

INFORMATION SERVICES/CIO

FEDERAL AVIATION ADMINISTRATION
Fiscal Year 2004 Business Plan



800 Independence Avenue, SW
Washington, DC 20591

www.faa.gov



TABLE OF CONTENTS

INTRODUCTION.....	3
INCREASED SAFETY.....	4
Flight Plan Objective 1: Enhance the safety of FAA’s air traffic systems	6
GREATER CAPACITY	7
Flight Plan Objective 1: Increase airport capacity to meet projected demand	9
INTERNATIONAL LEADERSHIP.....	11
Flight Plan Objective 1: Promote improved safety and regulatory oversight in cooperation with bilateral, regional, and multilateral aviation partners	13
Flight Plan Objective 2: Promote seamless operations around the globe in cooperation with bilateral, regional, and multilateral aviation partners	14
ORGANIZATIONAL EXCELLENCE	15
Flight Plan Objective 1: Make the organization more effective with stronger leadership, increased commitment of individual workers to fulfill organization-wide goals, and a better prepared, better trained, diverse workforce.....	17
Flight Plan Objective 2: Control costs while delivering quality customer service.....	19
Flight Plan Objective 3: Make decisions based on reliable data to improve our overall performance and customer satisfaction	22

INTRODUCTION

The Federal Aviation Administration (FAA) is responsible for providing a safe and efficient national aviation system. Within the FAA, the Assistant Administrator for Information Services and Chief Information Officer (AIO) has the primary responsibility to formulate agency information technology (IT) policy and strategy, to protect agency IT assets from cyber attack, to ensure alignment between IT investment and agency business needs, and to improve agency IT processes.

Information is critical to the operation and mission of the FAA. IT drives the creation, processing, and delivery of that information in every major agency business process. Agency spending on IT accounts for over \$2.5 billion annually, the largest cost item after salaries and benefits. The FAA Flight Plan for 2004-2008 recognizes both the cost and criticality of IT in the Increased Safety, Greater Capacity, International Leadership and Organizational Excellence Goals.

Developed in concert with the agency's Chief Information Officer (CIO) Council and Information Systems Security Managers (ISSMs), AIO's fiscal year (FY) 04 Business Plan directly supports these agency goals. Although the Council and ISSMs generally agree with this plan, they expressed concern about the aggressiveness of the performance targets given FY 04 budget uncertainties. AIO will work with them throughout FY 04 to meet these targets as budgets become final. The objectives, initiatives, and performance targets identified herein, which are to be accomplished by September 30, 2004 unless otherwise noted, reflect not only those of AIO, but also include many IT efforts planned by the various lines of business (LOBs) and staff offices (SOs). It is the combination of actions taken by all LOBs and SOs to improve IT cost and performance that enables increased safety, greater capacity, organizational excellence, and international leadership

INCREASED SAFETY



OVERVIEW

Safety is the FAA's primary mission. It is a responsibility we have to the people of America, and our continued dedication to keeping the skies safe is also the single most important commitment we can make to help revive an economically troubled industry. AIO will contribute to the following Flight Plan objective supporting the goal of Increased Safety:

This Office contributes to the following strategic Safety Objectives outlined in the FAA 2004-2008 Flight Plan:

FLIGHT PLAN OBJECTIVE

1. Enhance the safety of FAA's air traffic systems.

A more detailed description of each Objective, including its supporting Initiatives and Performance Targets follows.

FLIGHT PLAN OBJECTIVE 1: ENHANCE THE SAFETY OF FAA'S AIR TRAFFIC SYSTEMS

The FAA's air traffic control systems include tens of thousands of computer hardware devices, tens of millions of lines of software code, thousands of communications lines and networking elements, and hundreds of human-computer interactions every day for operations and maintenance purposes. The FAA's air traffic control systems are among the most complex systems in the world today, and must be operated, maintained and assured to the highest levels of integrity and availability. They must ensure that the safety of flight is never compromised due to hardware failures, software defects, or intentional or unintentional corruption of data.

FY04 PERFORMANCE TARGETS

- Reduce Operational Error (OE) and Operational Deviation (OD) runway incursions resulting from ATC Controller Actions from a FY 01-03 baseline of 85 to 81.
- Reduce the number of highest severity (Category A & B) operational errors to no more than 629.

Flight Plan Initiative 1. (AIO Leads)

Identify safety and security engineering best practices and integrate these practices throughout the acquisition lifecycle.

