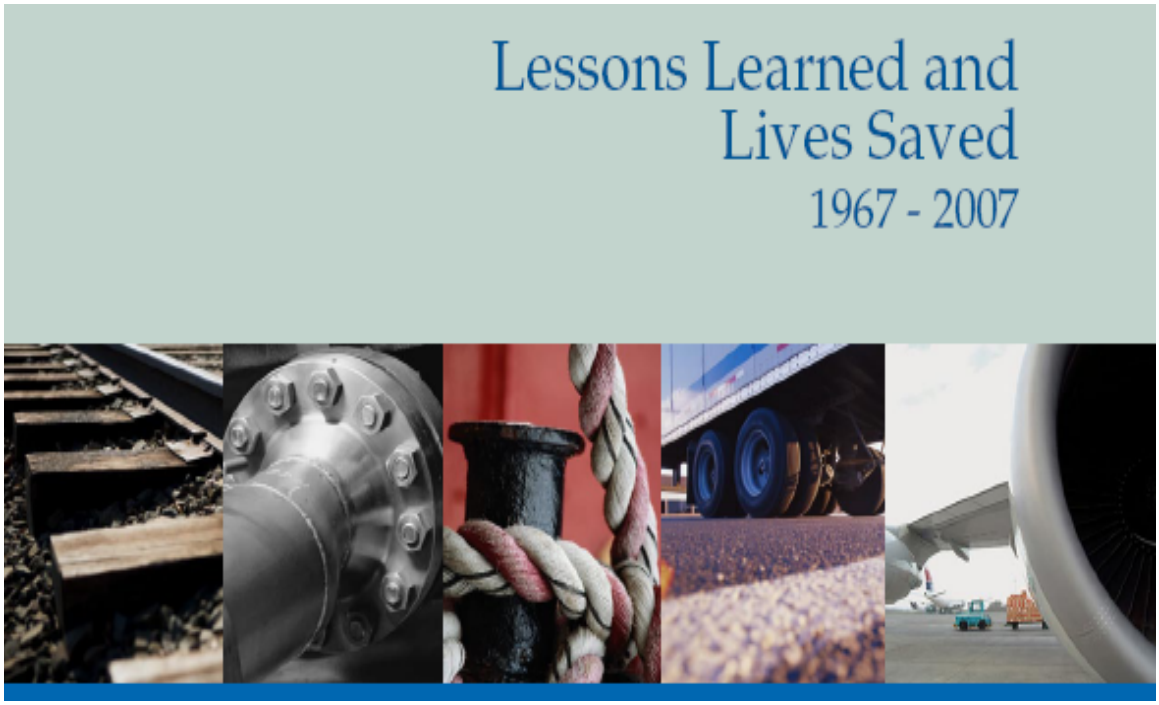


INFORMATION TECHNOLOGY STRATEGIC PLAN FY 2007 – FY 2012

A Key Component in Achieving NTSB's Mission

August 2007

Table of Contents

CIO's Message: Bob Scherer, Chief Information Officer

As a partner in achieving NTSB mission success, I am committed to efficiently and effectively deploying and managing Information Technology (IT) assets and investments while ensuring interoperability and security in a robust IT environment.

Information Technology will continue to become a more important *component* in achieving success in support of the National Transportation Safety Board's Mission:

to promote transportation safety by

- maintaining our congressionally mandated independence and objectivity;
- conducting objective, precise accident investigations and safety studies;
- performing fair and objective airman and mariner certification appeals; and
- advocating and promoting NTSB safety recommendations. And

to assist victims of transportation accidents and their families.

Our IT Strategic Goals are aligned with the Safety Board's Mission to maximize the innovative and effective use of technology. Emerging information technologies continue to create new challenges and opportunities for improving service to our customers while reducing costs.

This year, the Office of the Chief Information Officer (OCIO) worked to establish a foundation for improving the delivery of IT products and services at the National Transportation Safety Board (NTSB). One component of that foundation is the development of the first IT Strategic Plan at the Safety Board. In an effort to establish a solid foundation, I chose to not start from scratch but rather to adopt a best practice model from one of the premier IT operations in the Federal Government, the Department of the Interior.

I believe that an effective way to measure the performance of an IT organization, or any organization, is to apply a series of maturity models. Ultimately, the success of an IT organization relies upon its people, its processes, and its technology. As a result I am fully committed to effectively utilizing process maturity models to achieve and measure results; enhancing IT Security to protect our systems against future vulnerabilities and threats; and preparing our IT workforce for future requirements. To achieve an IT organization that fully supports the Safety Board, the OCIO has established seven IT Strategic Goals and corresponding Focus Areas: ***Enterprise Architecture, IT Security, E-Government, IT Capital Planning & Investment Control (CPIC), IT Infrastructure, Information and Records Management, and IT Workforce Management***.

Each employee in the OCIO should see at least one item, if not multiple items that highlights their contribution to support the office and the Safety Board as a whole.

Executive Summary

The National Transportation Safety Board's Information Technology Strategic Plan provides a specific course of action for effectively managing the Information Technology (IT) Program in support of the Safety Board's overall Mission. NTSB's IT strategy guides IT resources to align with the business goals and establishes specific IT Strategic Goals with Focus Areas and performance measures. This document is our roadmap to achieve targeted RESULTS in providing reliable services, meeting customer expectations, and creating savings.

In order to meet the current and future needs of customers, stakeholders, and employees; the Safety Board's exchange and management of information must be based on strategic plans that will improve our capacity for delivering mission results. As a key component in achieving the Safety Board's mission success, the IT structure must be based on strategic plans that incorporate the concepts of electronic government and modern IT enterprise architecture.

The Safety Board's emerging governance framework will embrace the distinct modal needs and strengths, and serves as the foundation for the Board's IT strategy. Our modal and support offices serve as leaders for a variety of NTSB initiatives, as well as recognized leaders in their specific fields of endeavor. The goal is to establish and mature an overall framework for integrating business needs and IT. This framework will facilitate cooperation and improve data sharing capabilities within and across modal lines and with the Safety Board's customers and stakeholders.

The Office of the Chief Information Officer has identified seven IT Strategic Goals to maximize the innovative and effective use of technology during the migration of its IT portfolio to integrated, agency-wide business processes and technologies.

NTSB IT Strategic Goals

Enterprise Architecture (EA): Leverage EA to improve NTSB's mission performance and realize its strategic goals and objectives. *(maps to NTSB Strategic Goal #3 – Outstanding Stewardship of Resources and Strategic Goal #4 – Organizational Excellence)*

IT Security: Protect the availability, confidentiality, and integrity of NTSB's IT resources. *(maps to NTSB Strategic Goal #3 – Outstanding Stewardship of Resources)*

E-Government: Improve the efficiency and effectiveness of NTSB business processes. *(maps to NTSB Strategic Goal #3 – Outstanding Stewardship of Resources and Strategic Goal #4 – Organizational Excellence)*

IT Capital Planning & Investment Control (CPIC): Improve the planning, execution, and management of IT investments. *(maps to NTSB Strategic Goal #3 – Outstanding Stewardship of Resources)*

IT Infrastructure: Provide enterprise solutions—improving the quality, accessibility, and information sharing capabilities between NTSB and its customers. *(maps to NTSB Strategic Goal #3 – Outstanding Stewardship of Resources)*

Information and Records Management: Create an effective knowledge-sharing environment while meeting information management standards and requirements. *(maps to NTSB Strategic Goal #3 – Outstanding Stewardship of Resources and Strategic Goal #4 – Organizational Excellence)*

IT Workforce Management: Ensure the availability of IT human capital capable of meeting the goals and NTSB mission challenges. *(maps to NTSB Strategic Goal #4 – Organizational Excellence)*

A corresponding Focus Area for each IT Strategic Goal has been identified to measure progress. Our strategy establishes the usage of process maturity models including those of the Government Accountability Office (GAO), Office of Management and Budget (OMB), National Institute of Standards and Technology (NIST), and the Federal CIO Council. The long-term goals and performance measures maintain our focus on the bottom line – specific results that we must achieve to be successful in accomplishing our IT Mission.

