COUNCIL STRATEGIC PLAN**

### **PROCEDURES:**

The Council will develop a concept of operations document which outlines specific operational procedures.

The Council Chair will establish the procedures for promulgating Council decisions and resolutions.

The Council will determine a meeting schedule adequate for ongoing implementation of the PRA and the ITMRA.

The Secretary/Treasurer will maintain an official archive of all minutes and Council documents.

### **COMMITTEES:**

The CIO Council has the authority to establish standing committees and working groups as necessary to consider items of concern of the Council.

### **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:**

OMB and the Vice-Chair will provide for staff support to the Council. GSA will provide support and assistance to the Council. This will be augmented by support from other Officers and members as necessary.

Adopted by Majority Vote on January 15, 1997 in Washington, D.C.

## **CIO COUNCIL STRATEGIC PLAN**

### **APPENDIX C:**

#### **CIO COUNCIL STRUCTURE**

**(WITH PICTURES)**

- 1. EXECUTIVE COMMITTEE**
- 2. E-GOVERNMENT COMMITTEE**
- 3. ENTERPRISE INTEROPERABILITY AND EMERGING IT COMMITTEE**
- 4. SECURITY, PRIVACY AND CRITICAL INFRASTRUCTURE**
- 5. OUTREACH COMMITTEE**
- 6. CAPITAL PLANNING AND IT MANAGEMENT COMMITTEE**

## CIO COUNCIL STRATEGIC PLAN

### APPENDIX D:

#### FY 2001 OBJECTIVES AND INITIATIVES WITH LEAD AND CONTRIBUTOR COMMITTEE RESPONSIBILITIES

GOAL/OBJECTIVE/INITIATIVE	LEAD COMMITTEE	CONTRIBUTOR COMMITTEE
<b>Goal 1: All Citizens Connected To The Products, Services, And Information Of Their Government</b>		
<b>Objective 1.1:</b> <b><i>Develop a single point-of-entry portal model to access Government services.</i></b>	e-Government	
1. Support implementation of FirstGov.gov.	e-Government	
2. Promote an expanded number of entry points to FirstGov.gov through "certified partnerships".	e-Government	
3. Develop a strategy for implementing functional portals at five Government agencies.	e-Government	
4. Support development of functional portals (e.g., Students, Seniors, and Fed-Commons).	e-Government	
5. Propose alternative models to provide universal citizen access to Government information and services.	e-Government	
<b>Objective 1.2:</b> <b><i>Increase the customer-value of Government sites.</i></b>	e-Government	
1. Promote work by agencies to modify their Web sites to support the functional portals.	e-Government	
2. Support the e-Gov awards program recognizing innovative Federal sites.	e-Government	
3. Support the dissemination of industry and Government "best practices" for site content.	e-Government	
4. Develop Government-wide guidelines and best practices and recommend standards for electronic information and services on Federal sites.	e-Government	
5. Establish five moderated, open discussion groups for citizen interaction with agencies.	e-Government	
6. Assist Federal agencies in offering online rule making such that 50% are online.	e-Government	
7. Promote the transition of Federal data to geo-spatial form.	e-Government	
8. Support OMB in the smooth implementation of GPEA.	e-Government	
<b>Objective 1.3:</b> <b><i>Make transactions across all levels of Government seamless.</i></b>	e-Government	Outreach
1. Develop and issue a strategy for integrating electronic information and services with State Governments.	e-Government	Outreach
2. Develop and issue a strategy for integrating electronic information and services with local Governments.	e-Government	Outreach
3. Plan, organize and hold an Inter-Governmental e-Congress.	e-Government	Outreach
4. Develop and issue a strategy for integrating electronic information and services in specific functional areas with five other countries.	e-Government	Outreach
5. Plan, organize, and hold an international e-Gov Congress.	e-Government	Outreach
<b>Objective 1.4:</b> <b><i>Citizen transactions and interactions with Government agencies are easily and properly authenticated.</i></b>	e-Government	Security, Privacy, and Critical Infrastructure
1. Promote the use of digital signatures by citizens and businesses.	e-Government	Security, Privacy, and Critical Infrastructure
2. Cross-certify at least five vendor PKI certificates for Government use	e-Government	Security, Privacy, and Critical Infrastructure; Enterprise Interoperability and Emerging IT
3. Develop five cross-agency digital signature approaches.	e-Government	Security, Privacy, and Critical Infrastructure
<b>Objective 1.5:</b> <b><i>Establish communities of practice and affinity groups</i></b>	e-Government	