AIO Activity

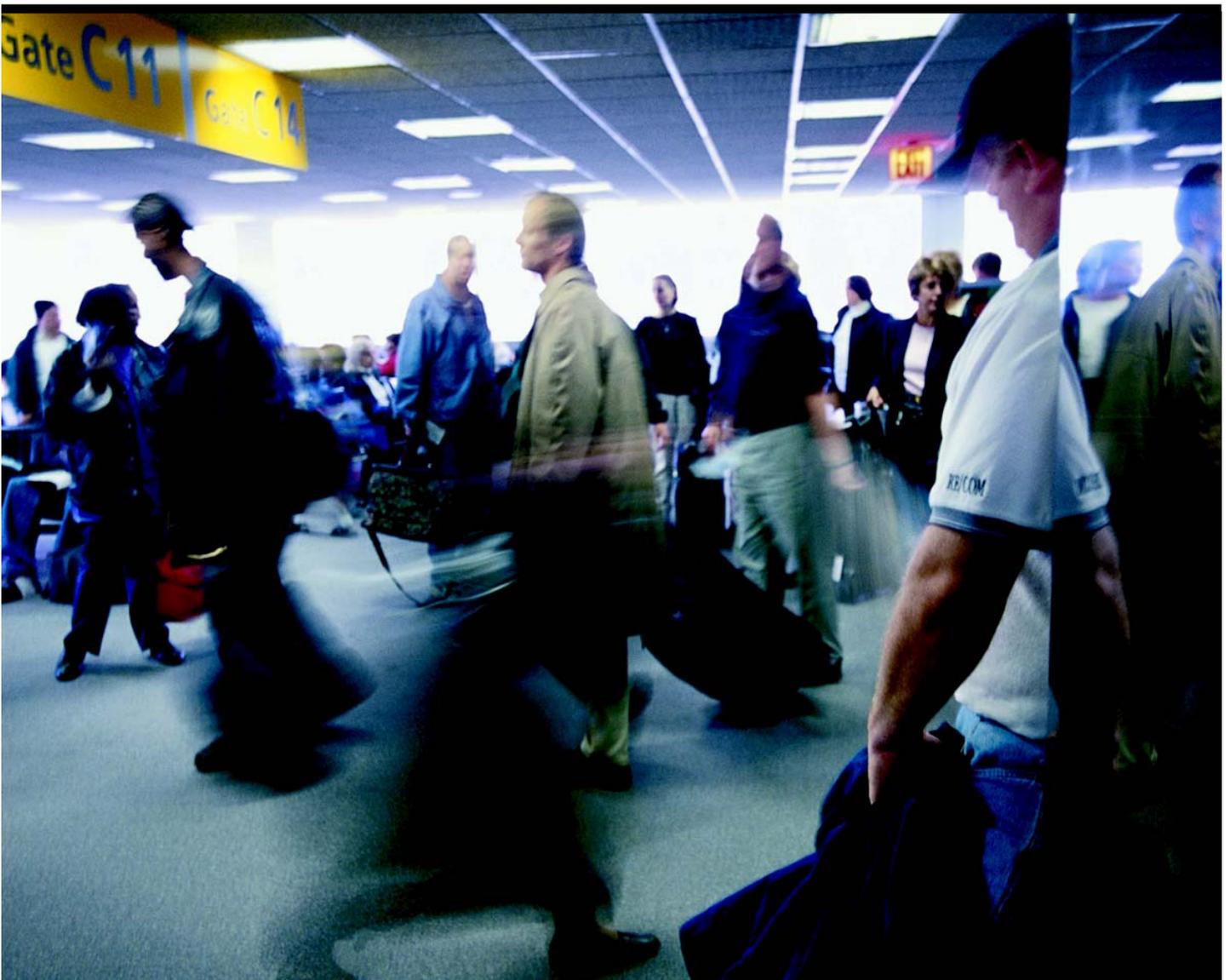
A. The safety of the FAA's air traffic control systems can be maintained and enhanced by continuing to adopt and implement proven best practices throughout the lifecycle of these systems. These best practices include national and international standards and guidelines for systems engineering, software engineering, security engineering and safety engineering. The integration of emerging best practices for security engineering together with long standing best practices for safety engineering is especially critical to ensure that FAA's systems are not compromised by outside threats or that the integrity or availability of systems are not jeopardized as modifications to the NAS are made through such changes as adaptation, adding new software patches to systems, or the dynamic quarantining of systems that are actively under attack. Over this past year, AIO has been carrying-out a joint effort with the Department of Defense (DOD) to identify government and industry best practices for safety engineering and security engineering, and to integrate these best practices within the FAA's

integrated Capability Maturity Model (FAA-iCMM) and DOD's Capability Maturity Model Integrated (CMMI). AIO will identify safety and security engineering best practices and integrate these practices throughout the acquisition lifecycle by:

- Publishing safety and security engineering best practices as extensions to the FAA-iCMM;
- Piloting these best practices on an FAA acquisition program that has significant safety and security requirements; and
- Applying lessons learned from the pilot to develop guidelines applicable to other acquisition programs and add these guidelines to AMS/FAST.

Performance Target: Best practices for safety and security are published as extensions to the FAA-iCMM, by September 2004.

GREATER CAPACITY



OVERVIEW

Air travel will continue to grow only if the aviation system's capacity grows with it. Passengers will seek to travel by air only if they can move through the system safely and efficiently. Increased capacity is the vital link to meeting their demand and realizing the full power and potential of aviation.

