

**FEDERAL AVIATION ADMINISTRATION  
INFORMATION TECHNOLOGY STRATEGY  
FISCAL YEARS 2003 – 2005**



**Prepared by Office of the Assistant Administrator for Information Services and CIO  
in association with the FAA's CIO Council**

**September 30, 2002**

## TABLE OF CONTENTS

<b>EXECUTIVE SUMMARY.....</b>	<b>i</b>
<b>1.0 INTRODUCTION.....</b>	<b>1</b>
<b>2.0 INFORMATION TECHNOLOGY STRATEGIC GOALS.....</b>	<b>5</b>
2.1 CYBER-SECURITY.....	5
2.2 ELECTRONIC GOVERNMENT (E-GOVERNMENT).....	7
2.3 BUSINESS VALUE.....	10
<b>3.0 CONCLUSION.....</b>	<b>14</b>
<b>APPENDIX A: FAA STRATEGIC AND PERFORMANCE GOALS.....</b>	<b>16</b>
<b>APPENDIX B: LINKS BETWEEN FAA STRATEGIC AND IT GOALS.....</b>	<b>17</b>
<b>APPENDIX C: TABLE OF FAA IT GOALS, OBJECTIVES, STRATEGIES, AND METRICS.....</b>	<b>18</b>
<b>APPENDIX D: FAA CIO COUNCIL MEMBERS.....</b>	<b>23</b>

## Executive Summary

Information is critical to the operations and mission of the Federal Aviation Administration (FAA) and every function of the agency is dependent upon the use of information technology (IT). Agency spending on information systems now accounts for over \$2.1 billion annually, the largest cost item after FAA personnel salaries and benefits. Recognizing the critical role of IT, the FAA has produced this IT Strategy as a guide in making wise choices in both IT investments and management during fiscal years (FY) 2003-2005. The purpose of this strategy is to align the agency's IT planning, investment decisions, and overall IT programs with its business needs. This strategy updates the earlier FY 2000-2002 Information Technology Strategy produced by the FAA's Chief Information Officer (CIO) in September 1999.

This strategy is intended for the use of the new FAA Administrator and her Management Board, and the anticipated Air Traffic Organization and its oversight board. It will also be useful to the Department of Transportation (DOT), other government agencies, and aviation stakeholders, businesses, and user organizations. Its implementation will be led by the agency's CIO (AIO-1) and by the CIO Council, composed of the senior IT leaders of the agency's major business units. The strategy will be reviewed at least quarterly to set or adjust targets and to evaluate progress towards goals. It will be revisited yearly to identify areas that need update or revision.

The IT Strategy is designed to support high-level Federal Government and FAA strategic goals. It is tied to two key national goals in the President's 2003 Budget: homeland security and economic growth. The IT Strategy is linked to the Administration's E-Government initiative, aimed at enhancing the government's ability to conduct business electronically. The strategy also supports the FAA strategic goals as described in the FAA Strategic Plan and Performance Goals. This IT Strategy is built around the following FAA information technology goals:

### **Cyber-Security: Defend the FAA against cyber-attacks and support national homeland security initiatives with special emphasis on the National Airspace System (NAS)**

International terrorism has become a major threat to U.S. national security. There are also nation states that have cyber capability and are unfriendly to the U.S. The phenomenal growth of the Internet and the worldwide distribution of sophisticated computer skills have created the potential to threaten the critical information infrastructure in the U.S., including the air traffic control system. The FAA has three objectives in this area. The first objective is to ensure effective preparedness, detection, response, and recovery to cyber-attacks. The second objective is to integrate information security efforts into all phases of acquisition and operations to protect FAA people, buildings, and information. The third objective is to support the nation's efforts to safeguard homeland security, in particular this country's aviation infrastructure and industry. Specifically, the FAA will continue to foster information sharing with other Federal agencies, signing memoranda of understanding and Information Security Advisory Council (ISAC) agreements in collaboration with DOT.

### **Electronic Government (E-Government): Improve and expand the electronic delivery of agency services and information to external customers and employees by providing high-quality, easy to find and use, one-stop points of service**

This goal has specific targets for growing the amount of business that the FAA conducts through

electronic means. The main objective under this goal is to provide the capability for external customers and employees to transact business with the FAA electronically. This will be accomplished through continued improvement of service delivery capabilities and development of project portfolios aimed at the key customer groups of citizens, businesses, other government agencies, and employees, as well as projects dedicated to improving internal efficiency and effectiveness. E-Government is also one of the five main goals of the President's Management Agenda and mandates the use of "best IT management practices." These are imbedded into every goal and objective within the IT Strategy. Overall, the strategy will move the FAA to a "green" status on the DOT and Office of Management and Budget (OMB) E-Government scorecards in terms of progress, and ultimately in terms of status.

As part of this goal, the FAA will ensure that data and information that are used to conduct critical agency business, or disseminated outside the agency, are timely, accurate, accessible, understandable, and secure. The FAA, in partnership with the aviation community, depends on vast amounts of information to safely manage air traffic and regulate the aviation industry. The demand for increased collaboration between airspace users and the FAA requires that the agency provide reliable and timely information to its users, partners, and staff.

**Business Value: Obtain maximum value for IT resources (people and dollars) in terms of their contribution to agency goals**

As stated previously, the FAA depends upon, and makes a significant annual investment in, IT services and information systems to achieve its business goals and to perform its many business processes, missions, and functions. The FAA acquires, develops, and operates over 800 IT services and information systems in order to carry out virtually all of its business functions. To accomplish its mission, the agency also employs a large number of IT professionals and contractors in every line of business and staff office. It is critical that the agency obtains the maximum value from its IT resources and looks closely for ways to control major cost drivers. The objectives in this goal are, therefore, to provide the right mix of qualified IT professionals and IT tools for each business need of the agency; to select the right IT investments and manage them for maximum contribution to agency goals, consistent with the agency's Acquisition Management System; to manage large cost and performance drivers such as telecommunications; and to develop and use an enterprise architecture to ensure IT investments are aligned with FAA business needs.

**Next Steps**

The next steps are to develop more detailed implementation plans and strategies, both corporately and within individual business units, for each goal. Targets will be set for each measure and progress will be tracked against targets. Additional resources, both in terms of personnel and funding, will be needed for some of these targets to be met. All business units of the agency, including agency field and regional offices, will participate fully in the implementation of this strategy, and employees and their unions will be consulted and involved in the implementation and impact areas. As part of this process, clear written agreements on targets and resources will be reached with each business unit, and incorporated into the implementation plan. The plan will be reviewed quarterly to track progress and will be revised annually. This strategy has been signed by the CIO, Chief Financial Officer, and the Associate/Assistant Administrators of all the lines of business and staff offices represented on the CIO Council.

## 1.0 Introduction

The Federal Aviation Administration (FAA) has over 800 individual information technology (IT) systems on which it spends over \$2.1 billion annually,<sup>1</sup> around 15 percent of the total agency budget. The FAA's corporate IT challenge is to align that investment with the agency's evolving business needs, strategic objectives, and performance goals. This strategy has been developed to guide the agency during fiscal years (FY) 2003-2005 in establishing and maintaining that alignment.

