Chief Information Officers Council

Strategic Plan

Fiscal Year 2000

Table of Contents

CIO Council Strategic Agenda

Appendices

> ***" I see the Council more and more involved in the key information technology issues affecting government, taking a leadership role [in those issues] and recommending guidance."***
>
> *Federal Times - Jim Flyzik, CIO, Treasury Department*

Foreword

This Strategic Plan for Fiscal Year 2000 represents an important development in the history of both the Chief Information Officers (CIO) Council and information technology (IT) in government. As we enter the new century, the CIO Council has shifted its focus beyond Y2K to help shape the strategic Federal IT agenda.

This Plan builds upon the strong foundation created in our FY 1998 and 1999 Strategic Plans. Jointly published by the Council and the Office of Management and Budget (OMB), the Plan reflects sophistication in both process and content. As we refine our strategic management and investment processes, we find new areas that demand our attention. We also see a continuing need for a unified voice on significant issues.

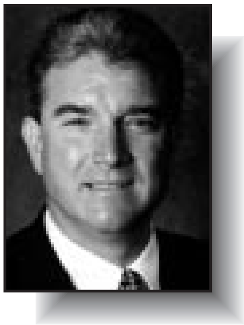
The FY 2000 Strategic Plan shows a CIO Council maturing in its leadership role. The Plan articulates the goals, objectives, and initiatives the Council envisions in addressing IT issues of strategic importance to the Federal community.

Ideas from stakeholders in both government and the private sector were instrumental in setting the tone and direction for this Plan. Our list of partners continues to grow and includes the Information Technology Resources Board, the Government Information Technology Services Board, the Chief Financial Officers Council, the Procurement Executive Council, and the Human Resources Development Council. These relationships greatly expand our collective knowledge base and capacity to address key issues. We continue to seek feedback from our partners on the proper direction and implementation of our strategic vision.

A great deal of time, effort, and critical thinking have gone into this Plan. We are particularly grateful to our Committee Chairs and members for their dedication and their commitment to continuous improvement in the Federal Government. We also extend sincere appreciation to our OMB, Treasury, and General Services Administration staffs for their invaluable support of the Council. These Federal employees represent the very best in government. They are serving the American people well.

John T. Spotila

John T. Spotila
Acting Chair, CIO Council



Jim Flyzik

Jim Flyzik
Vice-Chair, CIO Council

Introduction

The CIO Council was established by Executive Order 13011, Federal Information Technology, in 1996 (Appendix I). The Council is the principal interagency forum for improving practices in the design, modernization, use, sharing, and performance of agency information resources. CIOs and Deputy CIOs of the 28 largest federal agencies, and two CIOs representing the smaller federal agencies, comprise the Council's membership. The purpose of the Council is to lead and direct the strategic management of federal IT resources and to serve as a focal point for coordinating challenges that cross agency boundaries. The Council also partners with other federal executive councils to address management challenges that require multidisciplinary solutions.

In addition, the Council Charter defines the following leadership responsibilities:

- Recommend overall federal IT management policy
- Propose IT standards and best practices to address shared management challenges
- Identify, promote, and sponsor promising IT solutions and initiatives
- Address the hiring, training, and development issues of the federal IT workforce
- Advise executive agencies and OMB on the governmentwide strategic plan required by the Paperwork Reduction Act of 1995
- Coordinate, collaborate, and share resources within the Council, and in cooperation with other federal executive councils, develop and implement governmentwide business strategies to improve program services and operations

CIO Council Strategic Agenda

The CIO Council envisions a government that uses information and technology as strategic assets in meeting the missions of the federal agencies. Information technology is pivotal to successful delivery of services and the CIO must be a full member of any agency's senior management decision-making. The CIO Council provides a vehicle and unified voice for cross-agency leverage, information sharing, and interoperability. This Plan represents the continued refinement of the strategic priorities that capture the Council's attention. In the spirit of the Government Performance and Results Act, and OMB Circular No. A-11, the Council reaffirmed the Mission of the Council, as well as the overall Vision for this planning horizon, from FY2000-2005. The Council's goals and the Committees' focus are guided by the compass of this Mission and Vision.

CIO Council Vision

The Chief Information Officers Council is the principal interagency forum to improve the design, modernization, use, sharing, and performance of agency information resources. The Council's role includes: developing recommendations for IT management policy, procedures, and standards; identifying opportunities to share information resources; and assessing and addressing the needs of the Federal Government for an information technology workforce.

As the CIO Council looks to the future, federal agencies have already made great strides in their implementation of IT. Day after day, more and more agencies rely on IT to accomplish their mission. Progress to this point has been easy compared to the challenges ahead. No longer will IT be used in pockets of isolation to accomplish separate and distinct tasks. Agencies can no longer succeed as standalone, independent entities. Government agencies must integrate IT into every facet of their operations as they become truly digital enterprises. This will reduce the costs of government and deliver better quality and integrated products and services to the public.

Public and private sector organizations alike are faced with the fast-paced decisions required in the digital economy. There is a great need for concerted leadership in the government IT community. The CIO Council helps to fulfill that need by providing a united voice to help the highly diversified federal government enterprise find its place in the digital economy.

In championing issues that extend beyond any one agency, that affect the entire federal community, the Council is singularly positioned to synthesize the critical issues of highest impact to the overall federal enterprise. In order to take best advantage of its placement, the Council seeks recognition for the leadership focus it brings. In establishing this recognition, the Council plays a powerful role in identifying the strategic IT direction and priorities for the federal enterprise. The CIO Council's goals unify and direct the focus and direction presented in this Plan.

CIO Council Mission

The fundamental purpose of the CIO Council is to be a resource that 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 capital programming processes, business process reengineering, continuous process improvement, and measurable increases in employee productivity in the performance of work related to the achievement of agency objectives.

As part of the ongoing strategic management process, the full Council examined crosscutting issues affecting the federal community, and evaluated the impact of Council participation in five topic areas:

- Governance and Funding
- Federal IT Workforce
- Future of Information Technology
- Knowledge Management
- Critical Infrastructure

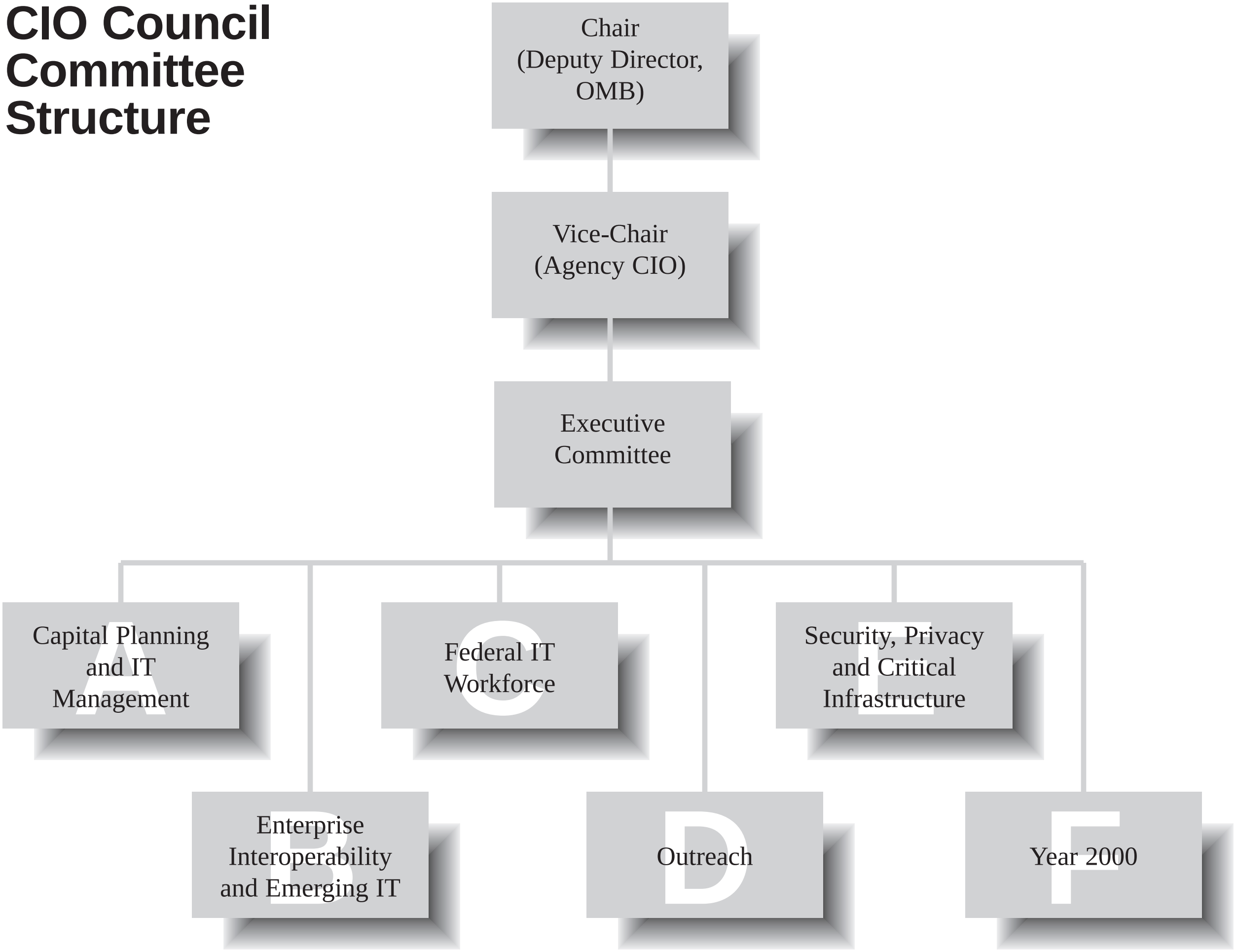
Evaluation of the relevance of Council action in these areas, combined with previous Committee experience in other strategic areas—interoperability, security, Year 2000 conversion, capital planning and IT investment—refined the Council's direction for the future. Emerging from this evaluation arose four Council-wide goals.