This Office contributes to the following strategic Greater Capacity Objectives outlined in the FAA 2004-2008 Flight Plan:

GREATER CAPACITY OBJECTIVE

1. Increase airport capacity to meet projected demand

A more detailed description of each Objective, including its supporting Initiatives and Performance Targets follows.

FLIGHT PLAN OBJECTIVE 1: INCREASE AIRPORT CAPACITY TO MEET PROJECTED DEMAND

Two major aspects of maintaining a high level of operational availability are:

Protecting the air traffic control systems and associated telecommunications from external cybersecurity threats; and

Ensuring that operations and maintenance activities do not themselves affect the target levels of availability.

The agency information systems security (ISS) plan has initiatives that will implement protections and other related assurance activities, such as Security Certification and Authorizations, to ensure that the operational availability of the air traffic control systems is not negatively impacted by cyber threats.

FY04 PERFORMANCE TARGETS

- Achieve an Airport Arrival Efficiency Rate of 95.67% at the 35 OEP airports.
- Achieve an Airport Arrival Capacity at the 35 OEP airports in excess of 51,332 per day.
- Open two new runways, while increasing the annual service volume (ASV) of the 35 OEP airports by at least 1%.
- Sustain Operational Availability at 99% for the reportable facilities that support the 35 OEP airports.

Flight Plan Initiative 1. (AIO Leads)

Identify data and processes that provide greater contribution to sustaining operational availability, and ensure that they are continuously improved and protected.

AIO Activity

A. **Protect, Detect, Respond, And Recover.** Protecting the agency's IT assets requires an aggressive program to protect from, detect, respond to, and recover from cyber-attacks. The agency has been operating such an information systems security program for several years in accordance with numerous executive and legal requirements, including the Computer Security Act, Executive Order 13231, and the Federal Information Security Management Act (FISMA), as well as in accordance with DOT and FAA policy.

The FAA's ISS Program has eight key elements:

- Simplify the enterprise architecture without degrading service

- Harden network elements, defined as both systems and connections
- Protect network boundaries, external as well as internal boundaries between subnetworks
- Quarantine compromised sections of the network in an orderly manner and reconfigure the rest of the network to minimize service impact
- Monitor the network systemically and ensure that controls are adequate
- Recover in an informed manner from network compromises
- Train and educate appropriate personnel
- Leverage cyber research opportunities

During FY 04, the following activities associated with the key program elements are noteworthy (with associated performance targets grouped at the bottom of the activity list):

1. **Simplify:** The agency will complete version 4.0 of the ISS architecture; develop a white paper on the NAS ISS concept of operations; and validate the existing IT system inventory.
2. **Harden:** The agency will publish a new version of the cyber security review handbook that describes much more flexible and lower cost ways to: conduct cyber security reviews; conduct additional cyber security risk reviews at a much greater rate than in previous years, using the guidance from the new handbook; remediate systems by leveraging remediation techniques that address vulnerabilities in many systems at once; and use the Foundscan security product to scan internal network servers for common vulnerabilities and then remediate discovered vulnerabilities as appropriate.
3. **Protect Boundaries:** The agency will begin to deploy intrusion detection systems in significant numbers at key NAS facilities, primarily through the FAA Telecommunications Infrastructure Program, which is replacing the wide area network infrastructure of the NAS.
4. **Systemically (i.e., both locally and globally) Monitor:** AIO operates a Computer Security Incident Response Center (CSIRC), which monitors "vital signs" from intrusion detection and other scanning devices. The volume of data flowing to the CSIRC is expanding significantly as an additional quantity and diversity of monitoring devices are brought online. During FY 04,

the CSIRC will upgrade its ability to “fuse” those myriad data flows in order to provide more concise information to analysts who are constantly assessing whether and where the agency may be under cyber attack. Individual LOBs and SOs will continue to monitor their own network segments and to upgrade their own ability to detect cyber attacks.

5. **Orderly Quarantine:** Even though the agency aggressively defends both its boundaries and its individual network nodes, the potential for a successful attack exists. When an attack is successful, the challenge becomes to limit damage by “quarantining” the compromised part of the network and reconfiguring the rest of the network to minimize service impact. This is a relatively new thrust for the FAA. During FY 04, efforts to develop a near-term concept of operations on quarantining and reconfiguring will begin with a white paper. Exploration of advanced technology to support automated quarantining and reconfiguring began in FY 03 and will continue in FY 04.
6. **Informed Recovery:** If a cyber attack is successful in compromising part of the network, the agency must first quarantine the compromised segment, then repair it, and then return the repaired segment to service. During FY 04, the agency will complete a policy describing how to handle cyber events, including recovery. The LOBs and SOs will begin developing procedures to implement that policy. LOBs and SOs will also test their continuity of operations plan through exercises and drills.
7. **Train and Educate:** All efforts to protect the agency require a well-trained cadre of ISS professionals. During FY 04, the agency will train its ISS workforce consistent with the requirements established in FISMA.
8. **Co-invest in Research Opportunities:** Essential to all activities stated above is advanced technology and research. The rapidly evolving ISS field, combined with limited resources, dictate that the agency work with the National Science Foundation, the Defense Advanced Research Project Agency, or other research-funding Federal agencies to influence and leverage their ISS research direction.