Because IT enables so much of the FAA's business, the implementation of this strategy will touch most of the agency. The success of the FAA over the FY 2003-2005 time period will largely depend on how well IT supports its major programs and corporate projects, and how well it is used to enable many corporate goals. Because so much of the agency is heavily dependent on information technology, the FAA expects that the majority of the agency's programs and corporate projects will be materially improved by the successful implementation of this IT Strategy.

Much of the IT Strategy is also linked to the Administration's E-Government initiative, which is aimed at enhancing the government's ability to conduct business electronically. It is also directly tied to two key national goals in the President's 2003 Budget message: homeland security and economic growth. Information security is an important part of the nation's homeland security effort in and of itself; it also enhances the effectiveness of a broad range of physical and personnel security initiatives at all levels. A more responsive and efficient FAA will also have an important positive impact on the nation's aviation industry, a critical component of the national economy. Finally, the IT Strategy also supports the FAA strategic goals as described in the FAA Strategic Plan and Performance Goals (see Appendices A and B).

The term "information technology" has been used in a variety of ways within the FAA. Consistent with the Clinger-Cohen Act, this strategy defines *information technology* broadly as:

"... any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency ... The term *information technology* includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources ..."<sup>2</sup>

---

<sup>1</sup> FAA *Information Technology 5-Year Plan*, July 2002

<sup>2</sup> *Information Technology Management Reform Act of 1996* (a.k.a. Clinger-Cohen Act), Section 5002 (2); <http://irm.cit.nih.gov/itmra/itmra96.html>

This IT Strategy responds to the agency's primary business drivers. The drivers most directly affecting IT strategic goals include:

- ***Growing Physical and Information Security Threats.*** The increased threats to physical security and new technologies available worldwide put agency systems and information at ever-higher levels of risk. With the growth of global networks and interconnectivity of critical systems, the agency must be vigilant against intrusions initiated from both local and remote locations.
- ***Growth of the Web and the Mandate for E-Government.*** The growth of agency and agency-sponsored Web sites has spawned a need for standards and corporate strategies, as well as the need to assure that an adequate infrastructure and effective processes will be developed. The Web in turn will enable the rise of E-Government applications, a critical part of the President's management initiatives.
- ***Demand for Better Service from Key Customer Groups.*** Key technologies, such as the Internet, have fueled citizen expectations for services and information. Accordingly, there is a need for the Federal Government to tangibly demonstrate an ability to improve its service and access to the citizen.
- ***Constrained Budgets.*** Like all government agencies in the next decade, the FAA is being asked to do more with less. Aviation traffic is expected to increase more rapidly than is the funding needed to handle that increase by traditional means. Given the funding model under which the agency operates, the FAA cannot increase revenues to match the increased demand for services. In order to meet increased demand with fewer relative resources, the agency must use its resources more wisely. A key opportunity available to the agency is to use IT to increase the effectiveness and efficiency of available resources.
- ***New Technology Opportunities.*** The FAA must leverage new technologies in order to meet its mission goals and industry's demand for more services. Internet Protocol (IP) technologies can be used to create a more efficient, secure, and flexible means to move information around the wide area networks that provide for national air traffic services, aviation safety and certification services, and information exchange among FAA, trusted aviation industry partners, and now the Office (soon to be Department) of Homeland Security. The FAA must respond to these opportunities to keep pace with the needs of its customers.
- ***Replacement of Aging Systems.*** Between FY 2003 and FY 2005, the agency will replace a number of legacy systems. This strategy will help optimize agency investment in new systems by enabling all lines of business to take an agencywide view of their investments.

- ***Aging Workforce.*** The IT workforce, like other workers in the agency, is aging. There is a need to hire new workers and to look at what skills and tasks should be met through commercial sources (a part of the President's Management Agenda). The FAA also must ensure that the federal and non-federal workforce have the necessary training and are certified to do the ever-increasing specialization and complexity of tasks required for effective information management.

This IT Strategy was developed through collaboration among the members of the CIO Council, which consists of the IT leaders in each major business unit of the agency. Their members are listed in Appendix D. The IT Strategy was discussed at the CIO Council-sponsored Information Technology and Security Conference in May 2002, which was attended by more than 130 IT managers and senior staff from both FAA headquarters and field offices.

This IT Strategy will be a living document that will be reviewed at least quarterly to evaluate progress towards goals and targets. It will be revisited yearly to identify areas that need to be updated or revised.

This strategy is intended for the use of the new FAA Administrator and her senior management team, DOT and other government agencies, including the Office of Management and Budget (OMB) and the General Accounting Office (GAO), and various aviation stakeholders and user organizations. It is expected to guide FAA IT investment and management decisions throughout the FY 2003-2005 period.

Before addressing the new strategy, below is a review of some of the major agency IT accomplishments since the FAA FY 2000-2002 IT Strategy was published. These include:

1. The establishment of an effective Information Systems Security Program, with a widely acclaimed intrusion detection function that has successfully protected the agency's IT systems; strong security policies, standards, and processes; the acquisition of enterprise protection and detection tools; the certification of many of the agency's most critical systems software and a large cadre of security professionals; and the protection of the agency's Internet. The Information Systems Security Program is guided by FAA Order 1370.82, which was developed to ensure implementation of the Computer Security Act of 1987; OMB Circular A-130, Management of Federal Information Resources; DOT Handbook, DOT H 1350.2, Departmental Information Resources Management Manual (DIRMM); and Presidential Decision Directive 63. The FAA has also leveraged existing information security research and performed its own research, and conducted agencywide security awareness and training. The result is the recognition across the government and within industry that the FAA is a leading civilian agency in cyber-security.

2. The establishment of an agency Data Management Program<sup>3</sup>, building on the work done within the Air Traffic organizations, including a data management policy<sup>4</sup>, the establishment of standard data elements, the building of a data and system registry, and the increasing awareness throughout the agency, especially following the events of September 11, 2001, of the critical role of data sharing in Federal agencies.
3. The creation of a highly respected process improvement framework, the FAA integrated Capability Maturity Model (FAA-iCMM), and supporting infrastructure. The FAA-iCMM has been used by many FAA organizations and programs to guide improvement of their management and technical processes, with several organizations having been appraised at maturity level 2 for the integrated model, and one organization recently reaching maturity level 3.
4. The establishment within several major business units (Air Traffic Services, Regulation and Certification, and Region and Center Operations) and several major staff offices as well, of strong CIO functions and the alignment of IT standard processes and systems with their business needs.
5. The movement to improve the operations, security, accessibility, and content management of the agency Web site, and begin to position it for effective message delivery as well as to support E-Government.
6. A series of corporate-wide procurements in data management and security, as well as electronic messaging, which reduced costs and enabled easier collaboration among business units.
7. Significant upgrades of hardware and software in regional and field offices and collaboration around telecommunications and central computer support.
8. The awarding of the FAA Telecommunications Infrastructure (FTI), a major telecommunications contract that combines several contracts and positions, for the agency to get the high-quality support it needs for many years to come and to do it with appropriate attention to cyber-security and -privacy.
9. The development of a new process – portfolio management – to allow projects to be aggregated and managed as portfolios of investments focused on critical agency goals, and the recognition of the need to manage risks and keep focus on value throughout the lifecycle.