CIO Council Goals

- ***Establish the strategic IT direction for the Federal Government and identify governmentwide IT priorities.***
- ***Establish the Council as a recognized leader in the government IT community.***
- ***Be recognized as a key partner with the global IT community.***
- ***Improve management and results of IT in government to deliver better service to the citizen in accordance with Clinger-Cohen intent.***

These Council-wide goals govern the activities of the Council's Committees. As a result of the reevaluation of highest impact Council focus, several new areas emerged. In order to effectively operationalize objectives in these areas, the Council revamped its Committee structure to better align with current priorities. Some Committees expanded their purview, while others are novel. The Council is composed of six operational Committees, some having Subcommittees. The Executive Committee, made up of the Committee Chairs, provides an overarching Governance Committee to support Council operations and the management of budget and crosscutting initiatives.

CIO Council Committee Structure


Chair
(Deputy Director, OMB)
Vice-Chair
(Agency CIO)
Executive Committee
A
Capital Planning and IT Management
B
Enterprise Interoperability and Emerging IT
C
Federal IT Workforce
D
Outreach
E
Security, Privacy and Critical Infrastructure
F
Year 2000

The Role of Governance

The governance body is the Executive Committee, composed of the Committee Chairs, which will play a critical role in addressing key management challenges in the execution of the goals, objectives, and initiatives contained in this plan. Effective governance is the key to the Council's reputation and role as a trusted expert and partner on strategic issues and decisions relating to information resources. The Executive Committee will provide management for the Council in certain areas such as:

- Strategic priorities and budget impacts
- Governance requirements that address unifying management challenges
- Identification and management of cross-cutting activities
- Measurement
- Coordination of proposed policy development and promulgation
- Management support

To best execute its governmentwide charter, the CIO Council must actively work with Congress, the General Accounting Office (GAO), OMB, and other stakeholders. It is crucial that the Council maintain strong working relationships in order to contribute to critical crosscutting IT decisions, to lead the development of a unifying Strategic Agenda, and to help identify new global opportunities.

The governance objective to **"define the Council's leadership roles in creating a unified voice for the Government IT community"** will be achieved through the following initiatives:

1.1 Incorporate CIO Council Strategic Plan into the President's IT agenda

- Work with the White House/Office of Science and Technology Policy (OSTP) to recognize the CIO Council Strategic Agenda
- Establish the CIO Council as the "Federal CIO" - Become a "unified voice" for the IT community and establish the CIO role in governmentwide activities
- Create legislative language for funding (i.e., working capital fund)
- Identify issues for CIO Council to take positions on and leverage through other groups such as the Bureaus, National Economic Council, President's Council on Integrity and Efficiency (PCIE), National Archives Records Administration (NARA), President's Management Council (PMC), Chief Financial Officers (CFO) Council, and National Association of State Information Resources Executives (NASIRE)

1.2 Establish a mentoring program

1.3 Establish a Committee to work with CFOs on the Government Performance and Results Act (GPRA) (i.e., joint project to link CFO/CIO outcomes)

1.4 Produce guidelines for and provide examples of core IT performance measures that agencies can use to comply with GPRA and the Clinger-Cohen Act of 1996 (also known as the Information Technology Management Reform Act, or ITMRA)

1.5 Identify and promulgate CIO activities that have contributed to the successful implementation of the Clinger-Cohen Act governmentwide (e.g., FedCirc, CIO University)

1.6 Create a streamlined framework for developing and publishing guidance (incorporate processes used for personal use guidelines and software piracy)

1.7 Support the Centers of Excellence for IT (CEIT) as a way to promote best IT practices. The CEIT serves as a clearinghouse for best practices using web-enabled technologies to perform a wide range of business processes.

1.8 Coordinate with appropriate entities to develop a model business plan for use in organizations and promote the use of successful models

1.9 Review Clinger-Cohen Act and recommend changes that lead to improvement

1.10 Provide an avenue to appropriately elevate and address the challenges of bureau and small agency CIOs while complementing efforts of the CIO Council

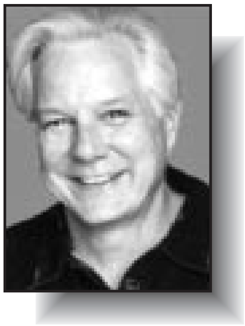
1.11 Create a governmentwide "inventory" of major systems development efforts, to identify opportunities for partnering and leveraging of resources

In the following chapters, the strategic focus for each Committee is outlined, governed by the Council's overall Strategic Agenda. Committee objectives, along with a select high priority initiative, are depicted on the next page.

Committee Strategic Agenda

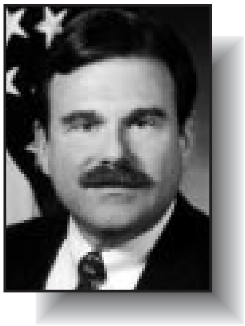
Committee Objectives	*High Priority Initiative*
A. Capital Planning and IT Management 1. Promote the effective implementation of IT management and its integration and alignment with agencies' missions and processes 2. Improve the linkage between IT Capital Planning and the budget and accounting processes 3. Promote and facilitate the development and use of effective tools for capital planning and investment management	Conduct an assessment of the lessons learned and best practices in the implementation of the Clinger-Cohen Act.
B. Enterprise Interoperability and Emerging IT 1. Facilitate the IT infrastructure of government 2. Support collaboration and resource sharing 3. Develop governmentwide architecture and technology strategy 4. Develop unified government voice on standards and technology requirements	Promote infrastructure to provide common physical/cyber access solutions.
C. Federal IT Workforce 1. Validate and substantiate the extent of the federal IT workforce challenge 2. Develop and implement strategies for recruitment, retention, and development of IT professionals and to upgrade skills of current workforce	Support full implementation of all 13 recommendations from the Federal IT Workforce Challenge Report.
D. Outreach 1. Create high-leverage partnerships with international, federal, state, and private sector IT leadership groups 2. Promote the Council's credibility in IT leadership 3. Establish CIO Council Intranet and Extranet for states and others	Expand and explore opportunities for increased interaction and outreach with the world-wide IT community to disseminate and share information, knowledge, policies, best practices, etc.
E. Security, Privacy, and Critical Infrastructure 1. Lead the establishment of integrated, governmentwide IT guidelines, best practices, tools, training, and proposed policies in areas of privacy, critical infrastructure, and security 2. Support service delivery capabilities of Federal agencies by determining security and privacy approaches that advance appropriate information access, exchange, and protection, and support Electronic Commerce 3. Promote awareness of security, privacy, and critical infrastructure issues 4. Establish a leadership role within the CIO Community in the implementation of PDD-63	Assist the National Coordinator, OMB, and the CIAO in tracking the progress of the implementation of PDD-63.
F. Year 2000 1. Reemphasize IT management practices to assure that mission-critical systems work on, before, and after January 1, 2000 2. Identify joint efforts to leverage resources for solving the Year 2000 problem	Maintain the Federal Government gateway for Year 2000 information directory website.

A. Capital Planning and Information Technology Management



Bill Piatt, GSA

Co-Chair



Daryl White, Interior

Co-Chair

Most of the IT decision-making challenges facing the Federal Government can be thought of as capital planning or IT management issues. This is because federal IT managers are constantly faced with buying the right technology for their agencies which entails both making the best capital investment decisions, as well as managing their IT budgets responsibly. Moreover, recent reform legislation has highlighted the importance of agencies managing their IT projects as business investments with an emphasis on desired results. In an environment of cutting costs and downsizing, IT projects must clearly communicate their business value and "payoff" to justify the investment. Reform legislation such as the Paperwork Reduction Act of 1995 and the Acquisition Streamlining Act, provides the opportunity to significantly improve the way the Federal Government acquires and manages information technology. In order to continue a critical governmentwide focus and leverage on these key areas, the CIO Council expanded the purview of this Committee from solely capital planning issues to Capital Planning and IT Management.

The Capital Planning and IT Management Committee seeks to promote systematic approaches to managing selection, control, implementation and evaluation processes for IT investments across government. A principal responsibility of the Committee is to coordinate development and implementation activities across federal government agencies. This coordination provides a means to identify best tools and practices, as well as to identify potential adverse impacts. One such tool is the Information Technology Investment Portfolio System (I-TIPS). This Committee has been instrumental in the development of I-TIPS, as it supports our goals and objectives. I-TIPS is now controlled and funded outside of the Committee as a self-sustaining activity, funded by participating federal agencies now using the system. Because of its importance to Capital Planning, this Committee and the Council will continue to be kept informed about I-TIPS development and use.

This Committee's work supports the CIO Council's goals to "establish the Council as a recognized leader in the government IT community" and to "improve management and results of IT in government to deliver better service to the citizen in accordance with Clinger-Cohen intent." The objectives of the Capital Planning and Information Technology Management Committee are to:

- Promote the effective implementation of Information Technology management and its integration and alignment with agencies' missions and processes.
- Improve the linkage between Information Technology capital planning and the budget and accounting processes.
- Promote and facilitate the development and use of effective tools for capital planning and investment management.

The following sections describe the objectives, strategies and initiatives that the CIO Council will pursue in order to contribute to government agencies' capability to effectively manage IT as "capital investments."

Objective #1

Promote the effective implementation of Information Technology management and its integration and alignment with agencies' missions and processes.

Strategies and Initiatives to achieve this objective

Since the enactment of Clinger-Cohen, organizations have had the opportunity to implement various IT investment and management processes, and begin assessing results. As government approaches become increasingly sophisticated, both public and private sector models can be better evaluated. The Capital Planning and IT Management Committee will conduct a review to learn how leading organizations, public and private, consistently apply capital planning and IT management practices to improve performance. In addition, this review will present lessons learned and best practices for evolving capital planning programs in the future. Once complete, the review will be used to gauge the CIO Council's Capital Planning and IT Management Committee's success in promoting and facilitating the evolution of capital planning and IT management programs throughout the federal IT community.

The following initiatives define the strategy to achieve this objective:

1.1 Conduct an assessment of the lessons learned and best practices in the implementation of the Clinger-Cohen Act.

1.2 Share the results of the assessment with the federal IT, CFO and budget communities.

Objective #2

Improve the linkage between Information Technology capital planning and the budget and accounting processes.