Performance Target: For FY 04, zero cyber events that significantly disable or degrade a NAS service.

By July 1, 2004, complete a security review of 90% of FAA’s NAS IT inventory.

INTERNATIONAL LEADERSHIP



OVERVIEW

The FAA's drive for excellence requires that it broaden its international network of partnerships with civil aviation authorities around the world to promote and enhance safety.

This Office contributes to the following strategic International Leadership Objectives outlined in the FAA 2004-2008 Flight Plan:

INTERNATIONAL LEADERSHIP OBJECTIVE

1. Promote improved safety and regulatory oversight in cooperation with bilateral, regional, and multilateral aviation partners.

A more detailed description of each Objective, including its supporting Initiatives and Performance Targets follows.

FLIGHT PLAN OBJECTIVE 1: PROMOTE IMPROVED SAFETY AND REGULATORY OVERSIGHT IN COOPERATION WITH BILATERAL, REGIONAL, AND MULTILATERAL AVIATION PARTNERS

Standardized data formats and meanings are important to sharing aviation information internationally. AIO participates in the Commercial Aviation Safety Team/International Civil Aviation Organization (CAST/ICAO) Common Taxonomy Team (CTT). The CTT is chartered to establish common terms, definitions, and taxonomies for aviation accident/incident data to enable worldwide coordination and focus on common safety agendas.

Adoption of Eurocontrol's Aeronautical Information Exchange Model (AIXM) will greatly enhance the FAA's ability to exchange information with the airline industry and international civil aviation authorities. Similarly, the "phases of flight" and "weather-related" data element standards represent a core set of mission-critical aeronautical data routinely exchanged with the airline industry and international civil aviation authorities.

FY04 PERFORMANCE TARGETS

- Provide new or expanded technical assistance to six key countries or regional authorities.
- Conclude new bilateral agreements recognizing safety certification/approval systems with two key countries or regional authorities.
- Secure a 20% increase, over FY 03 levels, in intellectual and financial assistance for international aviation activities from the United States and international government organizations, multilateral banks, and industry.
- No new regional aviation authorities or organizations created in FY 04. Activities are occurring to establish regional aviation authorities in FY 05 and beyond.

Performance Target The "phases of flight" and "weather-related" data element standards are approved by the National Airspace System (NAS) Change Control Board, by September 2004

Flight Plan Initiative 1. (AIO Supports)

With the worldwide aerospace community, develop tools and processes for collecting, analyzing, and sharing information and data.

AIO Activity

- A. A key element to sharing information and data is having commonly understood data definitions and formats – normally accomplished by establishing data element standards. The FAA has implemented such a data standardization process. To date, the FAA has 86 approved data element standards that relate principally to make/model/series, and adaptation. Many more are currently under review for approval. AIO's participation in the CTT ensures that the approved FAA data element standards are consistent with standards recommended by CAST/ICAO for international use.

FLIGHT PLAN OBJECTIVE 2: PROMOTE SEAMLESS OPERATIONS AROUND THE GLOBE IN COOPERATION WITH BILATERAL, REGIONAL, AND MULTILATERAL AVIATION PARTNERS

Ensuring the United States, ICAO, and other international partners implement new techniques and key operational procedures in a consistent and timely manner is a target of the FAA Flight Plan, which AIO will support through its extensive effort in information systems security (ISS).

Performance Target: Sign a bilateral agreement with Canada and a separate bilateral agreement with Mexico to share ISS technical and operational data, techniques, tactics, and procedures, and to work cooperatively towards better business practices, by September 2004.

FY04 PERFORMANCE TARGETS

Achieve all milestones in FY 2004 on time.

Flight Plan Initiative 1. (AIO Leads)

Establish bilateral and multinational agreements on ISS with other civil aviation authorities.

AIO Activity

A. Cyber attacks launched in one nation could impact air traffic control operations in other nations. To ensure effective international preparation, detection, response, and recovery from cyber attacks, there must be effective agreements allowing international sharing of technical and operational data. During FY 03, the FAA and NavCanada drafted an agreement to share ISS technology and operational data, techniques, tactics, and procedures, and to work cooperatively towards better ISS business practices.

Also, common global technology standards for biometrics on "smartcards" are essential to ensuring that pilots and other members of the aviation community can use the same credential in different countries, and that aviation information transmitted electronically between nations can be accepted with confidence that it is authentic and has not been modified in transit. Efforts to create needed international technical standards through the International Standards Organization (ISO) are now underway with active participation by AIO, representing the Department of Transportation (DOT) and the United States.

ORGANIZATIONAL EXCELLENCE



OVERVIEW

The FAA's drive for excellence requires that IT be delivered securely and cost effectively while meeting the agency's diverse business requirements.