Intensive efforts have been underway to standardize IT functions and organizations throughout the Federal Government. These efforts will continue and impact NTSB to varying degrees in the coming years. Further standardization along business lines will enable NTSB to accrue costs savings. When opportunities that make business sense arise NTSB will move to take advantage of Lines of Business solutions.

The OCIO will continue to implement business and IT initiatives while upgrading information technologies, improving security, and bringing better connections to personnel in the field. We will establish policies that create consistent practices; and develop teams, tactics, and tools to cut cycle time, reduce friction, and improve communication. At the same time, we will work to spread best business practices across the Safety Board. These collective approaches will improve performance, reduce inefficiency and duplication, and provide the support needed to achieve our Mission.

Section 1: Introduction

This section introduces key factors that impacted the formation of the Safety Board's IT Strategic Plan. This document is designed to support the Safety Board's overall strategic mission, vision, goals and targeted outcomes previously defined by the Safety Board. The key factors are being presented prior to the Safety Board's IT Strategic Goals and Focus Areas.

Purpose

The National Transportation Safety Board is embarking on a more structured, goal and results oriented planning process both from a strategic and operational planning perspective. A component of this overall effort is the development of an IT Strategic Plan. The Information Technology Strategic Plan builds upon and aligns with the National Transportation Safety Board's FY2007 – FY2012 Strategic Plan. The IT Strategic Plan serves as a catalyst to drive toward the implementation of agency-wide business process and technology improvement efforts and is intended to strengthen the Safety Board's capacity and success in delivering Mission results.

Scope

This IT Strategic Plan provides a specific course of action for integrating the Safety Board's IT strategic planning process with the Board's Strategic Plan for Fiscal Years 2007 through 2012.

The IT Strategic Plan is designed to support the Safety Board's strategic mission and management goals. This plan aligns IT with the Safety Board's major program concerns. The IT Strategic Goals, and Focus Areas are tied *to Enterprise Architecture, IT Security, E-Government, IT Capital Planning & Investment Control (CPIC), IT Infrastructure, Information and Records Management, and IT Workforce Management.*

IT Challenges

There are many challenges that the Safety Board will continue to encounter including new IT mandates, funding, and limited human resources. Simultaneously, there are rising challenges for enhanced security and safety in support of Homeland Security initiatives; rapid changes in technology; retirement of the "baby boomer" generations and its impact to the IT Workforce; as well as increased expectations of stakeholders for innovative and faster IT service applications.

The Safety Board recognizes that making smart investments, integrating architectures, ensuring secure IT environments, and providing an adequate IT workforce are vital to overcoming these challenges and fulfilling its Strategic Plan. The Safety Board must leverage IT resources through enterprise solutions and increased partnerships, in fulfilling its ultimate commitment of improving IT performance and guaranteeing efficient and effective customer-oriented business operations. Continuous evaluation of process and technology improvement is incorporated into this IT Strategic Plan in order for the Safety Board to meet its four Strategic Goals.

Legislation and Presidential Directives

The Safety Board recognizes the need to adapt to changes mandated by the Administration and Congress and has developed an IT strategy to address legislation and presidential orders that include the items identified below. ***Note: Legislation and Presidential Directives are accessible via: http://www.whitehouse.gov/omb/.***

- FY 2002 President's Management Agenda (PMA)
- E-Government Act of 2002
- Federal Information Security Management Act (FISMA) of 2002
- OMB's Federal Enterprise Architecture Program
- IT Management Reform Act of 1996 (ITMRA) or Clinger-Cohen Act
- Federal Acquisition Reform Act of 1996 (FARA)
- Government Paperwork Elimination Act 1998 (GPEA)
- Government Management Reform Act of 1994 (GMRA)
- Federal Acquisition Streamlining Act of 1994 (FASA)
- Paperwork Reduction Act of 1995 (PRA)
- Presidential Decision Directive 63 (PDD-63)
- Government Performance and Results Act of 1993 (GPRA)
- Chief Financial Officers Act of 1990 (CFO Act)
- Privacy Act of 1974
- The Freedom of Information Act (FOIA)
- The Federal Records Act (FRA)
- Federal Financial Management Improvement Act (FFMFIA)
- Section 508, Rehabilitation Act of 1998 (29 U.S.C. 794d)
- Rehabilitation Act Amendments (Section 508)
- OMB Circulars:
  - A-11 Preparation, Submission and Execution of the Budget
  - A-130: Management of Federal Information Resources
  - A-16: Coordination of Geographic Information and Related Spatial Data Activities
  - A-76: "Performance of Commercial Activities.
- Homeland Security Presidential Directive (HSPD-12)

OMB M-06-02: **Improving Public Access to and Dissemination of Government Information Using the Federal Enterprise Architecture (FEA) Data Reference**