Strategies and Initiatives to achieve this objective

The Capital Planning and IT Management Committee will develop an ongoing relationship with the CFO Council and the Budget Officers Advisory Council (BOAC) to develop and implement new initiatives to improve the monitoring and tracking of IT investments. This effort will also create a foundation to institutionalize the linkage between the budget and IT capital planning processes contributing to stronger consideration of capital planning, and greater involvement by the CIO in the process of developing budget submissions under OMB Circular A-11 .

The following initiative defines the strategy to achieve this objective:

2.1 Work with the CFO Council and BOAC to develop accounting structures that permit identification and tracking of IT expenditures.

Objective #3

Promote and facilitate the development and use of effective tools for capital planning and investment management.

Strategies and Initiatives to achieve this objective

Tools for federal agencies that support effective capital planning and IT management are important in managing costs and improving the results of associated processes. The Committee will provide a governmentwide focal point to identify and promote useful tools and techniques utilized or developed across government. The information will be available for use by all government organizations. This cross-organization collaboration will foster partnerships among agencies. This strategy will also support the Clinger-Cohen requirements for full and accurate accountability for IT investments.

The following initiatives define the strategy to achieve this objective:

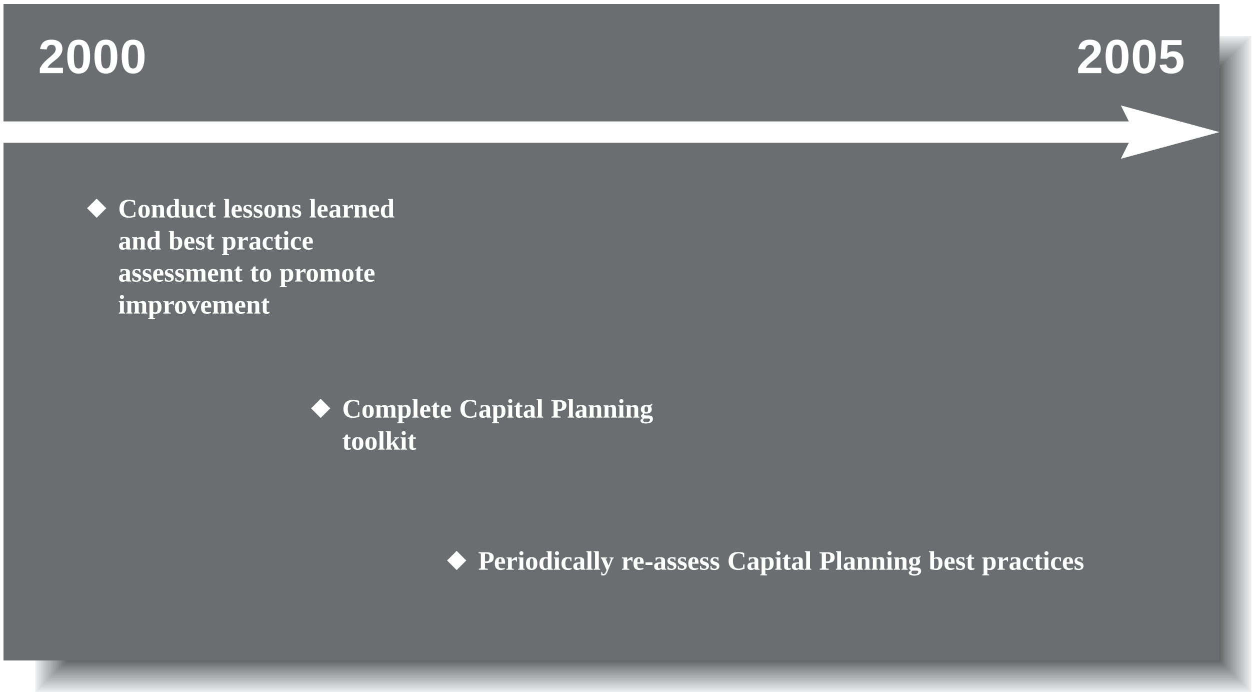
3.1 Develop a capital planning toolkit for use by all agencies.

3.2 Achieve integration of government capital planning tools to gain a governmentwide perspective on IT investments.

Success Indicators

This Committee will oversee activities to establish a mechanism that will show improvement in IT capital planning and investment management throughout the Federal Government. In conjunction with performing the assessment and review, an initial set of performance goals will be established. Timely and satisfactory completion of projected mile-stones will provide interim measures of progress.

Selected high-level milestones, are illustrated in the following chart:

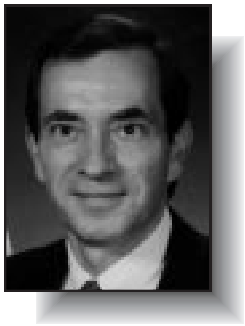


- ◆ Conduct lessons learned and best practice assessment to promote improvement
- ◆ Complete Capital Planning toolkit
- ◆ Periodically re-assess Capital Planning best practices

The Committee's success in achieving the goals of the CIO Council will be indicated by the following:

- Agencies will utilize concepts of model programs for capital planning and IT management
- The CIO, CFO and budget communities continue to collaborate and share information for the improvement of managing IT investments
- Federal agencies will have the capability and tools available to manage IT investments
- Voluntary adoption and use of recommended tools across federal agencies

B. Enterprise Interoperability and Emerging Information Technology



Marvin Langston, DoD

Co-Chair

Lee Holcomb, NASA

Co-Chair

Many of today's systems are narrowly focused, not fully interoperable, support a single function or organization, and require users to assemble information from incompatible sources. As information generation capabilities become more complex, and as citizens' service expectations rise, the Federal Government must begin to manage information for the user, integrating and modernizing its information infrastructure.

The focus of the Enterprise Interoperability and Emerging Information Technology Committee is to lay the foundation for government business processes and systems to operate seamlessly in a governmentwide enterprise architecture that provides models and standards that identify and define the information services used throughout the government. This will require:

- A Federal Enterprise Architecture Framework
- Standard applications and technology solutions to support the framework
- The necessary collaboration during the transitional processes to bring it all together

Guided by the priorities of the Clinger-Cohen Act, the Council directed development of a Federal Enterprise Architecture to maximize the benefits of information technology within the government. Architectures for selected high-priority, cross-agency business lines, or segments, will be developed to populate the Federal Enterprise Architecture. Version 1.1 of the CIO Council's Federal Enterprise Architecture Framework was published in September 1999 and will serve as the foundation to provide consultation on and implement the Federal Enterprise Architecture Framework. The CIO Council developed the nonrestrictive framework to be easily adaptable to all federal agencies, especially those with existing architectures. The Council members and related working groups, consisting of representatives from several agencies, maintained the appropriate regard for current architecture efforts within their agencies while focusing on the need for a governmentwide framework.

Successfully implementing the framework will provide the following benefits:

- Consistent organization of federal information
- Increased data quality
- Reduced data collection burden
- Promote information and resource sharing
- Provide common business processes to support federal re-invention initiatives
- Help federal organizations develop their architectures

- Allow for consistent presentation of federal information through the Internet

Standard applications and technology solutions will be supported by the Committee through sponsorship and coordination of monitoring and evaluation efforts for emerging technologies applicable to enterprise-wide use in two ways. The first will provide awareness of new leading-edge technologies to provide an understanding of the strategic trends and their impact. The second will provide advisory and consulting services to assist in evaluating the viability of using emerging technologies in the federal environment. This information will be tailored to supplement, not replace, the knowledge resources available at the agency level.

The following Enterprise Interoperability and Emerging Information Technology Committee objectives directly support the CIO Council's goals to, "establish the Council as a recognized leader in the government IT community," and to "improve management and results of IT in government to deliver better service to the citizen in accordance with Clinger-Cohen intent":

1. **Facilitate the Information Technology infrastructure of government**
2. **Support collaboration and resource sharing**
3. **Develop governmentwide architecture and technology strategy**
4. **Develop unified government voice on standards and technology requirements**

The following sections describe the Committee's objectives, strategies and initiatives the Committee will pursue to enhance federal enterprise interoperability and best use emerging technology.

Objective #1

Facilitate the Information Technology infrastructure of government

Strategies and Initiatives to achieve this objective

This objective will provide tools and resources that will enable the rapid insertion of advanced technologies to support federal agencies' missions and movement toward a federal enterprise. The Committee role will strive to ensure that the selection and deployment of new technologies are accessible (e.g., work with adaptive technologies for people with disabilities), compatible with the current and future infrastructure, and meet common business needs. Partnerships in the policy, technical, business, and legal arenas will be leveraged to amplify impact. As the linkages of the extended federal enterprise are created, the Committee will explore how to best apply and promote knowledge management throughout the enterprise.

A high priority initiative is supporting the common physical/cyber access solution pilot, which uses the Public Key Infrastructure (PKI) smart card. The Committee's role will focus on the infrastructure component of the project and be conducted in close coordination with the Security, Privacy, and Critical Infrastructure Committee and other coordinating bodies (e.g., Smart Card Project Managers, Federal PKI Steering Committee, PKI Technical Working Group, and Biometrics Consortium).

The following initiatives define the strategy to achieve this objective:

1.1 Next Generation Internet infrastructure to provide connectivity for non-R&D agencies

1.2 Promote infrastructure to provide common physical/cyber access solutions

1.3 Develop a partnership between participants from policy, technical, business, and legal arenas; promote a forum to bring all together

1.4 Build an understanding of relationships to promote knowledge management throughout government

1.5 Promote accessibility and usability in the Federal Government

Objective #2

Support collaboration and resource sharing

Strategies and Initiatives to achieve this objective

To provide the necessary collaboration during the transitional processes, clear and precise communications must be established and maintained to solve common business problems and share resources. Affinity groups will address inefficiencies in key business process applications that affect multiple federal agencies by facilitating standardization. In the near-term, the Committee will focus on facilitating the standardization of select federal government administrative information processing, e.g., human resources and budget. Program subject matter experts and IT professionals will collaborate to ensure that common solutions meet shared business needs while employing the optimum information technology as an enabler.

This critical role will be performed in close coordination with the Outreach Committee as appropriate.

The Council sponsors development of the Federal White Pages Directory (directory.gov) as the first stage to deployment of standards-based, interoperable directories to support transactions within and between agencies, and with federal customers and partners.