This Office contributes to the following strategic Organizational Excellence Objectives outlined in the FAA 2004-2008 Flight Plan:

STRATEGIC ORGANIZATIONAL EXCELLENCE OBJECTIVES

1. Make decisions based on reliable data to improve our overall performance and customer satisfaction.
2. Make the organization more effective with stronger leadership, increased commitment of individual workers to fulfill organization-wide goals, and a better prepared, better trained, diverse workforce.
3. Control costs while delivering quality customer service.

A more detailed description of each Objective, including its supporting Initiatives and Performance Targets follows.

FLIGHT PLAN OBJECTIVE 1: MAKE THE ORGANIZATION MORE EFFECTIVE WITH STRONGER LEADERSHIP, INCREASED COMMITMENT OF INDIVIDUAL WORKERS TO FULFILL ORGANIZATION-WIDE GOALS, AND A BETTER PREPARED, BETTER TRAINED, DIVERSE WORKFORCE

The AIO workforce, in conjunction with the IT workforce across the agency, is the key to achieving our targets in support of the FAA mission. We are committed to finding and eliminating barriers to fairness and opportunity in AIO because we realize that the range of diversity directly *relates* to the strength of our office. Furthermore, we will make sure all personnel have the tools and resources they need to address successfully the challenges we face. In turn, employee compensation and salary increases will be performance-based, allowing the agency to control costs and reward success

FY04 PERFORMANCE TARGETS

- Directly relate 80% of all employee performance plans to FAA strategic goals and their organization's performance plans.
- Reduce the time it takes to hire mission critical positions by 3% over FY 03 baseline.

Flight Plan Initiative 1. (AIO Supports)

Implement an executive development program.

AIO Activity

- A. AIO executives will help guide corporate leadership development policies, processes, and programs and will hold their subordinate managers accountable for implementation. They will set an example by personally engaging in ongoing learning activities and will ensure that subordinate managers do likewise. Senior AIO managers and executives will serve as mentors, presenters, and advisors in executive development activities.

Performance Target: TBD through further guidance from AHR.

Flight Plan Initiative 2. (AIO Supports)

Put in place a management workforce planning and development program.

AIO Activity

- A. AIO executives will help guide corporate leadership development policies, processes, and programs and will hold their subordinate managers accountable for implementation. They will set an example by

personally engaging in ongoing learning activities and will ensure that subordinate managers do likewise. Senior AIO managers and executives will serve as mentors, presenters, and advisors in management development activities.

Performance Target: TBD through further guidance from AHR.

Flight Plan Initiative 3. (AIO Supports)

Undertake a timely and effective approach to conflict management.

AIO Activity

- A. Pending guidance regarding specific requirements, we commit to supporting the accomplishment of this corporate initiative.

Performance Target: TBD through further guidance from AHR.

Flight Plan Initiative 4. (AIO Supports)

Directly link all employee performance plans to FAA strategic goals and line of business and staff office performance plans.

AIO Activity

- A. AIO will track the percentage of employees with performance plans in place, and the percentage of performance plans that are directly linked to agency strategic goals and organizational performance plans.

Performance Target: TBD through further guidance from AHR.

Flight Plan Initiative 5. (AIO Supports)

Undertake and sustain agency human capital planning and measurement processes.

AIO Activity

- A. AIO executives will participate on the FAA Human Capital Board to provide oversight for the implementation of the FAA Human Capital Plan and leadership for the strategic management of the agency workforce. They will ensure a corporate and integrated

focus for FAA human capital planning, make corporate human capital investment decisions to meet agency goals, and address alignment of human capital solutions with competitive sourcing and the President's Management Agenda E-Government requirements. AIO will establish and resource a Human Capital Planning Team to develop and implement an office workforce/human capital plan aligned with our business plan, budget process, and the FAA Human Capital Plan. AIO executives and senior managers will communicate the Human Capital Plan goals and actions to our workforce. AIO will establish a Human Capital Planning Council comprised of executives/senior managers to set the strategic business direction, and guide the analysis of our office's workforce requirements.

Performance Target: TBD through further guidance from AHR.

Flight Plan Initiative 6. (AIO Supports)

Put in place a corporate and employee training and development program.

AIO Activity

- A. AIO will participate in the design and development of a corporate employee development program and leverage the existing programs and systems in support of this strategic initiative.

Performance Target: TBD through further guidance from AHR.

Flight Plan Initiative 7. (AIO Supports)

Implement corporate recruitment initiatives.

AIO Activity

- A. AIO will support this recruitment initiative.

Performance Target: TBD through further guidance from AHR.

AIO Initiative 1. (AIO Leads)

Put in place an IT employee training and development program.

AIO Activity

- A. AIO sponsors IT-related training at the Information Resources Management College (IRMC) not only for its own employees but also for other agency IT employees. In addition to individual courses, employees can sign up for one of three certificate programs: CIO, information assurance, and electronic government. AIO also sponsors ISS-related training for ISS personnel, as well as awareness for all computer users across the FAA. Additional training is provided by AIO to integrated product teams and other LOBs in areas such as the integrated Capability Maturity Model, Capital Planning and Investment Control, and Quality Assurance.