## CIO COUNCIL STRATEGIC PLAN

GOAL/OBJECTIVE/INITIATIVE	LEAD COMMITTEE	CONTRIBUTOR COMMITTEE
<i>through the use of collaborative tools.</i>		
1. Build collaborative software infrastructure to support communities of interest.	e-Government	
2. Develop at least three communities centered on CIO concerns.	e-Government	
3. Evaluate the effectiveness of communities of interest for interagency collaboration.	e-Government	
<b>Goal 2: Interoperable And Innovative Government-Wide IT Initiatives</b>		
<b>Objective 2.1:</b> <b>Develop an interoperable Government-wide Public Key Infrastructure (PKI) based on a sound policy/guidance framework.</b>	Enterprise Interoperability and Emerging IT	Security, Privacy, and Critical Infrastructure
1. Implement the Federal Bridge Certification Authority, using at least four different Certification Authority products.	Enterprise Interoperability and Emerging IT	Security, Privacy, and Critical Infrastructure
2. Interoperate with at least one foreign Government PKI and at least one State or local Government PKI.	Enterprise Interoperability and Emerging IT	Security, Privacy, and Critical Infrastructure; e-Government
3. Evolve the Federal White Pages Directory ("directory.gov") to support public certificates for the Government-wide PKI infrastructure.	Enterprise Interoperability and Emerging IT	Security, Privacy, and Critical Infrastructure
4. Recommend guidelines for the use of PKI in securing Government services.	Enterprise Interoperability and Emerging IT	Security, Privacy, and Critical Infrastructure; e-Government
<b>Objective 2.2:</b> <b>Establish the use of open, standards-based architectures.</b>	Enterprise Interoperability and Emerging IT	
1. Create models for Federal architecture segments.	Enterprise Interoperability and Emerging IT	
2. Promote common processes in specific functional areas across Government agencies.	Enterprise Interoperability and Emerging IT	
3. Develop an online information resource (at xml.gov) defining and documenting an evolving strategy and a set of tasks for the effective and well-coordinated usage of eXtensible Markup Language (XML) to support governmental functions.	Enterprise Interoperability and Emerging IT	
4. Develop and promote a process for ensuring that architectural concepts incorporate emerging technologies.	Enterprise Interoperability and Emerging IT	
5. Develop and promote a process that links IT Capital Planning and IT Architecture.	Enterprise Interoperability and Emerging IT	
<b>Objective 2.3</b> <b>Promote the adoption of accessible technology and develop a formal partnership between the Government and industry to work toward the institution of an IT accessibility test standard.</b>	Enterprise Interoperability and Emerging IT	
1. Develop a process to periodically review how innovative technologies contribute to achieving accessible IT architectures.	Enterprise Interoperability and Emerging IT	
2. Design and implement a process to identify and prioritize near-term action and long-range research needs to address remaining Government-wide IT accessibility challenges.	Enterprise Interoperability and Emerging IT	
<b>Objective 2.4:</b> <b>Foster collaboration and sharing of best practices related to Federal IT applications</b>	Enterprise Interoperability and Emerging IT	
1. Establish affinity groups for common business processes.	Enterprise Interoperability and Emerging IT	
2. Define three to five opportunities for common systems across two or more agencies.	Enterprise Interoperability and Emerging IT	
<b>Objective 2.5:</b> <b>Develop models of Knowledge Management Communities of Practice.</b>	Enterprise Interoperability and Emerging IT	
1. Establish virtual communities of practice through the knowledge management	Enterprise Interoperability	