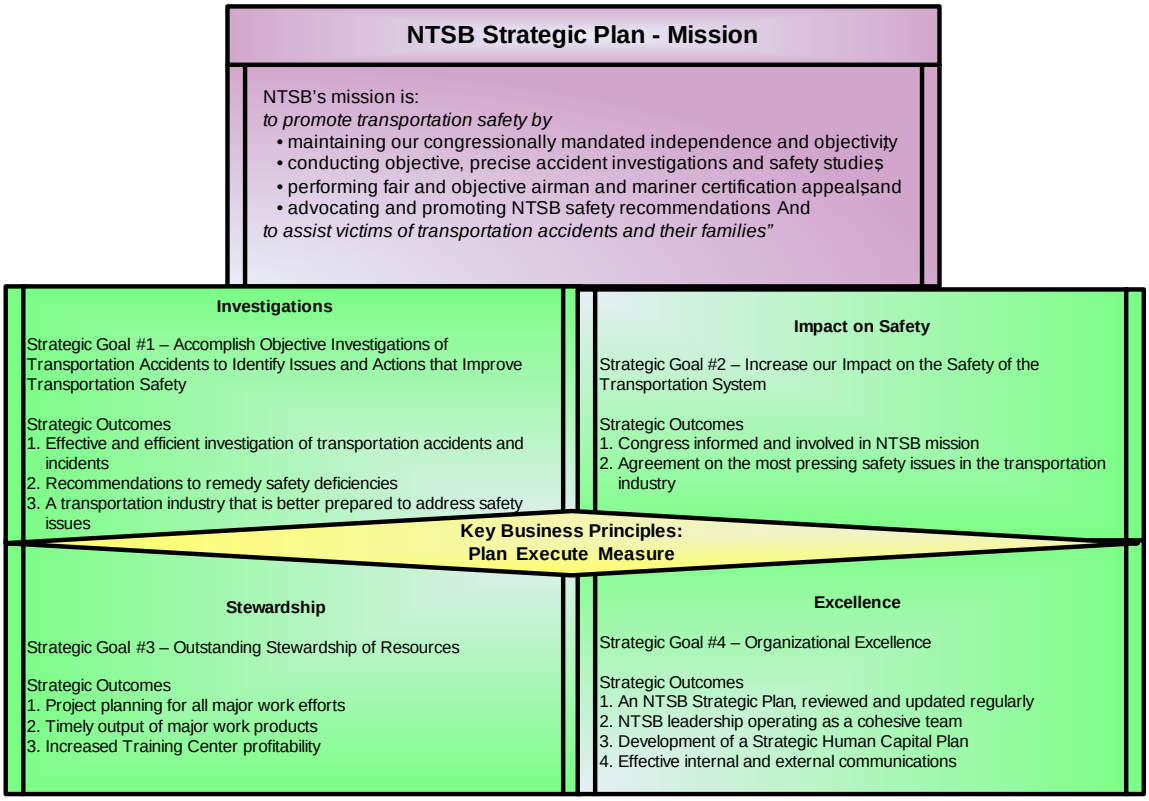
On December 16, 2005, the Office of Management and Budget released *OMB M-06-02* : *Improving Public Access to and Dissemination of Government Information Using the FEA Data Reference Model*. The guidance states that "cost-effective and consistent access to and dissemination of government information is essential to promote a more citizen-centered government." The memorandum identifies procedures to organize and categorize information and make it searchable across agencies to improve public access and dissemination, and discusses using the Federal Enterprise Architecture Data Reference Model (DRM). Agencies must continue to review the performance and results of their information dissemination program.

Appendix A provides the Safety Board's description of its models to assist in dissemination activities and the review process in compliance with OMB M-06-02 requirements.

Section 2: Strategic Framework

This section presents an overview of the high level linkages between the National Transportation Safety Board's FY 2007 – 2012 Strategic Plan and the Board's IT Strategic Plan FY 2007 – 2012

NTSB Strategic Plan 2007-2012 Framework



NTSB IT Strategic Plan FY 2007 -2012: IT Mission, Vision, and IT Strategic Principles

IT Mission*: *To enable the execution of the NTSB safety mission by providing information technology services that support and improve key work processes.

IT Vision*: *The vision of the Office of the Chief Information Officer is to apply a best practice, integrated approach to providing technology products and services in support of NTSB's mission and customers.

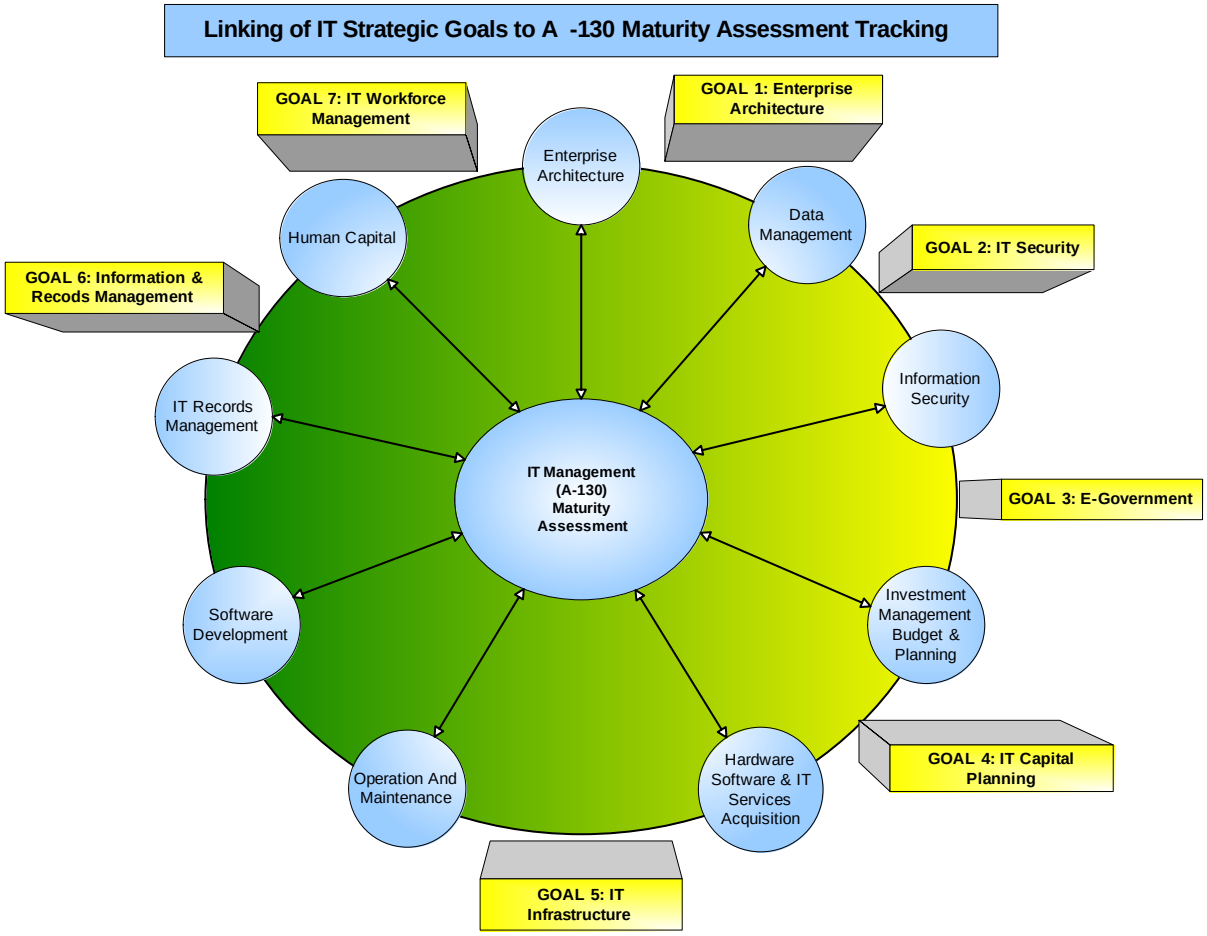
IT Strategic Principles

The following Strategic Principles provide the framework for delivering our IT Mission

- ***Alignment**: The Safety Board*'s strategic mission and management goals will be supported by aligning IT with major program areas.
- ***Enterprise Approach**:* To maximize effective use of technology, the Safety Board will migrate to integrated, agency-wide business processes and technologies.
- ***Teamwork**:* Offices will serve as partners for a variety of IT initiatives. This approach fosters shared ownership, embraces diversity, leverages strengths and is consistent with best practices.
- ***Process Maturity**:* Continuous improvement in IT processes will be achieved by following appropriate published process maturity models.
- ***Measurable**:* Achievement of strategic goals will be measurable and reported regularly.
- ***Support for Mandates**:* IT strategic goals will address legislative, regulatory and administrative mandates such as FISMA, OMB A-130, HSPD-12, etc.