The following initiatives define the strategy to achieve this objective:

2.1 Establish affinity groups (i.e., human resources, grants, and finance) for higher level business applications

2.2 Complete development, population, and 1st-year operation of the Federal White Pages Directory (“directory.gov”)

Objective #3

Develop governmentwide architecture and technology strategy

Strategies and Initiatives to achieve this objective

In serving the strategic needs and direction of the Federal Government, the Committee will sponsor and coordinate enterprise architecture teams to develop and facilitate the implementation of the top-level enterprise architecture for the federal enterprise. The framework provides an organized structure and a collection of common terms by which federal segments (major business areas) can integrate their respective architectures into the Federal Enterprise Architecture.

A pilot will be conducted to validate the framework's approach and value. The findings will be shared with participants and the architecture community. Segment development will include building and populating a federal architecture repository that will provide a defined set of tool interfaces and data exchange mechanisms. The Committee will continue to support the effort by sponsoring and coordinating enterprise architecture teams to develop, populate, and publish integrated architecture segments.

The following initiatives define the strategy to achieve this objective:

3.1 Federal Enterprise Architecture Framework consulting and quantifying benefits of architecture

3.2 Develop Federal Architecture Segments

3.3 Provide architecture tools to support segments

3.4 Establishing a central knowledge base for emerging technologies within the Federal Enterprise Architecture and evaluate emerging technologies

Objective #4

Develop unified government voice on standards and technology requirements

Strategies and Initiatives to achieve this objective

This objective will ensure that standards affecting governmentwide interoperability are properly developed and communicated by providing a dedicated organization to serve as a liaison with voluntary IT standards committees. The Committee will ensure that appropriate federal organizations are aware of opportunities to provide representation on voluntary standards committees. The Committee will support the development and maintenance of an automated, web accessible, repository of federal government representation to the various voluntary standards committees. This repository will provide a single authoritative source for federal government organizations to utilize when seeking either information about standards under development, or to input requirements into specific voluntary standards committees. Standards developed in the community will be regularly reviewed to ensure they satisfy requirements that were submitted by the Federal Government.

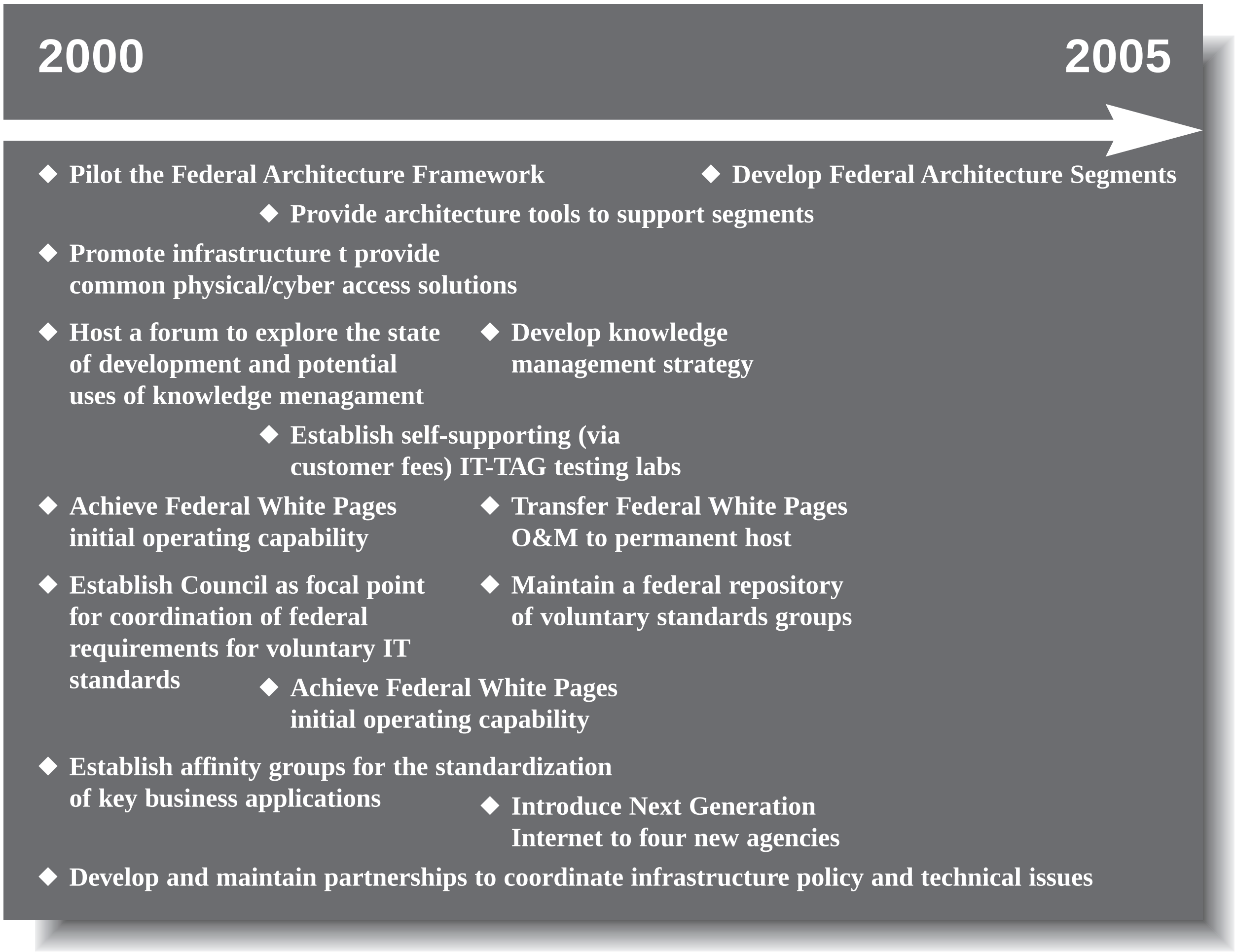
The following initiatives define the strategy to achieve this objective:

4.1 Sponsor the Electronic Documents Symposium

4.2 Focal point for discussion, definition, and coordination of federal requirements for voluntary IT standards

Success Indicators:

Selected initiatives and high-level milestones are as follows:



2000

2005

- ◆ **Pilot the Federal Architecture Framework**
- ◆ **Develop Federal Architecture Segments**
- ◆ **Provide architecture tools to support segments**
- ◆ **Promote infrastructure t provide common physical/cyber access solutions**
- ◆ **Host a forum to explore the state of development and potential uses of knowledge menagament**
- ◆ **Develop knowledge management strategy**
- ◆ **Establish self-supporting (via customer fees) IT-TAG testing labs**
- ◆ **Achieve Federal White Pages initial operating capability**
- ◆ **Transfer Federal White Pages O&M to permanent host**
- ◆ **Establish Council as focal point for coordination of federal requirements for voluntary IT standards**
- ◆ **Maintain a federal repository of voluntary standards groups**
- ◆ **Achieve Federal White Pages initial operating capability**
- ◆ **Establish affinity groups for the standardization of key business applications**
- ◆ **Introduce Next Generation Internet to four new agencies**
- ◆ **Develop and maintain partnerships to coordinate infrastructure policy and technical issues**

The Committee’s success in achieving the goals of the CIO Council will be indicated by the following:

- Successful PKI smart card interoperability testing
- Non-R&D federal agency transition to the Next Generation Internet
- Procurement officials acceptance of IT Testing for Accessibility Governmentwide (IT-TAG) certification of accessibility and usability

- Agency participation in and overall usage of the Federal White Pages
- Acceptance of the Committee’s role in coordinating infrastructure policy recommendations and technical issues
- Value, as determined by the pilot, of the Federal Architecture Framework
- Architecture segments are defined through collaboration among federal agencies
- Standards decisions are made as a result of the Electronic Document Symposium
- Voluntary standards committees actively seek Committee input on their work
- Usage, and reported accuracy, of the federal repository of voluntary standards groups

C. Federal IT Workforce

Gloria Parker, HUD

Co-Chair

Ira Hobbs, USDA

Co-Chair

The strategic agenda of the Council looks to the future as a time when every government organization transforms itself into a truly digital enterprise. However, as the Federal Government increases these efforts and continues to use technology to support the taxpayer in providing high-quality customer service, it must face the reality that IT human resources are in short supply. The increasing need for qualified IT professionals puts the government in direct competition with the private sector for scarce resources. In addition, the disparity in IT salaries between the government and private sectors augments the challenges facing federal IT managers.

Highlighting this issue, the Clinger-Cohen Act of 1996, the work of the National Partnership for Reinventing Government (NPR), GPRA, and the GAO all set-forth guidance to government agencies that supports the need for immediate action to ensure that the government's workforce has the skills necessary to effectively operate in today's high-tech environment. To effectively address this challenge, and leverage efforts governmentwide, the CIO Council developed the Federal IT Workforce Committee. This broadens the focus from the previous year in order to provide a unified focus across government to deal with the critical shortage of skilled IT professionals as well as to expand the skills of the federal workforce.

In direct support of the CIO Council's goals to "establish the strategic IT direction for the Federal Government and identify government-wide IT priorities" and to "improve management and results of IT in government to deliver better service to the citizen in accordance with Clinger-Cohen intent," the objectives of the Federal IT Workforce Committee are to:

1. **Validate and substantiate the extent of the federal IT workforce challenge**
2. **Develop and implement strategies for recruitment, retention, and development of Information Technology professionals and upgrade skills of current workforce**

The following sections describe the objectives, strategies and initiatives that the Committee will pursue in order to contribute to government agencies' capability to develop, attract, and retain a professional federal IT workforce.

Objective #1

Validate and substantiate the extent of the federal IT workforce challenge.

Strategies and Initiatives to achieve this objective

Determining the true nature and scope of complex issues facing the federal IT workforce is needed in order to take appropriate targeted action. It is critical to understand the true impact of competition between the sectors for scarce IT talent, the inherent barriers and constraints in the federal personnel management system, and the need for effective training to address the rapid changes in technology and service delivery. To this end, the Committee will champion a study to validate and substantiate the challenges identified in the CIO Council's 1999 "Federal IT Workforce Challenge Report." This study will address in depth the issues in the areas of IT workforce recruitment, retention, ongoing staff education and skill development as well as competitive salary recommendations. Completion of the study alone is not enough. The Committee plans to partner with the Office of Personnel Management (OPM) to gain widespread support in the development of a new occupational pay system for federal IT workers.