## CIO COUNCIL STRATEGIC PLAN

GOAL/OBJECTIVE/INITIATIVE	LEAD COMMITTEE	CONTRIBUTOR COMMITTEE
portal site ("www.km.gov").	and Emerging IT	
2. Identify, collect, and disseminate best/first practices in knowledge management across the Federal Government.	Enterprise Interoperability and Emerging IT	
3. Identify Chief Knowledge Officer competencies and establish Chief Knowledge Officer curriculum with academia and industry leaders in knowledge management.	Enterprise Interoperability and Emerging IT	
<b>Goal 3: A Secure And Reliable Information Infrastructure That The Customer Can Access And Trust</b>		
<b>Objective 3.1:</b> <b><i>Expand and operate a Security Best Practices repository</i></b>	Security, Privacy, and Critical Infrastructure	
1. Provide self-guided online "how to" security tutorial.	Security, Privacy, and Critical Infrastructure	
2. Provide users 200+ BSPs with a monthly turnover/refresh rate of 10%.	Security, Privacy, and Critical Infrastructure	
<b>Objective 3.2:</b> <b><i>Develop an initial Security Assessment Capability for Federal agencies.</i></b>	Security, Privacy, and Critical Infrastructure	
1. Publish Version 1.0 of the Information Technology Security Assessment Framework.	Security, Privacy, and Critical Infrastructure	
2. Publish measures in support of Version 1.0 of the Information Technology Assessment Framework.	Security, Privacy, and Critical Infrastructure	
<b>Objective 3.3:</b> <b><i>Implement a Government-wide process to collect, analyze, and rapidly disseminate security incident and early warning information.</i></b>	Security, Privacy, and Critical Infrastructure	
1. Identify and document roles and responsibilities to implement a Federal Government-wide incident handling and early warning system.	Security, Privacy, and Critical Infrastructure	
2. Demonstrate operational effectiveness of the early warning capability using an exercise.	Security, Privacy, and Critical Infrastructure	
<b>Objective 3.4:</b> <b><i>Develop a model security risk management program for use by Federal agencies.</i></b>	Security, Privacy, and Critical Infrastructure	
1. Work with key stakeholders to develop and publish a methodology to manage risk.	Security, Privacy, and Critical Infrastructure	
<b>Objective 3.5:</b> <b><i>Work to establish Critical Infrastructure guidelines and recommendations.</i></b>	Security, Privacy, and Critical Infrastructure	
1. Assist the National Coordinator, OMB and the CIAO in tracking progress in the implementation of PDD-63.	Security, Privacy, and Critical Infrastructure	
2. Work with the CIAO, GSA, OMB, and other governmental entities to explore and develop recommendations on funding mechanisms for agencies to use for implementing PDD- 63.	Security, Privacy, and Critical Infrastructure	
3. In conjunction with OMB and CIAO, recommend guidelines for Tier Two agencies to use as a model in order to meet the requirements of PDD-63.	Security, Privacy, and Critical Infrastructure	
4. Publicize information assurance/information security competencies and develop a process for public and private training providers to map to the competencies.	Security, Privacy, and Critical Infrastructure	
5. Create a CIP primer, including a brief video, to emphasize the business case and priority requirements of CIP for Federal executives.	Security, Privacy, and Critical Infrastructure	
6. Sponsor a broad Federal CIP awareness campaign about cyber threats and employee responsibilities.	Security, Privacy, and Critical Infrastructure	
7. Explore ways to work with NASIRE in order to promote CIP awareness and processes with our systems/infrastructures partners.	Security, Privacy, and Critical Infrastructure	
<b>Objective 3.6:</b> <b><i>Protect personal privacy in Government electronic information systems.</i></b>	Security, Privacy, and Critical Infrastructure	