IT Strategic Goals

The Safety Board's IT Strategic Goals directly link to the goals indicated in *OMB's A-130 Maturity Assessment Tracking* guide to provide for more effective management for the achievement of the vision. The diagram below illustrates how these goals map to process areas defined by OMB Circular A-130.



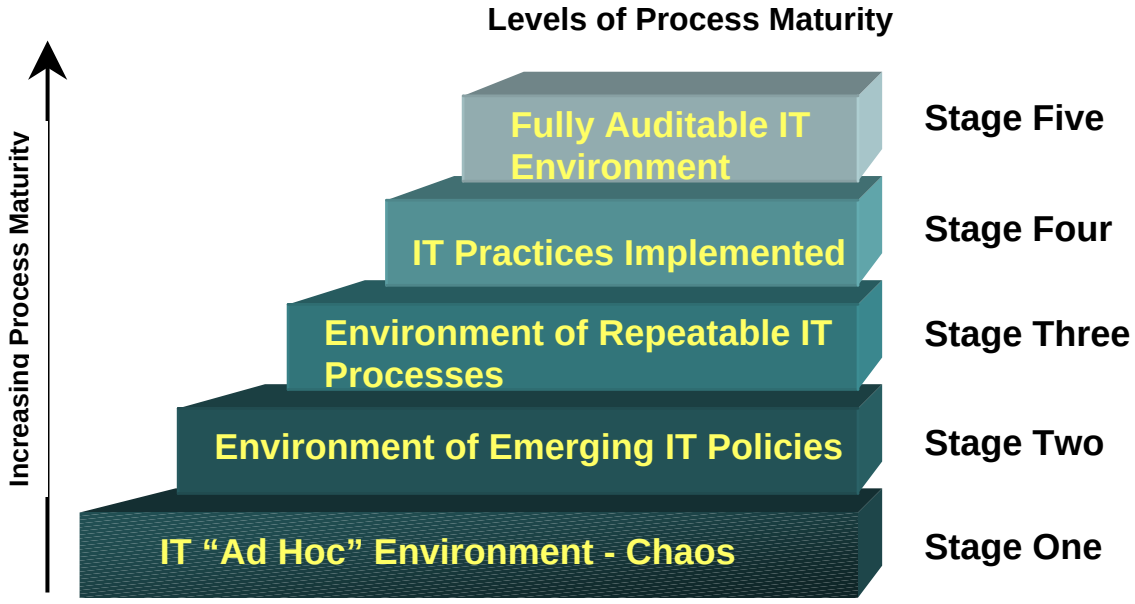
Section 3: Using Process Maturity Models for Managing Results

This section provides a framework for identifying best practices, and measuring progress in achieving IT strategic goals. Process models typically define five stages of maturity with attributes as illustrated below. A Process Maturity Model is provided for each IT Strategic Goal and its Focus Area.

Process Maturity Models

Progress in achieving IT Strategic Goals will be measured using a process maturity model that is specific to meeting the requirements of that goal. The Capability Maturity Model (CMM) illustrated below describes an evolutionary improvement path from an ad-hoc, immature process to a mature, disciplined process. A comparable model will be used to define specific goals and to measure progress for each IT Strategic Goal. Maturity Models used in this plan are based upon industry, international, or Federal Government models widely used in the IT community.

Capability Maturity Model (CMM)*

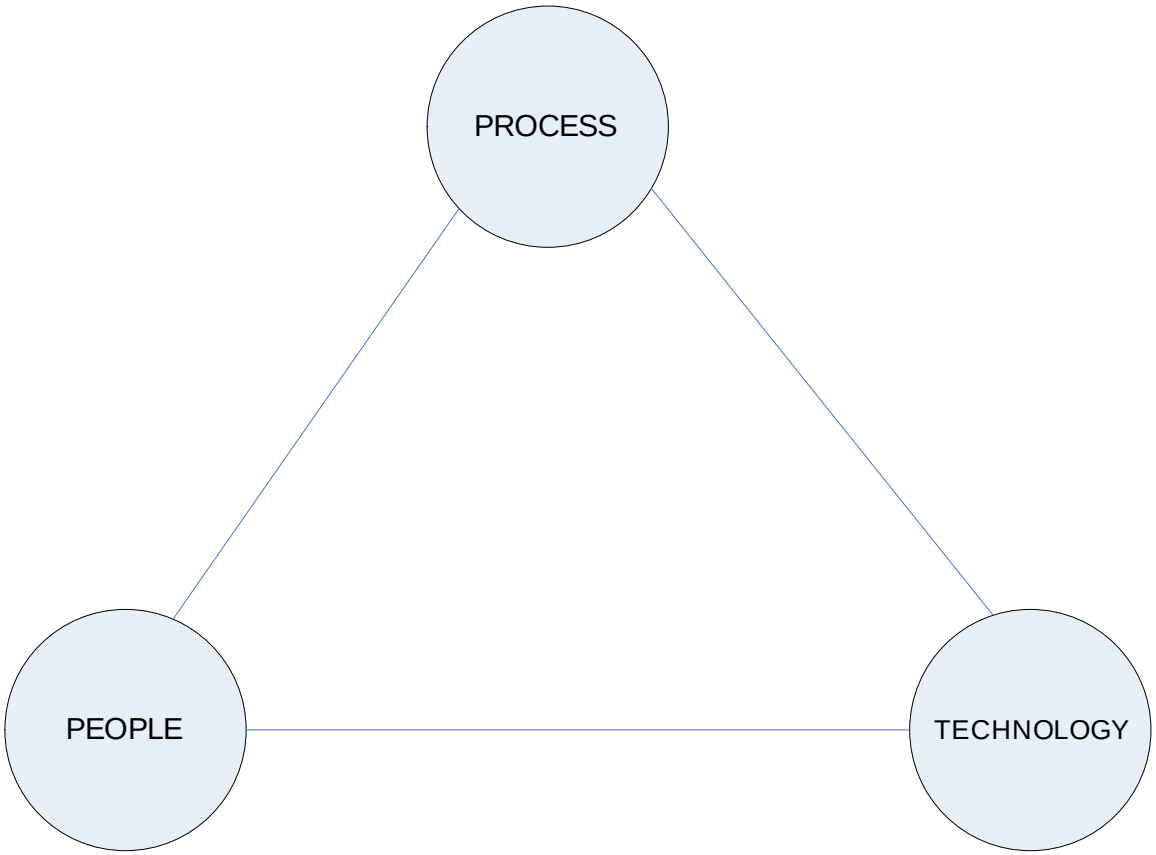


**The Capability Maturity Model* (CMM®) was developed by the Software Engineering Institute at Carnegie-Mellon University.

Process, People, Technology

In the Capability Maturity Model Integration (CMMI) Version 1.2* Overview presentation (http://www.sei.cmu.edu/cmmi/adoption/pdf/cmmi-overview07.pdf) the integrated role of Process, People, and Technology is highlighted. From the perspective of CMMI:

> "While process is often described as a node on the process-people-technology triad, it can also be considered the "glue" that ties the triad together. Everyone realizes the importance of having a motivated, quality work force but even our finest people cannot perform at their best when the process is not understood or operating at its best. Process, people and technology are the major determinants of product cost, schedule, and quality."