There are an increasing number of certifications possible for IT professionals occupying key positions within the agency. OMB strongly encourages program managers to be certified by the Program Management Institute (PMI) or an equivalent organization. The agency must provide the right mix of qualified IT professionals for each FAA business need by certifying IT professionals. The agency should gradually position its IT workforce to have the same caliber of selection, training, and certification as it does for its controller and inspector workforce. During FY 03, the agency certified program managers for programs identified as key by the FAA Acquisition Executive. Over the past three years, the agency has certified over 100 ISS professionals through the Certified Information Systems Security Professional (CISSP) Program. During FY 04, efforts at certifying program managers and ISS Managers will continue.

Performance Target: For FY 04, sponsor 15 employees towards the accomplishment of a CIO, information assurance, or E-Gov certificate from IRMC.

FLIGHT PLAN OBJECTIVE 2: CONTROL COSTS WHILE DELIVERING QUALITY CUSTOMER SERVICE

The FAA spends over \$2.5 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 300 IT services and information systems, which enable the agency to carry out virtually all of its business functions. AIO, together with the other LOBs and SO, is committed to controlling agency costs wherever possible and using resulting savings to fund other agency strategic priorities.

A key element of the agency IT strategy is to use a *federated* approach to infrastructure management. The federated approach explicitly recognizes that some aspects of infrastructure should be managed centrally while others should be reserved to the LOBs and SOs. For example, there is one messaging system for the agency and one standard for Section 508 compliance. The cost and service advantages of uniformity in messaging and Section 508 compliance outweigh the benefits of local choice. Similarly, agreements now being developed among the LOBs and SOs will establish uniform minimum hardware and software requirements for all desktops in the agency. However, each federation member may establish stronger local standards if their business needs dictate.

FY04 PERFORMANCE TARGETS

- Secure 10% of the unfunded portion of the strategic plan through budget requests, reprioritization, and cost savings.
- Complete the closeout of 100% (FY 01 baseline) of cost reimbursable contracts by end of FY 04 and maintain timely closure of future contracts.

Flight Plan Initiative 1. (AIO Supports)

Put in place an agencywide cost control program using Cost Accounting System (CAS) and Labor Distribution Reporting (LDR), including:

1. An executive-level review process;
2. Identification of cross-organizational initiatives focused on controlling operations costs starting with information technology expenditures. Savings identified will be used to fund unfunded aspects of the Flight Plan;
3. A program to create incentives for FAA organizations to identify and implement cost savings initiatives.

AIO Activity

A. *Effective Infrastructure and Federal E-Government Initiatives.* There are many opportunities across the

FAA to ensure the IT infrastructure is more effective while controlling costs. Generally, such opportunities fall into three categories:

1. Simplify the infrastructure,
2. Improve the infrastructure so that the LOBs and SOs can make it easier for citizens and employees to find information and transact business using FAA Internet and Intranet services, and
3. Improve the lifecycle management processes used to acquire IT systems.

Specific activities during FY 04 include: consolidating the IT infrastructure used to deliver Web services; meeting additional requirements of the Government Paperwork Elimination Act (GPEA) as they are established by the Office of Management and Budget (OMB); standardizing additional common data elements; finalizing a standard architecture for the agency Internet access points that are operated by different federation elements; establishing minimum service levels for those access points; bringing more Web sites into compliance with Section 508; developing an agencywide approach to patching servers; providing better separation of employee Web content from public Web content; and prototyping an enterprise "meta-directory" that will eventually enable users to log onto the network only once no matter how many applications they use. AIO will also continue to work with other Joint Resources Council (JRC) members to continuously improve the FAA's acquisition management processes, to include emphasizing greater use of spiral development processes and incremental delivery of new capabilities.

Over the past several years, both OMB and DOT have created a number of cross-agency IT initiatives focused on controlling costs while improving service delivery. Most of these initiatives leverage the Internet and are a cornerstone of the E-government element of the President's Management Agenda. The FAA has participated in several of those initiatives such as *e-grants*, which is producing a common IT system by which citizens can submit grant requests across the Federal Government. During FY 04, the FAA will enhance customer service and control costs by continuing to leverage Federal IT and E-government initiatives. Specific FY 04 initiatives include early use of *e-grants* by the Office of Research and Acquisitions (ARA) to accept research grant proposal and pilot use of *e-invoice*, also by ARA. The latter, based on a system developed elsewhere in DOT, will enable vendors to invoice the FAA electronically. In FY 03, the DOT began replacing its payroll and personnel automation systems with one

developed and operated by the Department of Interior as part of a larger consolidation of such systems across the federal government. By the end of FY 04, the Department of Interior's system will be in use across much of DOT with preparations nearly complete for use within the FAA in FY 05. A DOT system for Enterprise Document Management (EDM) will be started under FAA leadership with early piloting by AIO. EDM will enable users to use a common approach to collaboratively author, process, publish, and archive the many types of documents that drive FAA business. For the next two years, AIO will focus on reducing the cost of operating the more than 5,000 servers that use Administrative Data Transmission Network (ADTN) 2000, with the goal of reducing costs by 5 percent by FY 05.