## CIO COUNCIL STRATEGIC PLAN

GOAL/OBJECTIVE/INITIATIVE	LEAD COMMITTEE	CONTRIBUTOR COMMITTEE
1. Promote the effective implementation of OMB guidance on Website privacy policies and assist agencies in reporting on their efforts to comply with such policies and on other privacy practices in the budget process.	Security, Privacy, and Critical Infrastructure	
2. Explore methods of ensuring privacy protection in Federal authentication systems.	Security, Privacy, and Critical Infrastructure	
3. Promote the development and appropriate use of privacy impact assessments in the development of new Government computer systems.	Security, Privacy, and Critical Infrastructure	
4. Develop and provide sample guidance to agencies on complying with the standards in COPPA.	Security, Privacy, and Critical Infrastructure	
<b>Objective 3.7:</b> <b><i>Publish example security and privacy practices for common electronic services.</i></b>	Security, Privacy, and Critical Infrastructure	e-Government; Enterprise Interoperability and Emerging IT
1. Identify example security and privacy solutions for Web-based information sites, financial transactions, and procurement transactions.	Security, Privacy, and Critical Infrastructure	e-Government; Enterprise Interoperability and Emerging IT
2. Update initial example solutions and expand coverage of electronic services.	Security, Privacy, and Critical Infrastructure	e-Government; Enterprise Interoperability and Emerging IT
<b>Objective 3.8:</b> <b><i>Recommend policies and guidelines to improve protection of citizen and corporate information within Federal systems.</i></b>	Security, Privacy, and Critical Infrastructure	
1. Work with OMB and NIST to develop three draft or sample policies for use by Federal agencies in the areas of privacy and security.	Security, Privacy, and Critical Infrastructure	
<b>Goal 4: IT Skills And Resources To Meet Mission Objectives</b>		
<b>Objective 4.1:</b> <b><i>Improve the Federal Government's ability to attract and retain a top-notch IT workforce</i></b>	IT Workforce	
1. Establish, in partnership with the private sector, an outreach program to local high schools to develop interest in pursuing IT careers in the Federal Government.	IT Workforce	
2. Support full implementation of recommendations from the "Federal IT Workforce Challenge" report.	IT Workforce	
3. Support the implementation of the recommendations from the NAPA study of compensation and retention issues.	IT Workforce	
<b>Objective 4.2:</b> <b><i>Expand effective IT education and training opportunities for the existing Federal workforce.</i></b>	IT Workforce	
1. Review and revise CIO Core Competencies and associated learning objectives on a biennial basis.	IT Workforce	
2. Develop "road maps" for meeting the core competency training needs of staff.	IT Workforce	
3. Establish the CIO Executive Exchange program in collaboration with OPM.	IT Workforce	
4. Establish the CIO Council Mentoring Program.	IT Workforce	
5. Refine and enhance the STAR Program and deliver two pilot seminars.	IT Workforce	
<b>Goal 5: Collaborations Between The Public And Private Sectors Achieve Better Government</b>		
<b>Objective 5.1:</b> <b><i>Promote inter-governmental collaboration with representatives from all levels of Government.</i></b>	Outreach	
1. Develop and conduct a number of Common Ground Forums, comprised of Federal, State, and local agencies.	Outreach	
2. Develop and conduct Congressional Common Ground Forums.	Outreach	
3. Identify inter-governmental initiatives to be completed jointly with NASIRE.	Outreach	
<b>Objective 5.2:</b> <b><i>Establish stronger and more productive collaborative relationships between the leadership in the Federal sector and that in other sectors.</i></b>	Outreach	
1. Develop and conduct Common Ground Forums, comprised of government,	Outreach	