---

<sup>3</sup> FAA Data Management Strategy dated September 21, 1999

<sup>4</sup> FAA Order 1357.1C, Data Management, dated June 20, 2001.

10. The establishment of a CIO Council which allows for cross agency discussions and decision-making on IT policy, process, investments, and strategy, as well as the organization of a well attended and received IT and security conference in 2002.
11. The completion of 63 Security Certification and Accreditation Packages (SCAPs), with 17 additional under review, in compliance with FAA Order 1370.82 and the FAA ISS Program Handbook.

## **2.0 Information Technology Strategic Goals**

The FY 2003-2005 IT Strategy will focus on three goals: Cyber-Security, E-Government, and Business Value. For each goal, the FAA identified a concise set of high-level objectives, whose accomplishment will constitute the expected progress towards the agency goal. For each objective, the FAA provides several supporting strategies, as well as metrics to be used to measure progress towards achieving the objectives. The goals, objectives, strategies, and metrics are summarized in Appendix C. Further detailed plans and strategies are available for each goal. These are referenced within the strategy and can be found on the FAA CIO's Web site <http://www.faa.gov/aio>, where they will be updated regularly and their progress tracked. The remainder of this strategy will give more details on each goal, objective, and strategy.

### **2.1 Cyber-Security Goal: Defend the FAA against cyber-attacks and support national homeland security initiatives with special emphasis on the National Airspace System (NAS)**

The first objective is to ensure effective preparedness, detection, response, and recovery to cyber-attacks. The second objective is to integrate information security efforts into all phases of acquisition and operations to protect FAA people, buildings, and information. The third objective is to support the nation's efforts to safeguard homeland security, in particular this country's aviation infrastructure and industry.

This FAA IT security goal will directly support national homeland security goals and FAA strategic goals in the security, safety, and people areas. It will also provide indirect support to the FAA global leadership and system efficiency strategic goals.

#### **2.1.1 Ensure effective preparedness, detection, response, and recovery to cyber-attacks**

The first FAA objective under the IT security goal will be to maintain the FAA's position as a leading civilian agency in preparing for, detecting, responding to, and recovering from cyber-attacks. The FAA has established an Office of Information Systems Security (AIS) to lead this effort. The Office of Information Systems Security, in turn, has established a Computer Security

Incident Response Center (CSIRC) to ensure perimeter protections and safeguards are in place to protect the FAA networks against unauthorized modification, disclosure, destruction, and/or denial of service throughout all system lifecycle phases. The CSIRC is widely recognized as a “best practice” among members of the information security community; we will continue to mature this capability. Business units are responsible for information security systems within their organizational borders to include vulnerability discovery, mitigation and intrusion detection, development of system/application life-cycle oversight guidelines, implementing information security systems controls, incident protection/reporting/mitigation and response, configuration management, privacy controls, firewall management, local and remote access virus control, password maintenance/guidance, and general staff awareness/assurance training. We will continue to identify, research, and harmonize emerging security technologies into the information systems security architecture and will develop interoperability standards for such emerging technologies as Public Key Infrastructure (PKI) and biometrics.

The FAA expects to expand its information security systems architecture to harmonize the security requirements of the NAS and administrative architectures. The former was developed several years ago while the latter will be developed in late 2002, but both need to be harmonized as far as their security requirements are concerned. Minimum standards for the information systems security workforce, for recruiting, training, and especially certifying key information systems security personnel, will be pursued. Finally, the agency will leverage FAA information systems security funds by cooperative research with the Department of Defense (DoD) and the National Aeronautical and Space Administration (NASA), influencing their research programs and adapting their research into the FAA, including the CSIRC. The FAA will develop and implement a methodology for continuous, non-invasive monitoring of its information technology and cyber-security assets assuring, in this way, maximum effectiveness in detecting, responding, and recovering from attacks on FAA networks.

The FAA will integrate information, physical, and personnel security into a single methodology aimed at reducing overlaps, avoiding redundancies, and taking advantage of established security practices. Within this methodological framework, the FAA will deploy an information systems security architecture that harmonizes the security needs of the NAS and administrative architectures, reinforcing defense in depth through compartmentalization, redundancy, and hardening of individual systems and network components. These goals, and the associated initiatives, have been outlined in Version 1 of the FAA Information Systems Security Strategic Plan that was published in February 2002. They are consistent with the guidelines contained in The National Strategy to Secure Cyberspace developed by the President's Critical Infrastructure Protection Board as established under Presidential Executive Order 13231 and the revised version of OMB Circular No. A-130 published in August 2002.

### **2.1.2 Integrate information systems security into all phases of acquisition and operation**

The second objective is to integrate information systems security efforts with other agency

efforts to achieve a seamless security posture around facility protection – centered on protecting facilities and the people and systems they house. To accomplish this goal, the FAA will integrate information systems security throughout the FAA’s Acquisition Management System. The agency will also integrate common security requirements into each acquisition through the use of such mechanisms as the FAA NAS Protection Profile Template developed in March 2002 and continue to aggressively probe for vulnerabilities and risks to systems, facilities, and personnel, and then remedy critical shortfalls. Finally, the FAA will certify new facilities and systems prior to opening or deployment and existing key NAS facilities.

### **2.1.3 Position the agency as an effective member of the nation’s homeland defense effort in information systems security**

The third objective is to position the agency as an effective member of the nation's homeland defense effort in information systems security. In support of this objective, the FAA will continue to foster information sharing with other Federal agencies, signing memoranda of understanding and Information Security Advisory Council (ISAC) agreements in collaboration with DOT. As a result of the events that occurred on September 11, 2001, the FAA will most likely be assigned lead agency responsibility to implement an Internet protocol (IP) technology-based routeable surveillance network in the 2003-2006 timeframe.

The FAA will also conduct collaborative research to influence national policy on information systems security through such means as advising the Critical Infrastructure Protection Board and other policy-making bodies. Finally, the agency will implement Continuity of Operations Plans (COOP) for information warfare cooperatively with other elements of the nation’s critical infrastructure.

## **2.2 Electronic Government (E-Government) Goal: Improve and expand the electronic delivery of agency services and information to external customers and employees by providing high-quality, easy to find and use, one-stop points of service**

This goal has specific targets for growing the amount of business that the agency does through electronic means. The main objective under this goal is for the agency to provide the capability for external customers and employees to transact business with the FAA electronically. This will be accomplished through continued improvement of service delivery capabilities and development of portfolios of projects aimed at the key customer groups of citizens, businesses, other government agencies, employees, and internal efficiency and effectiveness. E-Government is also one of the five main goals of the President’s Management Agenda and mandates the use of “Best IT Management Practices.” These are imbedded into every goal and objective within the IT Strategy. Overall, the strategy will move the FAA to a “green” status for E-Government on the DOT and OMB E-Government scorecards.