The following initiatives define the strategy to achieve this objective:

1.1 Partner with OPM and National Academy of Public Administration (NAPA) to sponsor a study to document the compensation and retention issues associated with federal and private sector IT workers

1.2 Implement recommendations from study of compensation and retention issues

Objective #2

Develop and implement strategies for recruitment, retention, and development of Information Technology professionals and upgrade skills of current workforce.

Strategies and Initiatives to achieve this objective

The landmark report, "The Federal IT Workforce Challenge," released by the CIO Council in 1999, outlined 13 specific recommendations for near-term implementation. The Committee will continue to identify and promote best practices based on study recommendations including: critical needs hiring authorities; recruitment from non-traditional labor pools; IT career academies; scholarship and internship programs to promote IT careers in colleges and universities; mentoring programs and regional skill alliances. Development and delivery of governmentwide competency-based training and education programs will be a particular focus for the

Committee. Two key programs will be launched to address competencies required by recent reform legislation: CIO University and the Strategic and Tactical Advocates for Results (STAR) program. The CIO University is a virtual consortium of universities designed to enhance the skills of federal government's top executives. STAR focuses on tomorrow's government workplace emphasizing Clinger-Cohen results-based management, as well as IT as a strategic resource. The implementation of these recommendations and key programs are essential if the government is to fully address the IT workforce challenge. The CIO Council's role is as advocate of the recommendations. This will require partnerships across government and industry. To the extent possible the Committee will facilitate such actions acting as a catalyst for change.

The following initiatives define the strategy to achieve this objective:

2.1 Support full implementation of all 13 recommendations from the Federal IT Workforce Challenge Report

2.2 Pilot, evaluate and maintain the CIO University

2.3 Partner with the Critical Infrastructure Assurance Office (CIAO) to develop and foster educational programs and outreach efforts specifically focused on security management

2.4 Pilot and evaluate the STAR Project and Program Management project

2.5 Establish the CIO Executive Exchange program in collaboration with OPM

2.6 Promote recognition programs to showcase outstanding achievements of current federal IT professionals

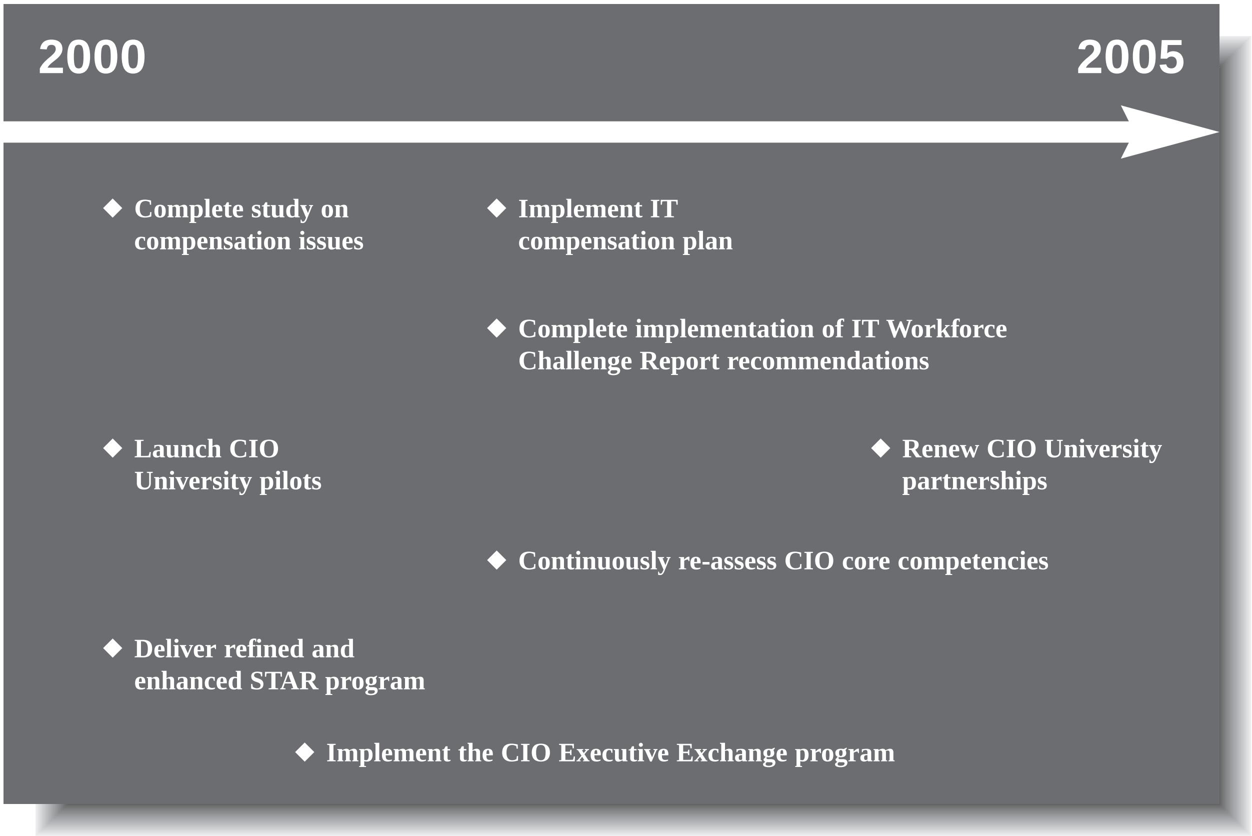
2.7 Develop "road maps" for meeting the core competency training needs of staff including ensuring a basic level of computer competency

2.8 Review and revise CIO core competencies on a biennial basis

Success Indicators

The Committee will oversee preparation of a Federal IT Workforce Challenge Study Implementation Plan. In conjunction with the contractor performing the study, an initial set of performance goals will be established which will include study completion by April 2000. Based on the Federal IT Workforce Committee's role, performance assessments will be specified. Timely and satisfactory completion of projected milestones will provide interim measures of progress. Distinct measures will be developed for key programs, such as CIO University and the STAR program, to measure their impact over time.

Selected high-level milestones, are illustrated in the following chart:



2000 **2005**

- ◆ **Complete study on compensation issues**
- ◆ **Implement IT compensation plan**
- ◆ **Complete implementation of IT Workforce Challenge Report recommendations**
- ◆ **Launch CIO University pilots**
- ◆ **Renew CIO University partnerships**
- ◆ **Continuously re-assess CIO core competencies**
- ◆ **Deliver refined and enhanced STAR program**
- ◆ **Implement the CIO Executive Exchange program**

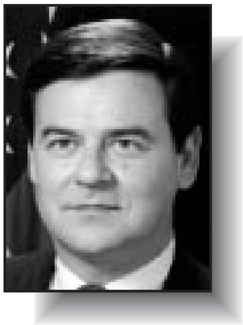
The Committee's success in achieving the goals of the CIO Council will be indicated by the following:

- Implementation of information technology and information management core competencies throughout the federal workforce
- Implementation of qualification and classification standards and competitive pay schedule for key IT occupations that contribute to recruitment and retention of IT professionals
- Agencies will have the tools and capability to address the gap in IT workforce resources
- Agencies will use model programs for successfully training and retaining their employees

D. Outreach

Alan Balutis, Commerce

Co-Chair



David Borland, Army

Co-Chair

In projecting the potential for the future of IT in government the Council asserts the need for a unified voice in championing issues that extend beyond any one agency and affect the entire federal community. Toward this end, collaboration and partnerships are critical to the priorities envisioned by the Outreach Committee.

The Committee has outreach responsibilities both external and internal to the Council. External responsibilities of the Outreach Committee focus on collaborations and partnerships to encourage communications between the Council and the Congress, state and local government counterparts, industry, academia, the media, and customers. The Council is shaping a more fluid interface with the federal CIO community and industry, various levels of government, and the American public. The Committee seeks to facilitate the development and sharing of information, knowledge, policies, and best practices among these groups.

Within the Council, the Outreach Committee serves as an integrating point for outreach-type initiatives, sponsored by the other Council Committees, to:

- Publicize and communicate their accomplishments, reports, and plans outside the Council
- Coordinate and interface between outside entities and the substantive Committees to guide and channel interactions and communications
- Serve as the gatekeeper and initial point of contact for those who want to interact with the Council

In support of the CIO Council's goals to "establish the Council as a recognized leader in the government IT community" and to "be recognized as a key partner with the global IT community," the objectives of the Outreach Committee are to:

1. **Create high-leverage partnerships with international, federal, state, and private sector Information Technology leadership groups**
2. **Promote the Council's credibility in Information Technology leadership**
3. **Establish CIO Council Intranet and Extranet for states and others**

The following sections describe the objectives, strategies, and initiatives of the Outreach Committee.

Objective #1

Create high-leverage partnerships with international, federal, state, and private sector Information Technology leadership groups.

Strategies and Initiatives to achieve this objective

The Committee will continue to expand and establish the necessary partnerships to support the Strategic Agenda. The Committee will serve as the coordinating point for interactions and communications with national and international partners. Partnerships or councils with entities such as the CFOs, PCIE, NASIRE, Internet II, NARA, OSTP, and the R&D community will be examined. The Council will seek to create an international partnership through existing conferences and alliances. The partnerships may also include the Committee's leadership in the establishment of a common government portal.

The Committee will gain insight into the internal operations of private sector CIO associations to determine private sector best practices, success models, and performance measurements applicable governmentwide.

The following initiatives define the strategy to achieve this objective:

1.1 Expand and explore opportunities for increased interaction and outreach with the worldwide IT community to disseminate and share information, knowledge, policies, best practices, etc.

1.2 Analyze private sector CIO associations

Objective #2

Promote the Council's credibility in Information Technology leadership.

Strategies and Initiatives to achieve this objective

The Committee will work with the Council's Executive Committee to gain the support of Congress, GAO, and the Inspector General (IG) on issues associated with the Council's Strategic Agenda.

The use of publishing, educational/informative audio/video products, web casts, and a website will be effectively applied across the Council's initiatives to reach target audiences and to interact with colleagues, constituents, and partners. The Council will actively participate in or sponsor key events that provide valuable opportunities to communicate or accomplish Council Strategic Agenda items.