**Capability Maturity Model Integration* (CMMI®) *was developed by the Software Engineering Institute at Carnegie-Mellon University. Copyright 2007 Carnegie-Mellon University.*

Section 4: IT Strategic Goals and Focus Areas

In order to more effectively manage the achievement of the IT Vision, an IT Strategic Focus Area has been directly aligned with each IT Strategic Goal. Focus Areas provide key information, the Long-Term Strategic Goal, the Process Maturity Model to MEASURE progress, and Outcome Goals.

Focus Area 1: Enterprise Architecture (EA)

Enterprise Architecture (EA) is an emerging discipline at the National Transportation Safety Board. As is the case with this plan, the goal is to not reinvent the wheel but rather draw upon best practices developed across the Government in the area EA. The goal of the EA Program is to ensure IT aligns with the Safety Board's major program concerns. IT alignment will be achieved through an iterative process of mapping business processes, reducing/eliminating redundancies, and through the development of transition plans that will drive the continual refresh and upgrade of infrastructure and applications to meet current and emerging mission needs. Through this iterative process the EA Program will also contribute to the effective alignment of the underlying IT investment portfolio.

Long-Term Strategic Goal

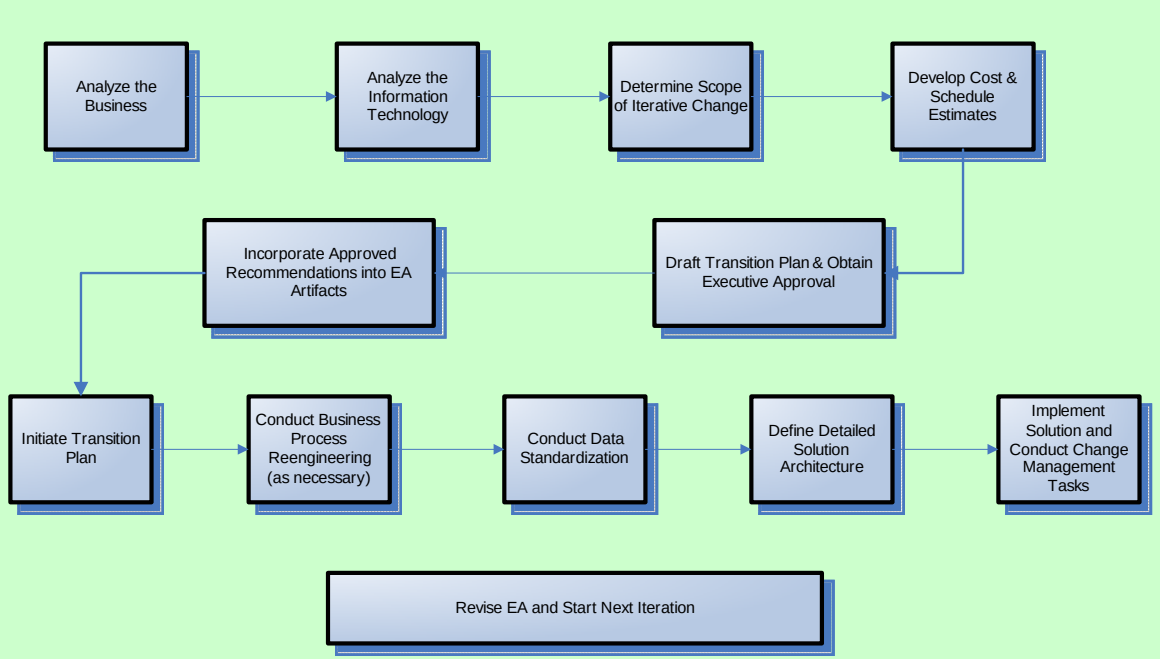
The goal of Enterprise Architecture (EA) is to improve the Safety Board's mission performance and realize its strategic goals and objectives. EA seeks to achieve this goal by:

- providing strategic business and architecture consulting services to program areas;
- improving the connection between stakeholders and investments;
- streamlining the processes and business rules in the program areas;
- minimizing system redundancies;
- improving data integration and data sharing;
- increasing the re-use of IT assets; and
- reducing the total cost of ownership of the Safety Board's IT Portfolio.

To carry out the iterative EA process and establish a transition, the Enterprise Architect will follow a modified version of the Department of Interior's Methodology for Business Transformation (MBT). The methodology identifies opportunities for improving mission performance and internal efficiencies and allows for the development of a transition plan for implementing these opportunities for improvement.

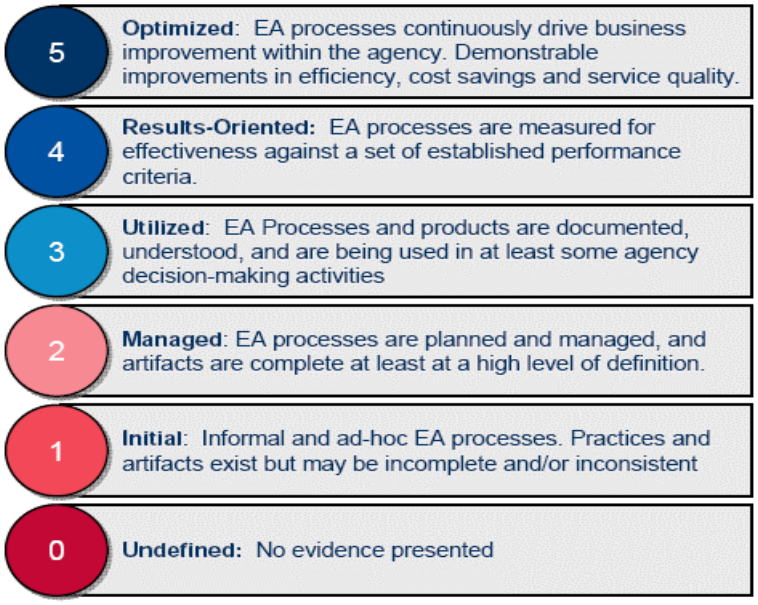
See Methodology for Business Transformation (MBT) process on next page.

Methodology for Business Transformation (MBT)



Process Maturity Model/Performance Measure

The Safety Board will use **OMB's Enterprise Architecture (EA) Maturity Framework v2.0 to** measure the agency's progress in this strategic goal.



Within this framework each Federal agency receives an average score in three capability areas: EA Completion, Use, and Results. The average is calculated by summing the score for all criterion within that capability area and then dividing by the number of criteria. Scores are rounded up to the nearest tenth. The results of the annual assessment process will be reflected in the Status score for E-Government within the President's Management Agenda. Agencies receive an overall score of Green for EA if the capability area score is equal to or greater than 3 in both the "Completion" and "Use" capability areas or have a score equal to 3 or greater in the "Results" capability area.