As part of this goal, the FAA will ensure that data and information used to conduct critical agency business, or disseminated outside the agency, are timely, accurate, accessible, understandable, and secure. The FAA, in partnership with the aviation community, depends on vast amounts of information to safely manage air traffic and to regulate the aviation industry. The dramatic growth in air traffic and increased collaboration between airspace users and the FAA has increased the importance and difficulty of providing reliable and timely information to agency users and staff.

The FAA has defined an objective to distribute data electronically through the use of:

- a. Intranetwide area networks to service data distribution needs of NAS mission critical data in a secure manner (defined in the information systems security architecture at <http://www.faa.gov/aio>);
- b. Extranet wide area networks to share selected business information or operations with trusted suppliers, vendors, partners, customers, or other businesses; and
- c. Internet Web portals.

The FAA has defined specific objectives under the E-Government goal to foster the President's Management Agenda. In addition to responding to the President's Management Agenda item for E-Government, this goal also directly supports the FAA system efficiency strategic and reform goals, and indirectly supports FAA strategic goals in the areas of safety, security, people, and global leadership. Details on the E-Government goal, and its response to the President's Management Agenda, can be found in the E-Government strategy at <http://www.faa.gov/aio>.

### **2.2.1 Ensure effective service delivery capabilities**

The first objective will require that the FAA modernize its Web presence to create an Internet Web site that fully meets the agency's requirements to deliver E-Government services and information. It will also provide a portfolio of automated service/information delivery capabilities aligned with the President's Management Agenda and the DOT E-Government scorecard. This portfolio will be tailored to the different sets of citizens, distinguishing members of the aviation community from the general public. Effective automation of services will require adoption of an e-authentication standard. This strategy recommends adoption of the Federal standard for e-authentication, which also contributes to the collaboration goal of E-Government.

### **2.2.2 Reduce the burden on agency customers by better leveraging Web-based technologies**

The second objective will require implementation of specific initiatives for each key customer group. For citizens, these include automating agency information collections wherever practical to comply with the Government Paperwork Elimination Act (GPEA). The agency will also participate in the development and implementation of the DOT's E-Government initiatives, such as the "recruitment one-stop" portal. For businesses, these include developing collaborative online rule-making and cross-agency integrated acquisitions. For other government agencies, these include collaboration on shared applications, acquisitions through enterprise license agreements, E-Grants, adoption of Geospatial Information System (GIS) data, and data sharing for homeland security. For employees and for the objective of internal efficiency and effectiveness, these include adoption of collaborative toolsets for FAA employees with core capabilities for knowledge management, workflow automation, document management, and program management, all integrated into an employee services portal.

### **2.2.3 Ensure that data and information that are used to conduct critical agency business, or publicly disseminated, are timely, accurate, accessible, understandable, and secure**

The next objective under this goal is to ensure quality data and information. In order to accomplish this objective, the FAA will manage agency data and information using best practices of industry and government; the data and information should meet highest standards of quality, objectivity, utility, integrity, accessibility, and security. The FAA will also establish and use appropriate national and international standards for aviation and other data and information elements that are critical to agency business functions. Additionally, the FAA will register critical agency information systems and metadata, identify official sources, and eliminate redundant data and information sources as appropriate. Furthermore, the agency will develop and implement an infrastructure to store, protect, access, and disseminate its own data and information. A certification process whereby data and information management requirements are integrated into IT systems development will be implemented, and for each critical data and information element, a process that ensures its quality will be institutionalized.

Section 515 of the FY 2001 Treasury and General Government Appropriations Act (Public Law 106-554), more of which can be learned at <http://www.faa.gov/aio>, requires all Federal agencies to ensure and maximize the quality, objectivity, utility, and integrity of publicly disseminated information. This applies to FAA information products and underlying data (including third-party data) that have a clear and substantial impact on important public policies and important private sector decisions. For example, data used as a basis for decisions in the rule-making process or that are published in aviation industry forecasts are required to meet the standards of quality.

The first priority under management reform of the President's Management Agenda (FY 2002) is to make government become citizen-centered. In accordance with the President's agenda and Section 515, this objective includes the establishment of an administrative mechanism to provide the public with the ability to seek and obtain correction of poor-quality information. The FAA will implement a certification process whereby data and information management requirements are integrated into IT systems development. The agency will also put in place processes to quickly respond to public inquiries regarding information quality and take appropriate actions to improve information quality.

### **2.3 Business Value Goal: Obtain maximum value for IT resources (people and dollars) in terms of their contribution to agency goals**

The FAA spends over \$2.1 billion annually on information systems and IT services, which represents the largest cost category in the agency's budget after personnel salaries and benefits. Currently, the FAA is acquiring, developing, and operating over 800 IT services and information systems, which enable the agency to carry out virtually all of its business functions. Four objectives have been identified to meet the goal of obtaining maximum value for IT resources. The first objective in this goal is to provide the right mix of qualified IT professionals and IT tools for each business need of the agency. The second objective is to select the right IT investments (consistent with the agency's Acquisition Management System) and manage them for maximum contribution to agency goals, including the use of business process improvements to ensure maximum efficiencies and effectiveness. The third objective is to manage large cost and performance drivers. The fourth objective is to use enterprise architecture to ensure IT investments are aligned with FAA business needs.

This IT Business Value goal will directly support the FAA strategic goals of system efficiency, reform, and people. It will indirectly support FAA strategic goals in the safety, security, and global leadership areas. More information on this can be found at <http://www.faa.gov/aio>.

#### **2.3.1 Provide the right mix of qualified IT professionals and IT tools for each business need of the agency**

The first objective will focus on finding and closing gaps between IT knowledge, skills, and abilities that are critical to supporting the agency's business. The FAA will determine the appropriate mix of Federal and contractor resources to apply, and begin to position the IT workforce for selection, certification, and training to be equivalent to other key FAA workforce groups (e.g., controllers, technicians, inspectors). Existing and new relationships with educational and certification organizations will be exploited.

The aviation paradigm and IT are changing so rapidly that the FAA must keep its IT workforce and technology current and constantly research and leverage new technologies matched to the critical business needs of the agency. Part of this goal is to provide the right mix of resources for

each business need of the agency and to perform the research necessary to allow the FAA to develop or leverage new information technologies in support of its critical business functions. In particular, the FAA will begin to position the IT workforce to be equivalent to other key FAA workforce groups (e.g., controllers, technicians, inspectors) in terms of selection, training, and certification.

The identification of the correct mix of IT technologies for each part of the workforce will also be critical. The agency will identify, evaluate, and pilot new technologies in support of business needs through the coordinated use of laboratories and other research facilities. The FAA will also develop and evaluate tools, techniques, models and methods that will provide for the automation of design, development, and deployment of complex systems using reusable and common components. Finally, the FAA will leverage Federally-funded advanced technology programs to maximize benefits to IT initiatives.