Examples of near-term publications include Best IT Practices, Vol. II and articles in Electronic Government, Federal Times, Federal Computer Week, Government Computer News, and the Washington Post Federal Page. Web casts, on TvontheWeb.com and other sites, may cover CIO Council bi-monthly meetings, special Committee meetings, and major events that CIO Council representatives participate in.

In support of other Council Committees' outreach related activities, the Committee will publish a "Quick Guide" to assist Committees in publicizing upcoming events and new products to their communities of interest. Committee members will work with the Outreach Committee, the Council Liaison Office, and others to publicize the work and accomplishments of their Committee and the CIO Council as a whole.

The following initiative defines the strategy to achieve this objective:

2.1 Publicizing and outreach activities

Objective #3

Establish CIO Council Intranet and Extranet for states and others.

Strategies and Initiatives to achieve this objective

In promoting the Strategic Agenda, the Council seeks to reach a targeted audience interactively within and outside the IT community. A CIO Council Intranet and Extranet will refine, expand, and explore open communication and information dissemination activities with various IT partners, including the states.

The Council will achieve this objective through leverage of existing resources to the maximum extent possible to:

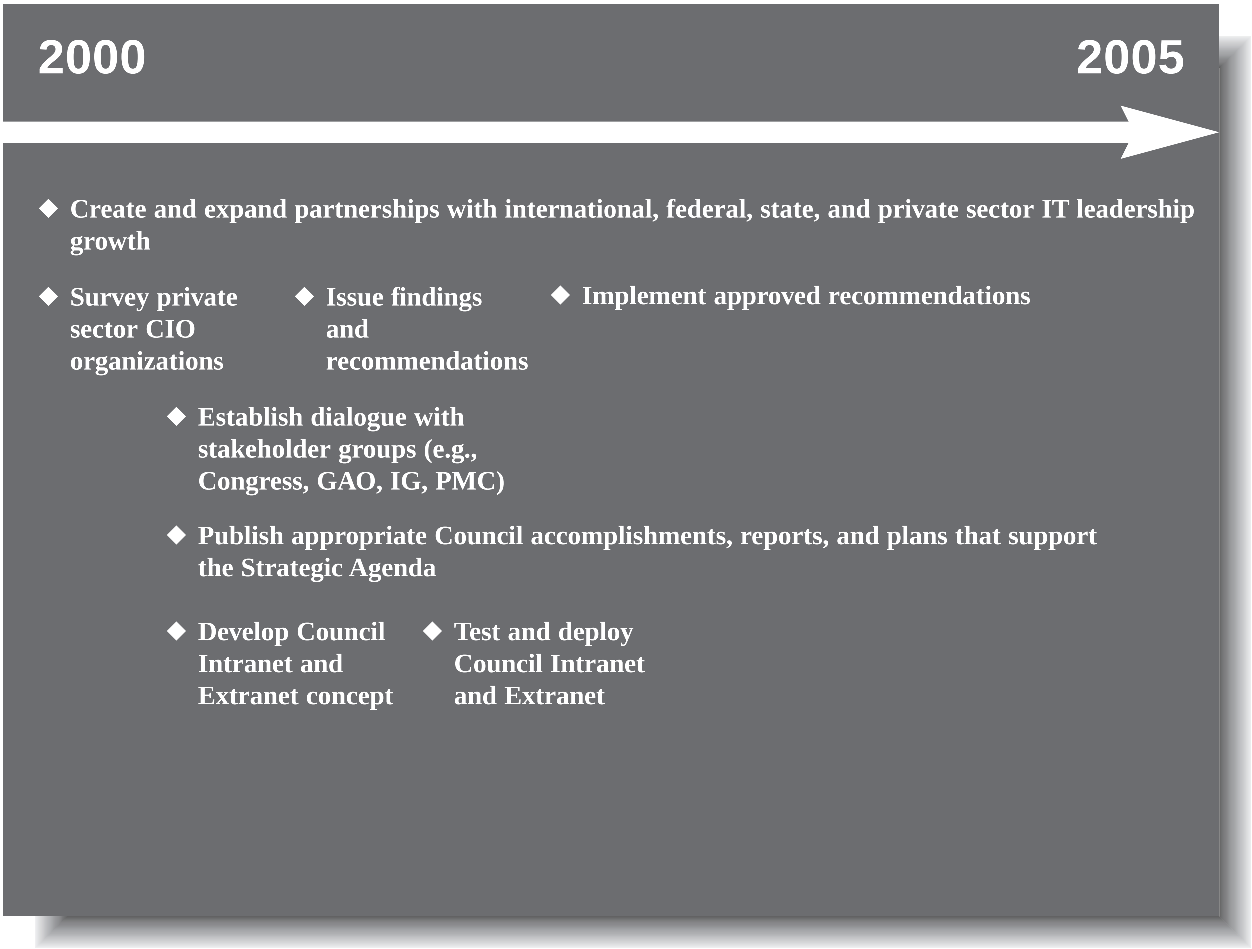
- Facilitate dialogue with states and others to develop concept
- Design and implement Intranet and Extranet linkages
- Implement test sites
- Develop and execute appropriate deployment strategies

The following initiative defines the strategy to achieve this objective:

3.1 Refine, expand and explore open communication and information dissemination activities with various IT partners

Success Indicators

Selected initiatives and high-level milestones are as follows:



2000

2005

- ◆ Create and expand partnerships with international, federal, state, and private sector IT leadership growth
- ◆ Survey private sector CIO organizations
- ◆ Issue findings and recommendations
- ◆ Implement approved recommendations
- ◆ Establish dialogue with stakeholder groups (e.g., Congress, GAO, IG, PMC)
- ◆ Publish appropriate Council accomplishments, reports, and plans that support the Strategic Agenda
- ◆ Develop Council Intranet and Extranet concept
- ◆ Test and deploy Council Intranet and Extranet

The Committee’s success in achieving the goals of the CIO Council will be indicated by the following:

- Increased efficiency and/or performance of the Council based on the private sector CIO associations survey (to be measured 6 months after recommendations are adopted)
- Increase in the number of valuable partnerships
- Usage of products (e.g., Intranet and Extranet usage)

E. Security, Privacy, and Critical Infrastructure

Roger
Baker,
Commerce

Co-Chair

Fernando
Burbano,
State

Co-Chair

John
Gilligan,
Energy

Co-Chair

The Federal Government has a crucial responsibility to maintain the security of its systems, the privacy of its citizens, and its critical infrastructure. Throughout government there is a shared realization that rapid advances in technology, interconnectivity, and expanding usage of the Internet increases the need for and priority on adequate security and privacy measures. In February 1997, GAO designated information security as a new governmentwide high-risk area. On May 22, 1998 Presidential Decision Directive (PDD) 63 was issued and declared that “the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructure, including especially our cyber system.”

The Committee provides leadership, support, and awareness to address the three interrelated areas of security, privacy, and critical infrastructure to benefit the entire federal community. Critical infrastructure involves the security of physical and cyber-based systems essential to the minimum operations of the economy and government. The highly personal and sensitive nature of the data contained in today’s automated systems calls for a reexamination of the proper balance between the competing values of personal privacy and the need for the sharing of information required by current and future interoperability.

Federal agencies’ plans for the protection of their respective critical infrastructure have been prepared and reviewed by the Expert Review Team (ERT). The agencies are now in the process of implementing their plans by May 22, 2003 to establish and maintain the ability to protect our nation’s critical infrastructure from intentional acts that would significantly diminish the ability to perform essential public services. This will require coordinated efforts throughout the federal community in order to avoid inappropriate duplication of effort and ensure governmentwide cooperation. Entities with which the Committee will collaborate include the CIAO, National Institute of Standards and Technology (NIST), National Security Agency (NSA), the Government Information Technology Services (GITS) Board, the National Infrastructure Assurance Council (NIAC), and others. As interoperability will also support overall security objectives, close coordination of crosscutting initiatives with the Enterprise Interoperability and Emerging Information Technology Committee will be maintained.

To support the Council’s goals to “establish the strategic IT direction for the Federal Government and identify governmentwide IT priorities,” "establish the Council as a recognized leader in the government IT community," "be recognized as a key partner with the global IT community," as well as "improve management and results of IT in government to deliver better service to the citizen in accordance with Clinger-Cohen intent," the following objectives have been developed.

1. **Lead the establishment of integrated, governmentwide Information Technology guidelines, best practices, tools, training, and proposed policies in areas of privacy, critical infrastructure, and security**

2. **Support service delivery capabilities of federal agencies by determining security and privacy approaches that advance appropriate information access, exchange, and protection and support Electronic Commerce**

3. **Promote awareness of security, privacy, and critical infrastructure issues**

4. **Establish a leadership role within the CIO Community in the implementation of PDD-63**

The following sections describe the Security, Privacy, and Critical Infrastructure Committee's objectives, strategies, and initiatives.

Objective #1

Lead the establishment of integrated, governmentwide Information Technology guidelines, best practices, tools, training, and proposed policies in areas of privacy, critical infrastructure, and security.

Strategies and Initiatives to achieve this objective

The Committee will identify and 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 security guidance and the Privacy Act. The Committee will promote greater efficiency and preserve valuable public resources by coordinating and consolidating, as appropriate, ongoing federal security best practice activities and initiatives, and by developing a model "privacy impact assessment" as a tool for agencies to provide privacy protections when creating or revising new information systems. In evaluating government and industry-developed practices and proposed model agency security and privacy policies, the Committee will apply a management perspective to ensure that such practices and policies:

- Conform to OMB policies and NIST guidance
- Enable and do not unnecessarily impede business operations
- Are risk-based, cost-effective, and provide sufficient flexibility to accommodate individual agency requirements

As appropriate, the Committee will make recommendations to NIST for the development of security related Federal Information Processing Standards.

Incident response teams note that one of the most serious security threats to the Internet results from the failure to install patches for known security vulnerabilities. NIST, GSA, CIAO, and OMB will address this issue. The Committee will actively participate in the development of an "options paper" to address this problem governmentwide. The Committee will further support this effort by proposing and disseminating relevant policies and procedures.