## CIO COUNCIL STRATEGIC PLAN

GOAL/OBJECTIVE/INITIATIVE	LEAD COMMITTEE	CONTRIBUTOR COMMITTEE
academic and industry participants, at various conferences (such as Virtual Government Conferences, IAC/ELC, FOSE, etc.)		
2. Facilitate an ongoing exchange of ideas and information between industry leaders and the Capitol Hill community.	Outreach	
<b>Objective 5.3:</b> <b>Significantly raise the level of awareness and acceptance among key stakeholders and decision-makers of the CIO Council's efforts and accomplishments.</b>	Outreach	
1. Deliver the Council's transition message in a special <i>Government Computer News</i> (GCS) supplement.	Outreach	
2. Webcast a full CIO Council meeting.	Outreach	
3. Create a Council presence at major conferences (e.g., FOSE, Virtual Government, IRMCO, and TechNet).	Outreach	
4. Coordinate CIO Council coverage with major trade and national publications (e.g., <i>Federal Times</i> , <i>Government Computer News</i> , <i>Federal Computer Week</i> , <i>Government Executive</i> , <i>Wall Street Journal</i> , and the <i>Washington Post</i> ).	Outreach	
<b>Goal 6: Investment Management Policies, Practices, and Tools That Enable Improved Delivery of Government Programs and Services</b>		
<b>Objective 6.1:</b> <b>Foster better integration of planning, budgeting, acquisition, and program management communities and processes.</b>	Capital Planning and IT Management	
1. Develop a framework and agreements for working relationships and collaboration with the CFO Council and the PEC through Information Sharing Forums.	Capital Planning and IT Management	
2. Bring in strategic planning representation to the Information Sharing Forums.	Capital Planning and IT Management	
<b>Objective 6.2:</b> <b>Achieve consistent application of investment management measures, methodologies, and policies.</b>	Capital Planning and IT Management	
1. Develop criteria for agencies to evaluate the performance measures for their major IT investments.	Capital Planning and IT Management	
2. Conduct pilot demonstrations at a volunteer agency to evaluate methodologies that measure the contribution of IT to mission results.	Capital Planning and IT Management	
3. Ask agencies to conduct a self-evaluation using the criteria on their FY2001-FY2002 investment portfolio.	Capital Planning and IT Management	
<b>Objective 6.3:</b> <b>Seamlessly integrate Federal statutory requirements into the investment management process.</b>	Capital Planning and IT Management	
1. Develop a framework and agreements for working relationships and collaboration with the other CIO Council committees.	Capital Planning and IT Management	
2. Develop guidelines and framework for linking requirements.	Capital Planning and IT Management	
<b>Objective 6.4:</b> <b>Improve the quality, accuracy, consistency, and currency of data used to support investment decision-making and meaningful reporting</b>	Capital Planning and IT Management	
1. Develop cost models, cost report capturing processes, and formats for reporting; integrate with I-TIPS.	Capital Planning and IT Management	
<b>Objective 6.5:</b> <b>Improve information technology acquisition strategies.</b>	Capital Planning and IT Management	
1. Assess the viability of the Seat Management approach to acquiring information technology.	Capital Planning and IT Management	
2. Evaluate contractual ways of assuring that highly qualified IT professionals are available to Federal agencies and share the findings with the agencies.	Capital Planning and IT Management	

# CIO COUNCIL STRATEGIC PLAN

## APPENDIX E: GENERAL ABBREVIATIONS

BSP - Best Security Practice  
CIAO - Critical Infrastructure Assurance Office  
CIO - Chief Information Officer  
CIP - Critical Infrastructure Protection  
COPPA - Childrens' OnLine Privacy Protection Act  
EEP - Executive Exchange Program  
EOP - Executive Office of the President  
FASA - Federal Acquisition Streamlining Act  
FBCA - Federal Bridge Certification Authority  
FEMA - Federal Emergency Management Administration  
FOSE - Federal Office Systems Exposition  
GAO - General Accounting Office  
GPEA - Government Paperwork Elimination Act  
GPRA - Government Performance and Results Act  
GSA - General Services Administration  
IAC - Industry Advisory Council  
IRMCO - Interagency Resources Management Conference  
IRS - Internal Revenue Service  
ISF - Information Sharing Forum  
IT - Information Technology  
ITAA - Information Technology Association of America  
I-TIPS - Information Technology Investment Portfolio System  
ITSAF - Information Technology Security Assessment Framework  
KM - Knowledge Management  
NACO - National Association of Counties  
NAPA - National Association of Public Administration  
NASIRE - National Association of State Information Resource Executives  
NIST - National Institute of Standards and Technology  
NLC - National League of Cities  
OMB - Office of Management and Budget  
OPM - Office of Personnel Management  
PDD - Presidential Decision Directive  
PEC - Procurement Executive Council  
PKI - Public Key Infrastructure  
SSA - Social Security Administration  
STAR - Strategic and Tactical Advocates for Results Program  
TCO - Total Cost of Ownership  
USPS - United States Postal Service  
VA - Department of Veterans Affairs  
XML - eXtensible Markup Language