### **2.3.2 Select the right IT investments and manage them through to value, including the use of business process improvements to obtain maximum efficiencies and effectiveness of these investments**

The second objective, also built around well known best practices for IT management, will be to select the right IT investments (consistent with the agency's Acquisition Management System) with a focus on managing towards value, i.e., achievement of agency goals. The FAA will focus on the industry and government "best practice" of IT capital planning and investment control and incorporate that into agency lifecycle management policies and processes. In particular, the agency will establish a capital planning process for significant information technology investments not currently covered under the acquisition management system process. This will greatly improve the quality of the business cases for each major IT investment.

The FAA will organize IT and other related investments into portfolios and select investments by their contribution towards achieving improvements of corporate metrics, including the planned Air Traffic Organization metrics, while balancing risks. As part of portfolio management and capital planning and investment control, the agency will review investments continuously to manage risks and ensure that benefits are being realized. By leveraging the IT enterprise architecture, the FAA will seek to add value and reduce agency costs by building corporate systems within the agency and across the department, or across multiple government agencies.

The FAA is also working on strategies to allow the Joint Resources Council (JRC), which is the group of agency senior executives charged with oversight of major capital investments, to improve their oversight of capital and lifecycle investments through the use of best practices in portfolio management. One approach is to manage NAS facilities and equipment (F&E) investments as service portfolios, and the other involves managing all major administrative IT investments corporately. To this end, several organizations within the FAA are involved in reinventing the way the JRC identifies portfolios of programs aimed at specific metrics rather

than reviewing stand-alone projects. The FAA's aim is that the JRC will have the tools to ensure that all projects requesting funding will receive consideration with focus on the benefit to the entire NAS and FAA priorities overall.

Another approach to this objective is to extend, align, and evolve process improvement models, methods, and tools (including the FAA-iCMM and ISO-9000) to incorporate best practices and thereby improve the performance of agency information systems. For specific areas, the agency will measure current performance and establish and pursue measurable targets for improvement. Where improvements in business performance can be enabled by process improvement, then the agency will apply best practices such as those embodied in the FAA-iCMM. Here the FAA can build on previous agency successes. The FAA will extend the FAA-iCMM by adding safety engineering and security engineering, and other IT management best practices. The agency will also align iCMM- and ISO-9000-based process improvement efforts to ensure consistency and to minimize duplication of effort. Additionally, the agency will work through the FAA's integrated Process Group to ensure major process improvement efforts are tightly aligned with FAA goals, objectives and performance targets, and with individual business unit business improvement objectives and performance targets. Finally, the FAA will evolve process improvement models, frameworks, methods, and tools through collaboration with the Department of Defense, other government agencies, industry, and academia.

### **2.3.3 Manage large cost and performance drivers**

Another objective is to manage large cost and performance drivers. Acquisition programs that involve a large budget undergo regular acquisition reviews within the FAA. As part of this process, the FAA will plan to develop better models to anticipate changes in IT demand. The agency will then develop strategies to manage large cost and performance drivers within industry cost benchmarks, and incorporate these through service level agreements (SLAs) between business units and service providers to meet that demand effectively. Telecommunications is one of FAA's largest cost drivers, and performance of its network capabilities affects overall system performance. The agency developed the FAA Telecommunications Infrastructure (FTI) Program to anticipate and manage telecommunications needs and ensure the infrastructure can support those needs cost effectively. The FTI support contract was recently awarded and its capabilities are being put in place. FTI will contribute to managing telecommunications demand by allowing its service provider to optimally configure the network as demands evolve. It includes an improved capability to review, verify, and approve invoices for telecommunications services, thereby ensuring that invoices received are correct and paid in a timely manner. The strategy will also result in the ability to compare telecommunications costs to similar industry cost benchmarks, ensuring that the agency will pay fair and reasonable prices, vis-à-vis the private sector and other public sector agencies, for telecommunications services.

#### **2.3.4 Standardize and simplify the enterprise architecture to ensure IT investments are aligned with FAA business processes**

This objective will require the FAA to complete the IT enterprise architecture so that it is consistent with Office of Management and Budget guidance, Federal CIO Council guidance, the DOT enterprise architecture, and the Federal enterprise architecture. The FAA enterprise architecture will document the alignment of IT investments with the business needs of the agency and also show the integration and alignment with the other enterprise architectures being developed at the department and Federal Government level. The enterprise architecture will show the baseline or current architecture, the desired or target architecture, provide a gap analysis, provide a project sequencing plan to close the gap, and establish a standards profile to help drive standardization within the IT infrastructure. The enterprise architecture will be integrated with other existing architectures already defined for the FAA such as the NAS architecture and the information systems security architecture. Once defined and established, the enterprise architecture must be continuously referred to and used by the IT investment analysis process and must be continuously updated as the IT services and systems evolve.

The enterprise architecture will be implemented via a federated model that exploits commonalities within and across major business units. The federated model includes architecture domains or segments for NAS operations, FAA mission support services, and administrative services. In addition the architecture will define and document the NAS and non-NAS shared IT infrastructures that exist. For purposes of the shared IT infrastructure, the agency will divide into four “federations”, each of which will standardize and simplify its IT infrastructure through the use of standards in accordance with the overall enterprise architecture. The largest business units –Air Traffic Services/Research and Acquisitions, Regulation and Certification, and Region and Center Operations– plus a federation of the smaller business units and staff offices will constitute the four federations. The CIO’s office (AIO) will lead the development of standards for the latter federation. The enterprise architecture will document the alignment of the IT services and systems to their respective business processes and will allow the sharing of applications, data, technology, infrastructures, and standards where appropriate. This architecture will reduce the number of IT systems and components maintained by the agency, making their maintenance more efficient and less costly. While certain standards, such as many required for effective cyber-security, E-Government, and data management will necessarily be corporate-wide, the federated model will permit the enterprise architecture to be flexible enough to meet the individual needs of business units. It will also allow us to identify and eliminate redundant administrative systems, and standardize those applications across the entire agency, consistent with the enterprise architecture. Best practices will be incorporated into the architecture by drawing on the lessons learned from business and other government agencies. Again, the intent will be to simplify while maintaining flexibility to meet individual needs.

### 3.0 Conclusion

A common theme in many of the IT objectives discussed above is to focus on critical, selected or targeted information, data bases, positions, etc. Executives from the various lines of business and key staff offices will collectively select the items on which to focus. Leaving the selection open at this time allows the agency to concentrate on those items that will have the greatest impact on the agency's success. The criteria for this selection will be the importance to the agency of achieving individual mission goals, the cost of implementing required changes, and the ability to make improvements while continuing to deliver quality services.

Many of the goals have a strategy that proposes the establishment of a group or team to implement the goal. Where appropriate, existing groups or a combination of existing groups should be leveraged to serve as these implementation teams, rather than creating new teams. It is essential that the members of these implementation teams are at the appropriate level and have the authority to make the necessary decisions for their organization.

The next steps are to develop more detailed implementation plans and strategies, both corporately and within individual business units, for each goal. Targets will be set for each measure and progress will be tracked against targets. Additional resources, both in terms of personnel and funding, will be needed for some of these targets to be met. All business units of the agency, including agency field and regional offices, will participate fully in the implementation of this strategy, and employees and their unions will be consulted and involved in the implementation and impact areas. As part of this process, clear written agreements on targets and resources will be reached with each business unit, and incorporated into the implementation plan.