The following initiatives define the strategy to achieve this objective:

1.1 Identify, evaluate, and disseminate best practices, including products that have been certified or accredited under recognized federal authorities (e.g., Common Criteria, National Infrastructure Assurance Plan (NIAP), etc.)

1.2 Work with OMB and NIST to identify draft or sample policies (e.g., model procurement guidelines for the acquisition of information assurance products, systems, and services, and model privacy impact assessments) for use by federal agencies in the areas of security and privacy

1.3 Promote the maintenance of up-to-date system patches, the closing of vulnerabilities, and the establishment of other warning and noticing processes to improve the security of systems by federal agencies

Objective #2

Support service delivery capabilities of federal agencies by determining security and privacy approaches that advance appropriate information access, exchange, and protection and support Electronic Commerce.

Strategies and Initiatives to achieve this objective

To assist in assuring that the interests of Executive Branch agencies are balanced in federal computer security requirements and preservation of the right to privacy, where appropriate, the Committee will review proposed legislation, regulations, guidance and standards consistent with the interagency process governing such reviews. The Committee also will leverage its membership to identify security and privacy issues that are important to individual agencies and communicate concerns to lawmakers and regulatory agencies.

The Committee will support the risk assessment of mission enabling emerging technologies, including identification of mitigating security solutions. The Committee will leverage available resources and existing efforts, facilitate the consensus of recommendations, and disseminate resulting information. This approach encourages that the broader government risk/reward equation is considered and that informed decisions are made on implementing emerging IT solutions to satisfy agency needs.

The Committee will explore ways of ensuring privacy assurance for federal websites. Given that all federal agencies now have announced good privacy policies on their principal websites and are working toward ensuring that those notices appear in other appropriate places, the next step is to study ways to assure web users that agencies are complying with their stated policies. One mechanism to explore is the utility, feasibility, and appropriateness of a federal privacy seal. A seal, or other privacy assurance mechanism, would aim to win the confidence of the American citizen engaging in online transactions with the Government. This effort will consider the laws pertaining to federal agencies that are different than those that apply to commercial operations.

The following initiatives define the strategy to achieve this objective:

2.1 Assist with ensuring that the interests and concerns of Executive Branch agencies are expressed and addressed in the development or review of proposed legislation, regulations, guidance, or standards when appropriate and relating to security, privacy and critical infrastructure

2.2 Partnering with the GITS Board, promote coordinated agency efforts to use public key technology for authentication and confidentiality for transactions over open networks

2.3 Identify security and privacy solutions that enable delivery of services while ensuring adequate security and privacy in a risk balanced implementation

Objective #3

Promote awareness of security, privacy, and critical infrastructure issues.

Strategies and Initiatives to achieve this objective

The Committee will work with the National Coordinator for Security, Infrastructure Protection and National Security and the CIAO to coordinate a national education and awareness program to increase public, federal IT users, system administrators, security specialists, and information systems managers understanding and participation in the protection of critical infrastructure.

Adequate funding resources need to be identified and maintained to achieve appropriate focus on privacy. The government's ability to exploit the benefits of IT will be limited if privacy, as well as security, issues are not addressed. The Committee will work within existing structures and organizations, such as the National Science Foundation, to identify funding sources and mechanisms to advance IT privacy governmentwide.

The Council will work with the IG and other audit groups to accelerate change and compliance. The Committee's work products may include resources that help OMB and NIST establish acceptable governmentwide practices and policies for use by federal agencies. This will provide the IG and the external audit community the information necessary to conduct effective and useful audits.

The following initiatives define the strategy to achieve this objective:

3.1 Conduct Security Awareness Day

3.2 Work with other governmental and non-governmental entities to communicate and clarify privacy and security concerns (including legal issues) and the need for strong privacy and security protections on systems

3.3 Identify funding for technological solutions that advance secure information access and exchange with privacy

3.4 Work with the CIAO to sponsor Partnership for Critical Information Security

3.5 Share Committee work products with IG and audit community

Objective #4

Establish a leadership role within the CIO Community in the implementation of PDD-63.

Strategies and Initiatives to achieve this objective

Working closely with the CIAO, the Committee will develop a set of measures/metrics to standardize the tracking of progress toward implementing the requirements of PDD-63 within Federal Government. Further, the Committee will support the National Coordinator, OMB, CIAO, and the ERT in implementing standard audit/review processes across all departments and agencies. This may include measurement collection techniques, reporting procedures, independent verification and validation activities, security requirements, and cost estimates.

The Committee will establish a reputable website source for the public and the CIO community to access information regarding PDD-63, without replicating information already posted on other sites.

In coordination with Outreach Committee activities, the Committee will sponsor various forums for the promotion of activities and dissemination of issues in regard to PDD-63. This will include initiating and assisting in the creation of conferences and workshops with PDD-63 as the primary subject. It also will include participating in other technology conferences at which a keynote speaker from the CIO community promotes PDD-63 implementation and compliance [e.g., Interagency Resources Management Conference (IRMCO), Federal Office Systems Exposition (FOSE), E-gov (Electronic Commerce in Government), and the Industry Advisory Council (IAC).]

The following initiatives define the strategy to achieve this objective:

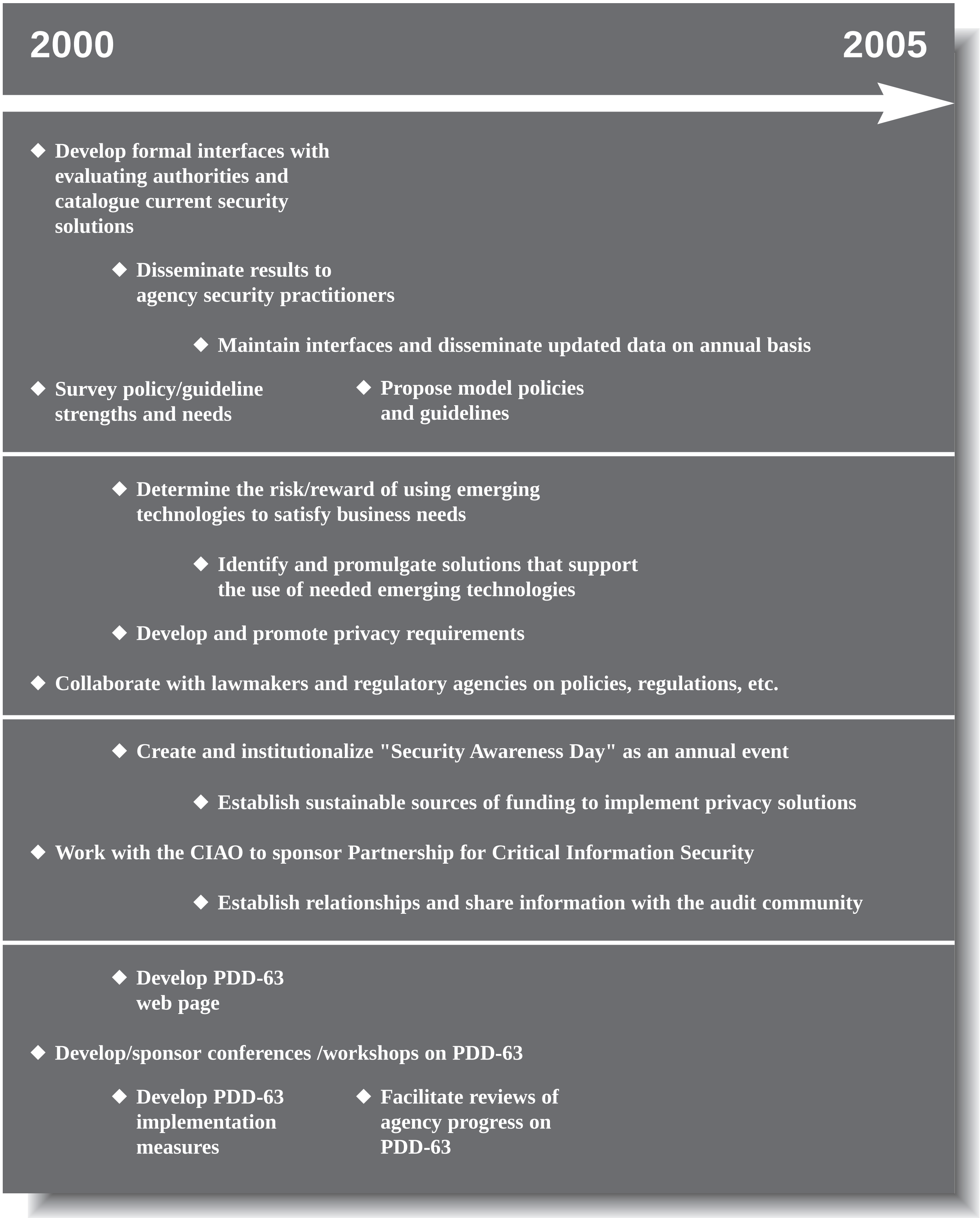
4.1 In conjunction with the CIAO, establish a webpage within the CIO Council website, to provide up-to-date information regarding PDD-63

4.2 Lead and partner with other organizations to sponsor conferences, newsletters, and workshops to promote activities and issues in regard to PDD-63 and privacy issues (e.g., IRMCO, FOSE, E-gov, IAC)

4.3 Assist the National Coordinator, OMB, and the CIAO in tracking the progress of implementing PDD-63

Success Indicators

Selected initiatives and high-level milestones, are illustrated in the following chart:



2000

2005

- Develop formal interfaces with evaluating authorities and catalogue current security solutions
- Disseminate results to agency security practitioners
- Maintain interfaces and disseminate updated data on annual basis
- Survey policy/guideline strengths and needs
- Propose model policies and guidelines

- Determine the risk/reward of using emerging technologies to satisfy business needs
- Identify and promulgate solutions that support the use of needed emerging technologies
- Develop and promote privacy requirements
- Collaborate with lawmakers and regulatory agencies on policies, regulations, etc.