Performance Target: The costs of operating the FAA's servers that use ADTN 2000 are reduced by 2%, while maintaining current service levels, by September 2004.

Performance Target: 80% of systems that begin development in FY 04, and are substantial enough to require an OMB Exhibit 53, will use existing standardized data elements, where applicable.

- B. *Architectural Simplification and Alignment.* Selecting the right investments in order to control cost and then managing the acquisition and operation of those investments is a significant challenge. Three approaches to proper selection and management include:
1. Share IT services where it offers cost or performance leverage;
 2. Standardize and simplify the FAA's enterprise architecture; and
 3. Link the FAA's enterprise architecture to agency budget and Capital Planning and Investment Control (CPIC) processes.

During FY 04, the FAA will establish three shared services on either a pilot or production basis: (i) pilot shared helpdesk services within one federation member and estimate the savings to be realized if those services become enterprisewide, (ii) implement a secure enterprisewide Blackberry wireless messaging service, and (iii) consolidate local area networks within at least one federation member. Additionally, to standardize and simplify the enterprise architecture, the FAA will: (i) refine the agency's "to be" enterprise architecture, (ii) establish agencywide standards in desktops and security appliances, and (iii) negotiate additional enterprise licenses for IT services and products.

Finally, the FAA will document CPIC processes for all significant IT investments, including linkage with the enterprise architecture.

Total agency IT investment costs, Operations & Maintenance plus Facilities & Equipment, have never been captured. During FY 04, the agency will baseline IT costs to include not only the funding and activities led by AIO, but also IT funding and activities from the other LOBs and SOs. This will allow the agency to see the totality of IT investment and to take steps to optimize the alignment of that investment with business needs.

Performance Target: Agency IT costs baselined, by September 2004.

AIO Initiative 1. AIO Supports

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.

AIO Activity

- A. The FAA has a rigorous process – the Acquisition Management System (AMS) – to select and control NAS investments. In practice, investments to reduce operating costs are not usually selected in the tradeoffs for new features and services. Moreover, the agency has not widely measured promised value during the acquisition and operations phases, and historically has had difficulties meeting schedule and cost baselines. Additionally, AMS has been used only sparingly to manage acquisitions not funded by facilities and equipment sources.

During FY 04, business process improvements will begin to address the shortcomings in the agency's processes for selecting and managing IT investments through to value. We will begin to use Exhibit 300s, which were prepared for all major acquisitions as part of the FY 05 budget submission, as management tools (such as beginning to include them in Joint Resource Council (JRC) and Acquisition Review meetings). We will establish the mechanisms to measure investment value throughout the lifecycle, and develop processes that improve both cost and schedule fidelity for acquisitions and operations, including fielding an automated NAS adaptation system for the Standard Terminal Automation Replacement System and other NAS programs. We will use the CIO Council to help the smooth rollout of corporate administrative IT systems.

During FY 04, AIO will continue to work with a number of programs to realize measurable improvements in their business processes that directly contribute to improved performance and achievement of acquisition cost and schedule baseline targets.

Performance Target: 80% of FY 06 Exhibit 300s receive a '4' or '5' rating by DOT as part of the FY 06 budget submission

FLIGHT PLAN OBJECTIVE 3: MAKE DECISIONS BASED ON RELIABLE DATA TO IMPROVE OUR OVERALL PERFORMANCE AND CUSTOMER SATISFACTION

International terrorism threatens national security. Several nations are capable of launching cyber attacks against the United States. Hackers and criminals are leveraging vulnerabilities exploitable through the Internet at an ever accelerating rate. The FAA, as an important element of the nation's critical infrastructure, is a plausible target for all these threats. AIO has the agency lead for ensuring that cyber attacks are not effective so that the decisionmaking and operational apparatuses of the agency, including the air traffic control system, are never disabled because of a cyber attack.

FY04 PERFORMANCE TARGETS

- Achieve 80% of designated milestones and maintain 80% of critical program costs within 10% of the total as published in the Capital Improvement Plan.
- Achieve 90% of all performance targets in the Flight Plan. Achieve 30 or more of the 33 performance targets in FY 2004.
- Increase customer satisfaction scores on the American Customer Satisfaction Index to 63.
- Achieve 90% of the FY 04 milestones for the agency information security plan.

Flight Plan Initiative 1. (AIO Leads)

Update and implement an agency security plan to protect our information assets.

AIO Activity

A. *Protect, Detect, Respond, And Recover.* Protecting the agency's IT assets requires an aggressive program to protect from, detect, respond to, and recover from cyber-attacks. The agency has been operating such an information systems security program for several years in accordance with numerous executive and legal requirements, including the Computer Security Act, Executive Order 13231, and the Federal Information Security Management Act (FISMA), as well as in accordance with DOT and FAA policy.