Teams with agencywide membership have developed the strategies for the security and E-Government goals. The FAA Electronic Government Strategy is nearing completion, and the FAA has implementation plans nearing completion in the FAA Data Management Strategy and the FAA Information Systems Security Remediation Plan, respectively. Meanwhile, the FAA Business Value Plan is under development to provide the strategies to achieve the FAA's business value goals.

The overall responsibility to lead the above efforts lies with the FAA CIO and the CIO Council, who will ensure alignment of the implementation plans with each other and with the FAA mission goals. It is important to note that, although planning will be led by the CIO Council, the implementation of the strategy will be conducted through the appropriate business units; specifically, implementation of portions of the strategy that affect the NAS will be conducted by organizations that manage the NAS. Periodically, the IT Strategy will be revised to respond to insights gained from the implementation teams, changes in the business or technological environment, and to ensure alignment with the FAA mission goals.

The FAA's strategic goals to increase the safety and efficiency of the NAS depend on effective management of the agency's IT resources. The IT Strategy represents the FAA's agencywide approach to IT management and will be used to guide the strategic IT investment decisions and the agencywide management of IT systems and services. The FAA must focus on optimizing decisions across the agency, which will require a culture change. The success of this strategy depends on making that change. Fortunately, there is a strong sense of commitment to that change from the FAA Management Board. That commitment and the willingness of the lines of business to work cooperatively and align funding to meet the strategy's goals, will ensure this strategy's success.

## Appendix A: FAA Strategic and Performance Goals<sup>5</sup>

### FAA Strategic Goals

- I. **Safety:** Reduce fatal aviation accident rates by 80% in ten years (2007)
- II. **Security:** Prevent security incidents in the aviation system
- III. **System Efficiency:** Provide an aerospace transportation system that meets the needs of users and is efficient in applying resources
- IV. **People:** Prepare the workforce for the demands of the 21<sup>st</sup> century
- V. **Reform:** Become more businesslike while increasing customer responsiveness
- VI. **Environment:** Maintain number of people exposed to aircraft noise at current levels
- VI. **Global Leadership:** Improve safety and security of the international aviation system

FAA PERFORMANCE GOALS	FY02 FINAL TARGET	FY03 PROPOSED TARGET	FY04 PROPOSED TARGET	FY05 PROPOSED TARGET	FY06 PROPOSED TARGET	FY07 PROPOSED TARGET
<b>SAFETY – GPRA</b>						
<b>COMMERCIAL AIR CARRIER FATAL ACCIDENT RATE</b> FATAL AVIATION ACCIDENT RATE FOR U.S. COMMERCIAL AIR CARRIERS PER 100,000 DEPARTURES	0.038	0.033	0.028	0.023	0.018	0.010
<b>GENERAL AVIATION FATAL ACCIDENTS</b> NUMBER OF FATAL ACCIDENTS IN A YEAR	379	374	368	362	356	350
<b>SAFETY – SUPPLEMENTAL</b>						
<b>RUNWAY INCURSIONS</b> NUMBER (#) AND RATE OF MOST CRITICAL INCURSIONS (CATEGORY A/B) PER 100,000 OPERATIONS	53# 0.084 RATE	50# 0.076 RATE	47# 0.070 RATE	TBD	TBD	TBD
<b>AIR TRAFFIC OPERATIONAL ERRORS</b> NUMBER OF CATEGORY A & B (HIGHEST SEVERITY) OPERATIONAL ERRORS. (THIS IS A REDUCTION OF 5% FROM THE FIRST FULL YEAR OF DATA COLLECTED, MAY 2001 – APRIL 2002)	N/A	642	TBD	TBD	TBD	TBD
<b>SYSTEM EFFICIENCY – GPRA</b>						
<b>ON-TIME ARRIVAL</b> PERCENT OF AIRCRAFT ARRIVING NO LATER THAN 15 MINUTES AFTER THE SCHEDULED ARRIVAL TIME	77.2%	78.2%	79.2%	TBD	TBD	TBD
<b>NOISE</b> CUMULATIVE NUMBER OF PEOPLE IN RESIDENTIAL COMMUNITIES THAT BENEFIT FROM AIRPORT IMPROVEMENT PROGRAM NOISE COMPATIBILITY PROJECTS (E.G., RESIDENTIAL SOUND INSULATION, RELOCATION OF RESIDENCES)	N/A	12,500	25,000	37,500	50,000	62,500
<b>SYSTEM EFFICIENCY – SUPPLEMENTAL</b>						
<b>AIRPORT CAPACITY LEVEL</b> SUM OF THE FACILITY-SET ARRIVAL RATES IN THOUSANDS ON AN AVERAGE DAY AT THE 35 OEP AIRPORTS	N/A	49.12	TBD	TBD	TBD	TBD
<b>AIRPORT EFFICIENCY RATE</b> PERCENT OF TIME ARRIVAL DEMAND IS SATISFIED AT THE 35 OEP AIRPORTS	N/A	95.49%	TBD	TBD	TBD	TBD
<b>ORGANIZATIONAL EXCELLENCE – INTERNAL</b>						
<b>PRESIDENT'S MANAGEMENT AGENDA – ACHIEVE A "GREEN LIGHT" IN THE FOLLOWING AREAS:</b> <ul style="list-style-type: none"> <li>▪ STRATEGIC MANAGEMENT OF HUMAN CAPITAL</li> <li>▪ COMPETITIVE OUTSOURCING</li> <li>▪ IMPROVING FINANCIAL PERFORMANCE</li> <li>▪ EXPANDED ELECTRONIC GOVERNMENT</li> <li>▪ BUDGET AND PERFORMANCE INTEGRATION</li> </ul>	N/A N/A N/A N/A N/A	YELLOW YELLOW YELLOW YELLOW YELLOW	GREEN GREEN GREEN GREEN GREEN	N/A	N/A	N/A
<b>CUSTOMER SATISFACTION: COMMERCIAL PILOTS</b> COMMERCIAL PILOT SCORE ON THE AMERICAN CUSTOMER SATISFACTION INITIATIVE	60	62	63	TBD	TBD	TBD

<sup>5</sup> FAA Strategic Plan, January 2002

**Appendix B: Links Between FAA Strategic and IT Goals**

	<b>Safety</b>	<b>Security</b>	<b>System Efficiency</b>	<b>People</b>	<b>Reform</b>	<b>Environment</b>	<b>Global Leadership</b>
<b>Cyber-Security:</b> Defend the FAA against cyber attacks and support national homeland security initiatives with special emphasis on the National Security System					N/a	N/a	
<b>E-Government:</b> Improve and expand the electronic delivery of agency services and information to external customers and employees by providing high-quality, easy to find and use, one-stop points of service						N/a	
<b>Business Value:</b> Obtain maximum value for each IT resources (people and dollars) in terms of their contribution to agency goals						N/a	