FY07 Outcome Goals

- Acquire slot for Enterprise Architect
- Develop position description and standards
- Initiate hiring process
- Hire Enterprise Architect

FY08 – FY12 Outcome Goals

- Synchronize EA activities with those of Information Security, Capital Planning, Strategic Planning, Program Management Office
- Complete initial Technical Reference Model, Business Reference Model, Service Reference Model, and Performance Reference Model
- Initiate Business Process Modeling
- Develop and Implement a Configuration Management process
- Complete Business Process Modeling
- Complete initial DRM model
- Retire redundant systems identified in Transition Plans
- Adhere to Federal EA Principles (see Appendix B)
- Achieve a minimum score of 2.5 out of 5.0 (self-assessed*) on the OMB EA Maturity Framework ***(FY10)***
- Achieve a minimum score of 3.5 out of 5.0 (self-assessed*) on the OMB EA Maturity Framework ***(FY11)***
- Achieve a minimum score of 4.0 out of 5.0 (self-assessed*) on the OMB EA Maturity Framework ***(FY12)***
- All EA models will be kept current and compliant with the FEA ***(annual)***
- Initiate the development of new Transition Plans based on prioritization actions ***(annual)***
- Release updated versions of the five EA Models as appropriate ***(annual)***

*Based upon assessment by an NTSB team comprised of employees outside of the OCIO.

Stretch Goals

- Reach EA Maturity Framework benchmarks ahead of schedule

Focus Area 2: IT Security

The Safety Board is committed to continuing improvements in its IT Security Program, and to complying with OMB Circular A-130, Appendix III Security Requirements. The Safety Board maintains a number of systems to support modal and office missions. This complexity makes security and IT management a very challenging undertaking, and underscores the need for further standardization.

Long-Term Strategic Goal

The goal of Information Security is to protect the availability, confidentiality, and integrity of the Safety Board's information technology resources. This goal is achieved through the application of requirements specified in OMB Circular A-130, the Federal Information Security Management Act (FISMA) and various U.S. Commerce Department's National Institute of Standards and Technology (NIST) publications. The NTSB IT Security Program uses a risk-based, cost-effective approach to secure information and systems, identify and resolve current IT security weaknesses and risks, and protect against future vulnerabilities and threats.

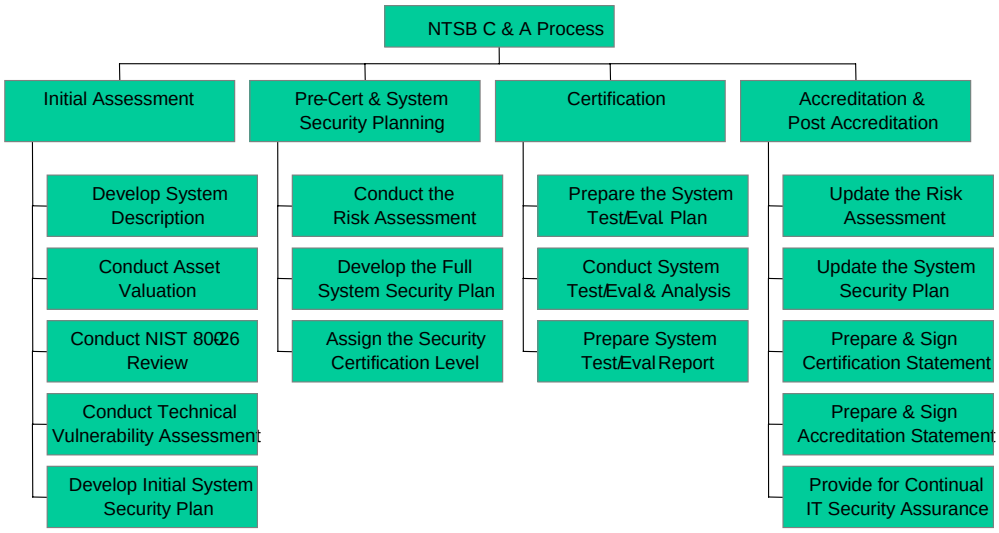
As shown in the table below, NIST has defined 17 areas that must be addressed as part of a world-class Information Security program. These 17 elements must be addressed in order to achieve the long-term strategic goal for this focus area.

NIST Security Program Elements

1. Risk Management
2. Review of Security Controls
3. Life Cycle
4. Authorize Processing (Certification & Accreditation)
5. System Security Plan
6. Personnel Security
7. Physical and Environmental Protection
8. Production, Input/Output Controls
9. Contingency Planning
10. Hardware and System Software Maintenance
11. Data Integrity
12. Documentation
13. Security Awareness, Training, and Education
14. Incident Response Capability
15. Identification and Authentication
16. Logical Access Controls
17. Audit Trails

The Certification & Accreditation (C&A) process is a key component of the security program as it consolidates many of the 17 program elements on a system-by-system basis. The Safety Board has adopted an iterative process to reach a level of maturity consistent with resources available.

The process is depicted on the next page:



Process Maturity Model/Performance Measure

The Federal IT Security Assessment Framework developed by NIST will be used to measure NTSB's progress in this strategic focus area.

Federal IT Security Assessment Framework

Level 1	**Documented Policy**
Level 2	**Documented Procedures**
Level 3	**Implemented Procedures and Controls**
Level 4	**Tested and Reviewed Procedures and Controls**
Level 5	**Fully Integrated Procedures and Controls**

FY07 Outcome Goals

- Address all outstanding Department of Transportation's Office of Inspector General recommendations
- Remain on schedule for existing Plan of Action and Milestones (POA&M)
- Mature the existing policy, procedure, and guidance capability to ensure the foundation of the NTSB IT Security Program
- Mature the existing risk management and compliance programs with regular vulnerability scanning and log review as key components of the Safety Board's continuous monitoring efforts
- Complete IT Security Awareness training for at least 95% of NTSB employees, contractors, and interns
- Enhance security controls and procedures for the protection of privacy data and other sensitive data for mobile computing devices, internal databases and applications, and remote access solutions

FY08 –FY12 Outcome Goals

- Achieve/Maintain C&A for 100% of the systems in the NTSB inventory
- Integrate IT Security into NTSB projects via the Information Systems Development Life Cycle (ISDLC)
- Develop necessary templates to support collection of IT Security and C&A data at appropriate point in ISDLC
- Develop and publish role-based IT Security training requirements
- Achieve a score of at least 2.5 out of 5.0 (self-assessed*) on the Federal IT Security Assessment Framework ***(FY08)***
- Achieve a score of at least 3.5 out of 5.0 (self-assessed*) on the Federal IT Security Assessment Framework ***(FY10)***
- Achieve a score of at least 4.5 out of 5.0 (self-assessed*) on the Federal IT Security Assessment Framework. ***(FY12)***
- POA&M development and execution for any items identified in FISMA audit ***(annual)***
- Mature and improve the existing policy, procedure and guidance capability to ensure the foundation of the NTSB IT Security Program ***(annual)***
- Mature and improve Incident Response Capability to ensure the proactive and reactive protection of NTSB infrastructure and data ***(annual)***
- Measure and improve the existing risk management and compliance programs with regular vulnerability scanning and penetration testing as the key components of OCIO's continuous monitoring efforts ***(annual)***
- Measure and improve Incident Response Capability to ensure the proactive and reactive protection of NTSB IT infrastructure and data ***(annual)***
- Measure and improve security controls and procedures for the protection of privacy data and other sensitive data for mobile computing devices, internal databases and applications, and remote access solutions ***(annual)***
- Measure and maintain C&A for 100% of the systems in the NTSB inventory ***(annual)***
- Continue to measure and improve the Security Awareness, Training and Education Program to ensure at least 95% of NTSB employees, contractors and interns have an increased level of awareness and experience commensurate to their areas of responsibility ***(annual)***

*Based upon assessment by an NTSB team comprised of employees outside of the OCIO.