The FAA's ISS Program has eight key elements:

- Simplify the enterprise architecture without degrading service
- Harden network elements, defined as both systems and connections
- Protect network boundaries

- Quarantine compromised sections of the network in an orderly manner and reconfigure the rest of the network to minimize service impact
- Monitor the network systemically and ensure that controls are adequate
- Recover in an informed manner from network compromises
- Train and educate appropriate personnel
- Leverage cyber research opportunities

During FY 04, the following activities associated with the key program elements are noteworthy (with associated performance targets grouped at the bottom of the activity list):

1. ***Simplify:*** The agency will complete version 4.0 of the ISS architecture; develop a white paper on the NAS ISS concept of operations; complete a secure wireless network standard which will be the basis for establishing either federationwide or enterprisewide wireless solutions in FY 05 and FY 06; and validate the existing IT system inventory.
2. ***Harden:*** The agency will publish a new version of the cyber security review handbook that describes much more flexible and lower cost ways to: conduct cyber security reviews; conduct additional cyber security risk reviews at a much greater rate than in previous years, using the guidance from the new handbook; remediate systems by leveraging remediation techniques that address vulnerabilities in many systems at once; and use the Foundscan security product to scan internal network servers for common vulnerabilities and then remediate discovered vulnerabilities as appropriate.
3. ***Protect Boundaries:*** The agency will begin to deploy intrusion detection systems in significant numbers at key NAS facilities, primarily through the FAA Telecommunications Infrastructure Program, which is replacing the wide area network infrastructure of the NAS. The FAA will also begin to deploy technology to protect Public Branch Exchange facilities that enable dial-up access to FAA administrative networks.
4. ***Systemically (i.e., both locally and globally) Monitor:*** AIO operates a Computer Security Incident Response Center (CSIRC), which monitors "vital signs" from intrusion detection and other scanning devices. The

volume of data flowing to the CSIRC is expanding significantly as an additional quantity and diversity of monitoring devices are brought online. During FY 04, the CSIRC will upgrade its ability to “fuse” those myriad data flows in order to provide more concise information to analysts who are constantly assessing whether and where the agency may be under cyber attack. Individual LOBs and SOs will continue to monitor their own network segments and to upgrade their own ability to detect cyber attacks. The agency will also pilot advanced technology to uncover postings on the agency Web site that are not individually sensitive, but collectively are security sensitive.

5. **Orderly Quarantine:** Even though the agency aggressively defends both its boundaries and its individual network nodes, the potential for a successful attack exists. For example, over the years several Web sites have been defaced and several worms and viruses have impacted e-mail delivery. When an attack is successful, the challenge becomes to limit damage by “quarantining” the compromised part of the network and reconfiguring the rest of the network to minimize service impact. In the past, those quarantines and reconfigurations have been effective, but they did not rely on a well-defined concept of operations. During FY 04, efforts to develop a near-term concept of operations on quarantining and reconfiguring will begin with a white paper. Exploration of advanced technology to support automated quarantining and reconfiguring began in FY 03 and will continue in FY 04.
6. **Informed Recovery:** If a cyber attack is successful in compromising part of the network, the agency must first quarantine the compromised segment, then repair it, and then return the repaired segment to service. During FY 04, the agency will complete a policy describing how to handle cyber events, including recovery. The LOBs and SOs will begin developing procedures to implement that policy. LOBs and SOs will also test their continuity of operations plan through exercises and drills.
7. **Train and Educate:** All efforts to protect the agency require a well-trained cadre of ISS professionals. During FY 04, the agency will train its ISS workforce consistent with the requirements established in FISMA.

8. **Co-invest in Research Opportunities:** Essential to all activities stated above is advanced technology and research. The rapidly evolving ISS field, combined with limited resources, dictate that the agency work with the National Science Foundation, the Defense Advanced Research Project Agency, or other research-funding Federal agencies to influence and leverage their ISS research direction.
- C. **Institutionalize.** Institutionalizing ISS into all phases of acquisitions and operations will reduce the number of vulnerabilities built into systems and minimize the impact those vulnerabilities have on operations. During FY 03, an effort began to develop an allocation of security requirements from the ISS architecture down to each of the integrated product teams responsible for acquiring NAS systems. That effort will be completed during FY 04 in conjunction with a process to ensure that those requirements are understood and acted upon. Additionally, work will continue on an advanced tool to help acquisition programs estimate the cost of implementing ISS requirements and AIO will publish a set of guidelines on how to perform security engineering during development.

All activities above are covered by the following performance targets:

Performance Target: For FY 04, zero cyber events that significantly disable or degrade an externally-visible FAA service.

Performance Target: By July 1, 2004, complete a security review of 90% of FAA’s IT inventory.

Performance Target: On September 30, 2004, there is an average of no more than 0.05 “high” vulnerabilities per network server that is scanned by the Foundscan tool.

Performance Target: By September 2004, co-invest in three cyber-related research projects, in universities and other institutions, with the National Science Foundation, the Defense Advanced Research Project Agency, or other research-funding Federal agencies.