- Create and institutionalize "Security Awareness Day" as an annual event
- Establish sustainable sources of funding to implement privacy solutions
- Work with the CIAO to sponsor Partnership for Critical Information Security
- Establish relationships and share information with the audit community

- Develop PDD-63 web page
- Develop/sponsor conferences /workshops on PDD-63
- Develop PDD-63 implementation measures
- Facilitate reviews of agency progress on PDD-63

The Committee’s success in achieving the goals of the CIO Council will be indicated by the following:

- Security practitioner use of, and feedback on, information provided
- Acceptance and usage of proposed policies and guidelines
- The number of agencies that adopt and promulgate privacy impact assessments as an integral part of their development of information systems
- Agencies primarily responsible for drafting governmentwide regulations on computer security (OMB, GSA, NIST, etc.) consistently turn to the CIO Council as part of the process to develop, revise, or interpret federal regulations
- Establishment of a Federal Privacy Compliance Program
- Positive feedback on sponsored awareness and training programs
- An increase in the number and appropriateness of education and awareness programs offered to employees
- Feedback on and access to the PDD-63 webpage on the Council website
- Implementation of a standard process and measures to evaluate the progress toward PDD-63 compliance

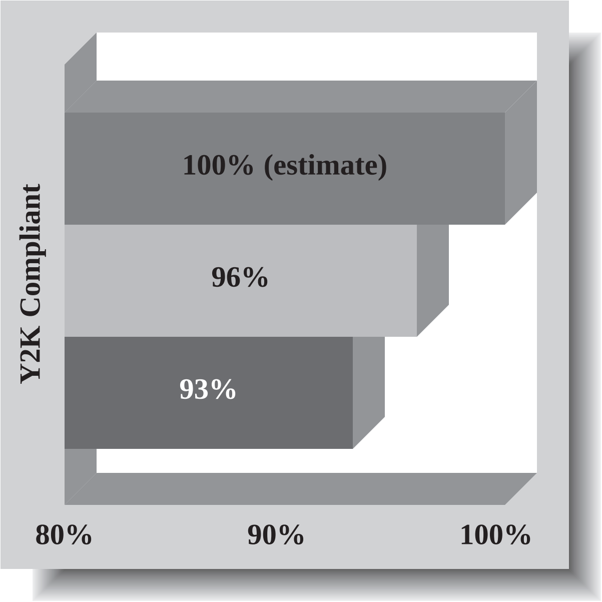
F. Year 2000

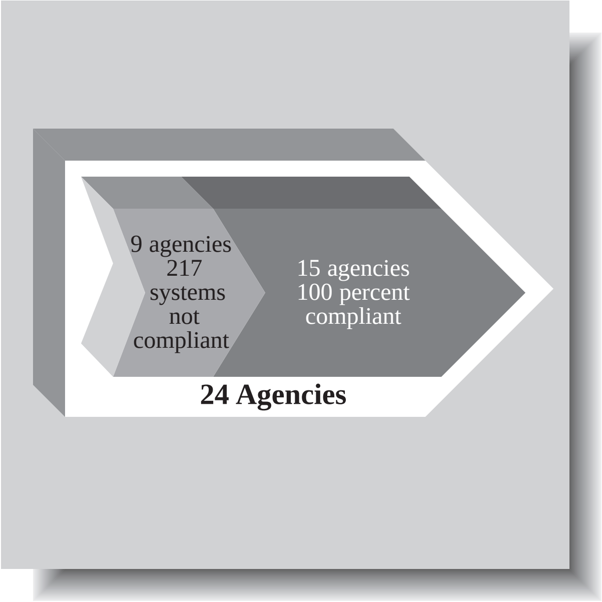
Shirley Malia, Labor

Chair

Agencies throughout the Federal Government are ready to bid farewell to the urgent demands of the Year 2000 (Y2K) conversion efforts. While these efforts continue to be necessary and prudent, they are consuming huge amounts of resources. The costly Y2K efforts have not ended and will not end until early in the year 2000. Even Y2K compliant systems must be subject to “clean management,” i.e., continued scrutiny for Y2K compliance of any changes or additions made to existing systems.

The most urgent need continues to be preserving the integrity of service delivery to the American taxpayer. As set forth in Executive Order 13073, the American people expect reliable service from their government and deserve the confidence that critical government functions dependent on electronic systems will be performed accurately and in a timely manner. Because of the Year 2000 problem, preeminent in many electronic systems, federal agencies have been diligently working to convert their systems for compliance and to avoid potential disruptions. Since dates are used in calculations throughout software applications, there are many risks threatening government information systems and related software both inside federal agencies, affecting internal operations, and outside agencies, in systems where federal data is shared or transferred. The CIO Council is diligently working in conjunction with the President’s Council on Year 2000 Conversion to mitigate potential problems. The CIO Council’s Year 2000 Committee anticipates that the problem will be mollified the first quarter of the fiscal year. Once systems are compliant, the immediate risk affecting federal agencies that need to deliver mission-critical services to large segments of the population will be mitigated.





As of September 1999, federal agencies are reporting that 96 percent of their mission critical systems are now Y2K compliant, an increase from 93 percent reported in June 1999. In addition, out of a total of twenty-four agencies, fifteen report that they have completed work on 100 percent of their mission critical systems. Nine report that they still have a combined total of 217 mission critical systems that are not yet compliant, down from the 410 systems reported as non-compliant in June. These agencies will continue to report on each mission critical system until 100 percent compliance is achieved.

The Year 2000 Committee supports the CIO Council's goals by pursuing the following objectives:

1. **Reemphasize Information Technology management practices to assure that mission-critical systems work on, before, and after January 1, 2000**

2. **Identify joint efforts to leverage resources for solving the Year 2000 problem**

The following sections describe the objectives, strategies and initiatives that the CIO Council will continue to pursue in order to contribute to the Federal Government's efforts to address the Year 2000 problem.

Objective #1

Reemphasize Information Technology management practices to assure that mission-critical systems work on, before, and after January 1, 2000.

Strategies and Initiatives to achieve this objective

As the Year 2000 problem presents significant technical, management, and contracting challenges requiring immediate attention, the CIO Council's Committee managing Y2K conversion has developed a clearinghouse for information that addresses the computer problem. This clearinghouse is sponsored by the CIO Council and is maintained by the GSA Office of Governmentwide Policy. Supporting the dissemination of information, including industry best practices, is an ongoing process. The Committee will continue to work with GSA to ensure that the public has access to the latest information related to the computer problem.

The following initiatives define the strategy to achieve this objective:

1.1 Maintain the Year 2000 website to share information

1.2 Maintain the Commercial off-the-shelf (COTS) database website

Objective #2

Identify joint efforts to leverage resources for solving the Year 2000 problem.

Strategies and Initiatives to achieve this objective

The Year 2000 problem will in some way, touch the lives of people of all nations. It is a challenge that requires worldwide cooperation and responsibility. The CIO Council's Committee on Y2K has collaborated with individuals throughout the public and private sectors, across industries, and participated in international partnerships to address crosscutting issues. The Committee will continue to capitalize on these partnerships and resources to resolve the problem facing federal agencies.

The Committee, having established a website that serves as a clearinghouse of Year 2000 information, provides ongoing support through Subcommittees which focus on specific areas of concern. Some of these areas include:

- The Telecommunications Subcommittee in conjunction with GSA's Federal Technology Service (FTS) maintains a website that lists the compliance status of telecommunications equipment and has links to over 60 industry sites containing Y2K compliance information.
- The Year 2000 Buildings Subcommittee in conjunction with GSA's Public Buildings

Service has established a public website that provides Y2K information for building systems. In addition, another website has been established which allows personnel from federal agencies to determine the Y2K compliance status of federally owned and leased facilities. This site, however, is for federal government use only.

- The U.S. Federal Government Gateway for Year 2000 Information Directories is managed and maintained by GSA on behalf of the CIO Council. It assists federal agencies in addressing the Year 2000 problems and among other services, it provides links to various organizations' Y2K readiness disclosures and compliance statements.

The following initiatives define the strategy to achieve this objective:

2.1 Meet with NASIRE to address federal/state policy and technical issues

2.2 Conduct telecommunications forums for government and industry

2.3 Maintain website with database of telecommunications products

2.4 Work with the Building Owners and Managers Association (BOMA) on embedded systems testing guidelines and contingency planning

2.5 Maintain and upgrade the building products database on the website

2.6 Maintain and upgrade website on Y2K compliance of biomedical equipment

2.7 The Food and Drug Administration (FDA) will continue to maintain and operate the biomedical equipment clearinghouse, adding future enhancements as necessary

2.8 The FDA will conduct biomedical outreach presentations throughout the remainder of 1999. In addition, the FDA will provide "early alerts," and other warnings to help health care providers to know the status of their biomedical equipment. Finally, the FDA will recall products that experience date failure either before or after January 1, 2000

2.9 Work with industry on Y2K issues of mutual concern

2.10 Maintain the Federal Government gateway for Year 2000 information directory website

Success Indicators

The CIO Council's Committee on Year 2000 intention is to enhance Y2K awareness through the sharing of experiences, problems, progress, solutions, and opinions.

The Y2K Committee will continually assess the readiness of federal agencies in completing mission critical system modifications. Timely and satisfactory completion of projected agency milestones including thorough system testing will provide measures of progress. The ultimate measure of success will be the preparedness of federal agencies in advance of December 31, 1999.

Appendix I
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;

(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

(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;

(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 form 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 quest 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;

(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, Untied 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 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

THE WHITE HOUSE
July 16, 1996

Appendix II
CIO Council Charter

February 20, 1997

UNITED STATES GOVERNMENT
CHIEF INFORMATION OFFICERS COUNCIL

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 cooperation 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.

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.

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.

Appendix III
Partnerships

Armed Forces Communications Electronics Association (AFCEA)
Association for Federal Information Resources Management (AFFIRM)
Chamber of Commerce
Chief Financial Officers Council
Coalition for Government Procurement
Congress
Electronics Industry Association (EIA)
Federal Information Management Exchange (FIMEX)
Federation of Government Information Processing Councils (FGIPC)
General Accounting Office
Government Information Technology Services (GITS) Board
Highway 1
Industry Advisory Council (IAC)
Information Resources Management College
Information Technology Association of America (ITAA)
Interagency Management Council
National Association of State Information Resource Executives (NASIRE)
National Institute of Standards and Technology (NIST)
National Security Agency (NSA)
Presidential Council for Integrity and Efficiency (PCIE)