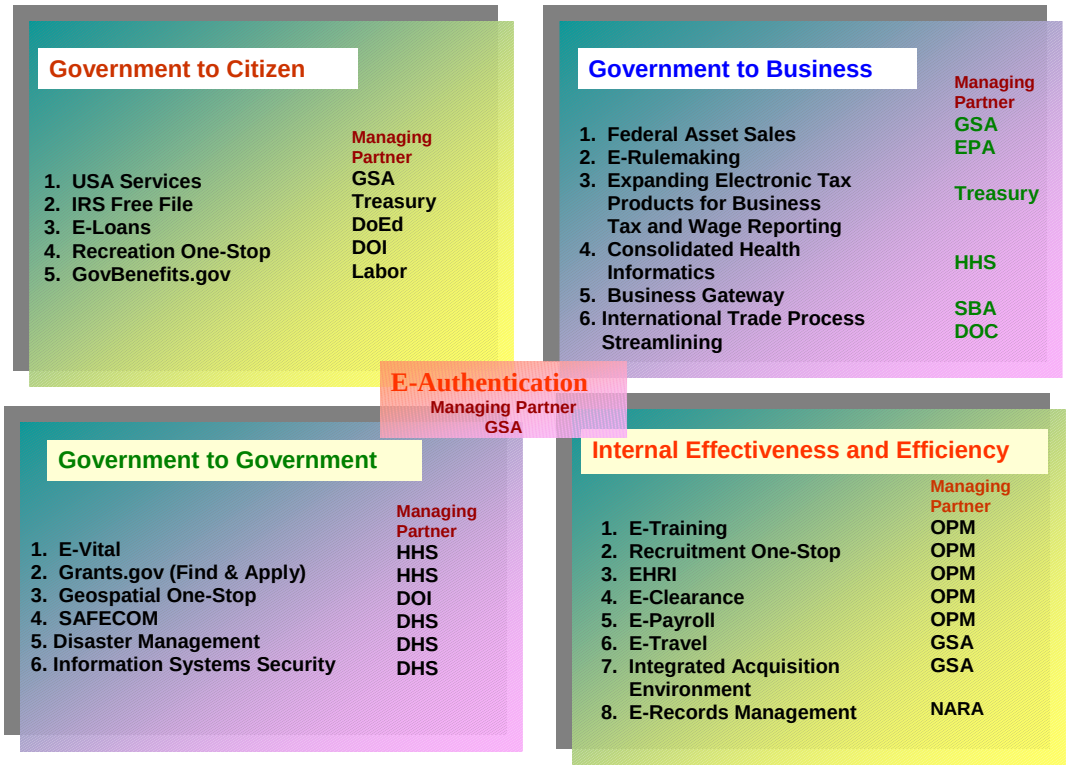
Stretch Goals

- Reach Federal IT Security Assessment benchmarks ahead of schedule

Focus Area 3: E-Government

E-Government has distinct and different meanings to individuals and organizations. For the purposes of this plan E-Government refers to the use of technology to deliver improvements in the Safety Board's mission areas and the Safety Board's partnership with existing and emerging Government-wide technology initiatives. For example NTSB currently partners with the Department of the Interior for financial and other services as part of their participation in the Human Resources and the Financial Management Lines of Business offerings.

E-Government Initiatives



E-Government initiatives cut across multiple Federal agencies and address opportunities to provide services in the areas of Government to Citizen, Government to Business, Government to Government, and Internal Effectiveness and Efficiency. Current initiatives in each of these areas are summarized in the diagram above.

Long-Term Strategic Goal

The goal of E-Government is to improve the efficiency and effectiveness of the Safety Board's business processes. E-Government technology will enable us to do our jobs better. Using Safety Board's emerging Enterprise Architecture program, the Office of the Chief Information Officer will explore and map NTSB mission needs and continue to look for opportunities for E-Government investment.

Another facet of the Safety Board's Strategic Goal regarding E-Government will include the development of a strong Project Management practice. The Safety Board will use Project Management throughout OCIO, and recognizes that the scope and nature of the Board's efforts undertaken as part of E-Gov will require strong Project Management (PM) skills. As a result, individuals in the System Support Division will serve as mentors for Project Management in OCIO.

This goal is directly supported by several of the other goals identified in this plan, in the EA, IT Security, and IT Infrastructure focus areas. In addition, this focus area covers the areas of Section 508 compliance and Web Management. The maturity model used to measure performance in this area is the President's Management Agenda.

The President's Management Agenda (PMA)

Released by the OMB in August 2001, the President's Management Agenda (PMA) identified five mutually reinforcing initiatives, each addressing a key element in management performance with a significant opportunity for improvement: Strategic Management of Human Capital; Competitive Sourcing; Improved Financial Performance; *Expanded Electronic Government*; and Budget and Performance Integration.

Expanded Electronic Government: This PMA initiative launched to make better use of Federal Government information technology (IT) investments, improve the accessibility of information and services, and reduce response time to citizens. The vision for e-Government involves citizens and businesses easily obtaining services and interacting with the Federal Government while improving overall efficiency and effectiveness (*see Appendix C – 2007 PMA Standards for Success*). The Safety Board's IT Strategic goals are aligned with PMA e-Government performance measures.

Process Maturity Model/Performance Measure

This aggressive strategy focuses on managing areas of weakness across the government, and making improvements where the most progress can be achieved. OMB measures and scores each Federal agency's PMA performance on a quarterly basis with its *Stoplight Scoring System*. The PMA Scorecard employs a simple grading system common today in well-run businesses: **Green** for success, Yellow for mixed results, and **Red** for unsatisfactory. One of the factors included in the scorecard is the Enterprise Architecture maturity score discussed in Focus Area 1. Additional scorecard items applicable to this focus area include IT Security, Privacy, and Project Management.

FY07 – Outcome Goals

- Initiate standard Project Management training
- Deploy new COTS-based Help Desk system
- Establish Web Guild
- Deploy FOIAXpress system
- Ascertain Section 508 Compliance

FY08 –FY 12 Outcome Goals

- Deploy eADMS in production environment
- Deploy agency-wide Project Tracking System
- Upgrade DMS architecture
- Shorten report turnaround time by 5-10 workdays via Adobe InCopy\InDesign upgrade
- Update Information System Development Life Cycle to support:
    - Enterprise Architecture
    - IT Security
    - Capability Maturity Model Integration (CMMI) Level II
    - Data Privacy
- Conduct NTSB web standards compliance reviews on NTSB websites
- Develop, maintain, and facilitate a sound and integrated web-related information technology architecture for the Safety Board by improving the quality of the Intranet and Internet websites
- 80% of E-Gov projects within 10% of the goals established in the cost, schedule, and performance baseline ***(FY08)***
- 90% of E-Gov projects within 10% of the goals established in the cost, schedule, and performance baseline ***(FY09)***
- 95% of E-Gov projects within 10% of the goals established in the cost, schedule, and performance baseline ***(FY10)***
- Achieve PMP certification for at least 75% of Systems Support Division staff ***(FY12)***
- Assess NTSB production systems per Steady State CPIC Phase requirements ***(annual)***
- Partner with Enterprise Architect on development and execution of Transition Plan ***(annual)***
- Review NTSB websites for compliance with applicable Federal statutes and directives ***(annual)***