**Legend:**

**Black – Directly supports**

**Grey – Indirectly supports**

### Appendix C: Table of FAA IT Goals, Objectives, Strategies, and Metrics

Goal	Objectives	Strategies	Measures
<p><b>Cyber-Security:</b> Defend the FAA against cyber-attacks and support national homeland security initiatives with special emphasis on the National Airspace System</p>	<p>Ensure effective preparedness, detection, response, and recovery to cyber-attacks</p>	<ul style="list-style-type: none"> <li>▪ Conduct continuous, non-invasive monitoring of the FAA's cyber-security assets</li> <li>▪ Integrate personnel, physical, and information systems security into a uniform agencywide methodology</li> <li>▪ Continue maturation of Computer Security Incident Response Center (CSIRC) with special emphasis on the National Airspace System (NAS)</li> <li>▪ Deploy standards for security (e.g. biometrics, Public Key Infrastructure, National Information Assurance Certification and Accreditation Process, etc.)</li> <li>▪ Deploy an information system security (ISS) architecture that harmonizes security needs of the NAS and administrative architectures, reinforcing defense in depth through compartmentalization, redundancy, and hardening of individual system and network components</li> <li>▪ Establish minimum standards for the information security system workforce (Federal and contractor), including recruiting, training, and certifying key information systems security personnel</li> <li>▪ Leverage FAA information systems security funds by cooperative research with the Department of Defense and the National Aeronautical and Space Administration, influencing their research programs and adapting their research into the FAA, including the CSIRC</li> </ul>	<ul style="list-style-type: none"> <li>▪ Effectiveness of the FAA in detecting, responding, and recovering to simulated attacks on FAA networks</li> <li>▪ Percent of key existing NAS facilities and systems certified</li> <li>▪ Percent of new systems and facilities certified prior to implementation</li> <li>▪ Degree to which identified information systems security best practices (e.g., SANS Institute Top 20) are uniformly practiced within the FAA</li> <li>▪ Degree to which FAA systems and networks comply with the information systems security architecture</li> <li>▪ Percent of key information systems security personnel that have completed recognized information systems security training</li> </ul>
	<p>Integrate information systems security into all phases of acquisition and operations</p>	<ul style="list-style-type: none"> <li>▪ Integrate NAS security requirements into the Acquisition Management System through a system engineering risk management-based approach</li> <li>▪ Probe for vulnerabilities and risks to systems, facilities, and personnel, and then remedy critical shortfalls</li> </ul>	<ul style="list-style-type: none"> <li>▪ Average age of open vulnerabilities after discovery in legacy systems or after deployment in new systems</li> <li>▪ Percent of new systems that specifically address information systems security requirements at acquisition program baseline</li> </ul>

Goal	Objectives	Strategies	Measures
------	------------	------------	----------

	Position the agency as an effective member of the nation's homeland defense effort in information systems security	<ul style="list-style-type: none"> <li>▪ Continue to foster information sharing with other Federal agencies, especially the new Department of Homeland Security (including the Transportation Security Administration), the White House Office of Cyber Security, the Federal Bureau of Investigations, the National Security Agency, and the Department of Defense</li> <li>▪ Influence national policy on information systems security through such means as advising the Critical Infrastructure Protection Board and other policy-making bodies</li> <li>▪ Implement Continuity of Operations Plans (COOP) for information warfare cooperatively with other elements of the nation's critical infrastructure</li> </ul>	<ul style="list-style-type: none"> <li>▪ Effectiveness of two-way communications with key government agencies in understanding cyber threats and accidents</li> <li>▪ Effectiveness of FAA Continuity of Operations Plans in a simulated attack on FAA networks</li> </ul>
--	--	---	--

<b>Electronic Government (E-Government):</b> Improve and expand the electronic delivery of agency services and information to external customers and employees by providing high-quality, easy to find and use, one-stop points of service	Ensure effective service delivery capabilities	<ul style="list-style-type: none"> <li>▪ Modernize FAA's Web presence to create an Internet Web site that fully meets the agency's requirements to deliver E-Government services and information</li> <li>▪ Provide a portfolio of automated service and information delivery capabilities aligned with the President's Management Agenda and Department of Transportation (DOT) E-Government scorecard; tailor this portfolio to the different sets of customers, distinguishing pilots and other members of the aviation community from the general public</li> <li>▪ Implement the Federal Government standard for e-authentication services for FAA Internet applications</li> </ul>	<ul style="list-style-type: none"> <li>▪ Web site usability as determined by formal external appraisal</li> <li>▪ Percent of agency Web sites that are compliant with agency and overall Federal policies, rules, and regulations</li> <li>▪ Achieving "green" on the Department's E-Government scorecard</li> <li>▪ Percent of automated transactions using e-authentication services</li> </ul>
	Reduce the burden on agency customers by better leveraging Web-based technologies	<ul style="list-style-type: none"> <li>▪ Automate agency information collections and distributions wherever practicable, including compliance with the Government Paperwork Elimination Act by October 2003</li> <li>▪ Participate in development and implementation of DOT's E-Government initiatives, such as "recruitment one-stop"</li> <li>▪ Implement collaborative online rule-making and cross-agency integrated acquisitions</li> <li>▪ Promote collaboration within the FAA, DOT and with other Federal agencies through shared applications (e.g., consolidated human resources and financial systems, International Trade Data System), enterprise license agreements, E-Grants, and Geospatial Information Systems (GIS) data standards</li> </ul>	<ul style="list-style-type: none"> <li>▪ Percent of transactions fully automated</li> <li>▪ Reduction in customer time to perform automated services over their current manual implementation</li> <li>▪ Reduction in agency time and cost to deliver automated services over their current manual implementation</li> <li>▪ Scores on customer satisfaction survey on service quality and</li> </ul>

Goal	Objectives	Strategies	Measures
		<ul style="list-style-type: none"> <li>▪ Share aviation data needed for homeland security with Department of Defense and other elements of critical infrastructure protection</li> <li>▪ Implement a collaborative toolset for FAA employees with core capabilities for knowledge management, workflow automation, document management, and program management</li> <li>▪ Consolidate online tools and information for employees through an employee services portal</li> </ul>	<p>availability</p> <ul style="list-style-type: none"> <li>▪ Number of Federal agencies with which information, applications, or enterprise license agreements are shared</li> </ul>
	<p>Ensure that data, and information that are used to conduct critical agency business, or publicly disseminated, are timely, accurate, accessible, understandable, and secure</p>	<ul style="list-style-type: none"> <li>▪ Manage agency data and information using best practices of industry and government; the data and information should meet highest standards of quality, objectivity, utility, integrity, accessibility, and security</li> <li>▪ Establish and use appropriate national and international standards for aviation and other data and information elements that are critical to agency business functions</li> <li>▪ Register critical agency information systems and metadata, identify official sources, and eliminate redundant data and information sources as appropriate</li> <li>▪ Implement a certification process whereby data and information management requirements are integrated into IT systems development</li> <li>▪ Develop and implement infrastructure to store, protect, access, and disseminate agency data and information</li> <li>▪ For each critical data and information element, institutionalize a process that ensures its quality</li> <li>▪ Respond to public inquiries regarding information quality and take appropriate actions to improve</li> </ul>	<ul style="list-style-type: none"> <li>▪ Percent of critical data and information that meets quality standards</li> <li>▪ Percent of critical data and information for which there is adequate “infrastructure” to maintain quality, including registration, stewardship, and a quality process</li> <li>▪ Number of information quality complaints received and the percent resolved</li> <li>▪ Scores on customer satisfaction survey relating to satisfaction with agency data and information</li> </ul>
<p><b>Business Value:</b> Obtain maximum value for IT resources in terms of their contribution to agency goals</p>	<p>Provide the right mix of qualified IT professionals and IT tools for each business need of the agency</p>	<ul style="list-style-type: none"> <li>▪ Find and close gaps between IT knowledge, skills, and abilities that are critical to supporting the agency’s business; determine the appropriate mix of federal and contractor resources to apply</li> <li>▪ Position the IT workforce (Federal and contractor) for selection, certification, and training to be equivalent to other key FAA workforce groups (e.g., controllers, technicians, inspectors); use existing and new relationships with educational and certification organizations</li> <li>▪ Identify the correct mix of information technologies for each part of the workforce</li> </ul>	<ul style="list-style-type: none"> <li>▪ Number of professional IT certificates held by the workforce in areas deemed critical to the agency, such as security, E-Government (architecture, Web management, IT program management), and related areas</li> <li>▪ Extent to which IT support is aligned with business needs as</li> </ul>

Goal	Objectives	Strategies	Measures
		<ul style="list-style-type: none"> <li>▪ Identify, evaluate, and pilot new technologies in support of business needs through the coordinated use of laboratories and other research facilities</li> <li>▪ Develop and evaluate tools, techniques, models and methods that will provide for the automation of design, development, and deployment of complex systems using reusable and common components for a new FAA standards based architecture being developed for streamlining the NAS</li> <li>▪ Leverage Federally-funded advanced technology programs to maximize benefits to IT initiatives</li> </ul>	<p>prioritized by business units and the FAA as a whole</p>
	<p>Select the right IT investments and manage them through to value, including the use of business process improvements to obtain maximum efficiencies and effectiveness of these investments</p>	<ul style="list-style-type: none"> <li>▪ Establish a capital planning process for significant information technology investments not currently covered under the acquisition management system process</li> <li>▪ Incorporate best practices for IT capital planning and investment control into the agency life-cycle management policies and processes</li> <li>▪ Organize IT and other related investments into portfolios and select investments by their contribution towards achieving improvements of corporate metrics, while balancing risks; review IT investment portfolios continuously to manage risks and ensure that benefits are being realized</li> <li>▪ Ensure major process improvement efforts tightly align with FAA goals, objectives, and performance targets, and with individual business unit business improvement objectives and performance targets through the support of the FAA's integrated Process Group (iPG)</li> <li>▪ Extend, align, and evolve process improvement models, methods, and tools (including FAA-iCMM and ISO-9000) to incorporate best practices and improve performance of IT systems</li> </ul>	<ul style="list-style-type: none"> <li>▪ Percent of capital planning and investment control best practices incorporated into life-cycle management system</li> <li>▪ Percent of major IT investment dollars (those requiring Office of Management and Budget Exhibit 300) managed as either business unit or agency portfolio</li> <li>▪ Percent of major IT investments that are delivering promised value within cost and schedule</li> <li>▪ Percent of IT systems reporting significant improvement in their business performance as a result of process improvement efforts</li> <li>▪ Demonstrated impact on corporate measures of process improvement programs</li> </ul>
	<p>Manage large cost and performance drivers</p>	<ul style="list-style-type: none"> <li>▪ Develop accurate models to anticipate changes in IT demand; develop a strategy to manage large cost and performance drivers within industry cost benchmarks and incorporate through service level agreements between business units and service providers</li> <li>▪ Develop and implement a strategy to anticipate and manage telecommunications needs and ensure the infrastructure can support those needs</li> </ul>	<ul style="list-style-type: none"> <li>▪ Percent deviation of costs from industry benchmarks</li> <li>▪ Percent cost reduction resulting from service level agreements</li> </ul>

Goal	Objectives	Strategies	Measures
	Standardize and simplify the enterprise architecture to ensure IT investments are aligned with FAA business processes	<ul style="list-style-type: none"> <li>▪ Implement a federated model of the enterprise architecture consistent with OMB and DOT guidance; integrate the enterprise architecture into the investment analysis process; exploit commonalities across major business units, sharing components and standards where appropriate; create standard IT infrastructures to support the major business units</li> <li>▪ Reduce operational cost, improve efficiency, and expand functionality by implementing a commercial off-the-shelf (COTS)-based Department-wide Enterprise Resource Planning system based on the financial management system DELPHI and planned human resources system replacements</li> <li>▪ Seek opportunities to collaborate with other government agencies to share IT infrastructure and applications</li> </ul>	<ul style="list-style-type: none"> <li>▪ Extent to which each of the federated architectures are documented in accordance with Office of Management and Budget and DOT requirements</li> <li>▪ Percent of shared components, standards, and infrastructures across multiple applications</li> <li>▪ Percent of IT investments that comply with enterprise architecture</li> <li>▪ Percent of local business unit financial and human resources systems retired because of functionality provided by Enterprise Resource Planning system</li> </ul>

## **Appendix D: FAA CIO Council Members**

**Chair:** Art Pyster, Deputy Assistant Administrator for Information Services and Deputy Chief Information Officer (CIO), AIO-2

### **Council Members:**

Tina Amereihn, Chief Information Officer, Office of the Associate Administrator for Regulation and Certification, AVR-10

Lorraine Berry, Chief Information Officer, Office of the Assistant Administrator for Region and Center Operations, ARC-20

Richard Boe, Director, Information Technology Division, Office of Acquisitions, ASU-500

Mike Brown, Director, Office of Information Systems Security, AIS-1

Mark Bruno, Manager, Information Systems Technology and Services Staff, Office of the Assistant Administrator for Financial Services and CFO, ABA-20

Rick Ford, Chief Information Officer and Manager, ATS Information Services Management Staff, Office of Airway Facilities Service, AAF-60

Rodney Herron, Manager, Information Systems Division, Office of Personnel, AHP-100

Bob Stevens, Program Director, Office of Information Services, Mike Monroney Aeronautical Center, AMI-1

Deborah Swank, Program Analyst, Office of the Chief Counsel, AGC-10

Wes Timmons, Manager, Information Technology and Administrative Services Staff, Office of System Safety, ASY-10

Shelly Yak, Manager, Information Technology Division, William J. Hughes Technical Center, Office of Operations, Technology & Acquisitions, ACX-20

### **Staff to the Council:**

Bob Rovinsky, Program Director, Strategy and Investment Analysis Division, Office of the Assistant Administrator for Information Services and CIO, AIO-100

Tom Fulcher, Program Director, Information Management Division, Office of the Assistant Administrator for Information Services and CIO, AIO-300