Stretch Goals

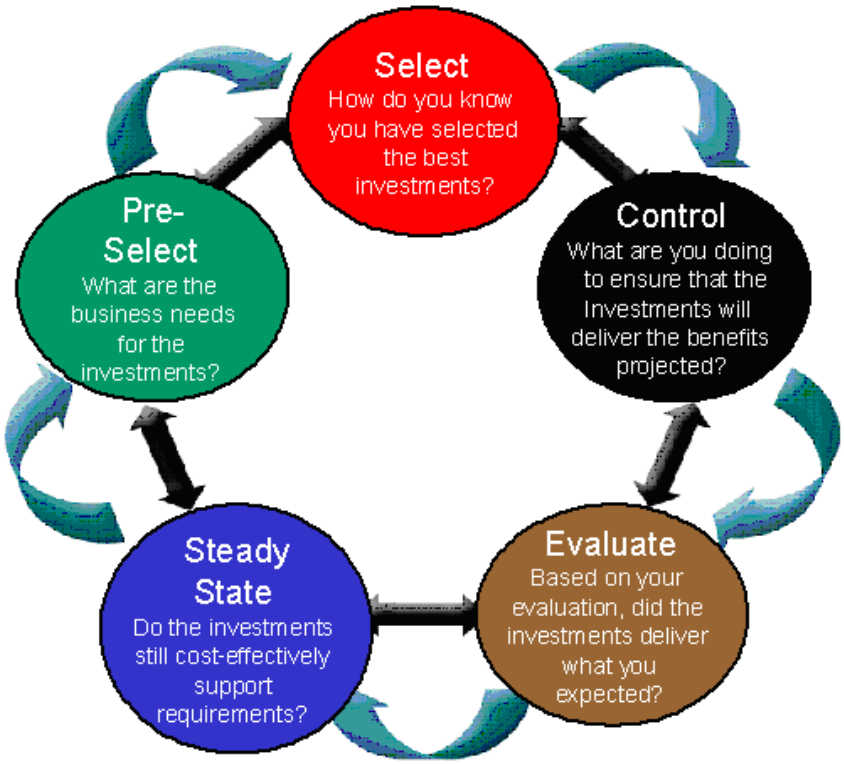
- Implement customizable portal ***(FY11)***

Focus Area 4: IT Capital Planning & Investment Control (CPIC) Process

Long-Term Strategic Goal

The goal of Capital Planning is to improve the planning, execution, and management of IT investments. The overall process for Capital Planning varies slightly from organization to organization but should include the five sequential phases represented in the diagram below.

NTSB Capital Planning Investment Control (CPIC) Process



Activities supporting the Capital Planning Focus Area are closely tied to activities in the Enterprise Architecture Focus Area. Capital Planning defines a process for reviewing, approving, and monitoring investments. Enterprise Architecture ensures that the investments being made are not redundant and that they support mission goals.

The goal over the next few years is to introduce standard CPIC processes to the Safety Board on a scale that is consistent with the threshold of IT investment dollars. These changes will be consistent with best practices and consistent with the GAO IT Investment Management (ITIM) Framework.

See Appendix D for NTSB's CPIC Process and Appendix E for the Non-Major IT Investment Business Case Template.

Investment Review Board (IRB): IT Portfolio Decision-Making

NTSB IT Investment Review Board (IRB): Collaborative IT governance process.

IT investments at the Safety Board are effectively managed but through processes that are outside standard CPIC processes. As the Safety Board progresses through the FY2007 – FY2012 Strategic Planning cycle, the Board expects the IT investment process to mature considerably. One of the steps in the CPIC process is to establish an IRB that makes "smarter" recommendations on the viability and prioritization of proposed initiatives; prevent duplicate investments; and leverage shared solutions, where appropriate. The IRB will ensure the NTSB IT Portfolio follows Management Objectives and Business Priorities criteria as listed.

Management Objectives - Criteria to evaluate investments in the CPIC process.

- Implement legal and judicial mandates
- Respond to internal and executive mandates
- Obtain positive return on investments
- Improve performance (showing links to NTSB Strategic Plan and performance goals, avoiding duplication, managing risk, improving efficiency, achieving specific objectives)

Business Priorities - The second tier of management guidance for portfolio decisions.

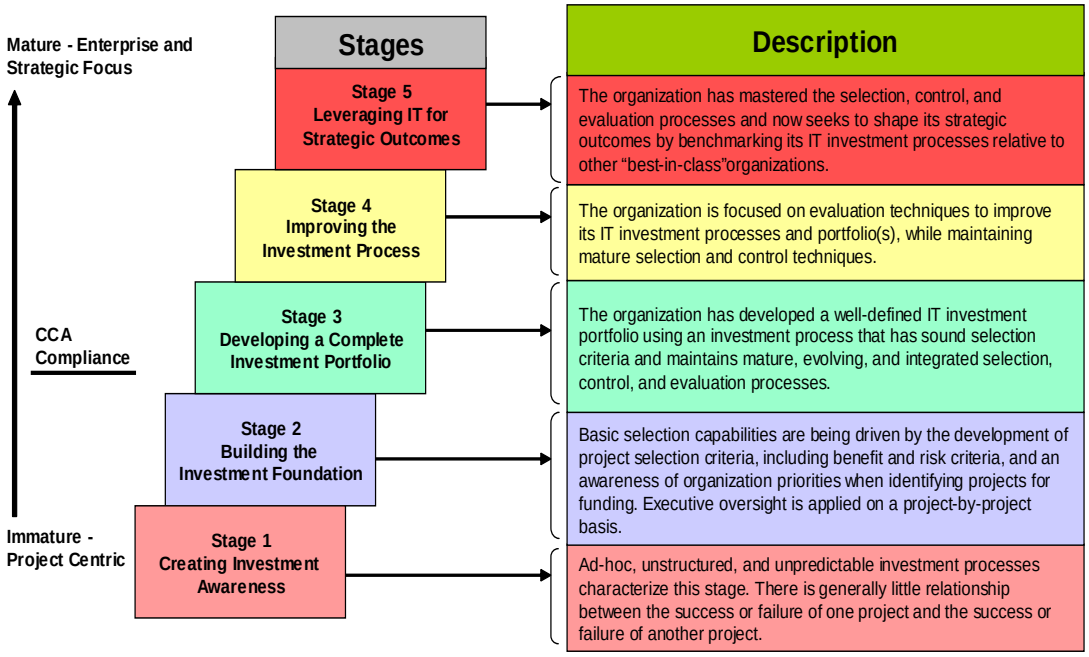
- Enterprise projects
- Projects on schedule, within costs, meeting expectations (evaluated through control reviews)
- Projects that are consistent with EA Transition Plan
- Management objectives and business priorities provide general guidance

Process Maturity Model

Progress in the Capital Planning focus area will be tracked using the GAO IT Investment Management (ITIM) Framework.

See next page for GAO IT Investment Management (ITIM) Framework.

GAO's Investment Technology Investment Management (ITIM) Model *(GAO-04-394G)*



FY07 Outcome Goals

- Establish basic business case template (short version) for IT investments
- Develop business case for IT Infrastructure refreshment
- Develop basic NTSB IT CPIC procedures

FY08 –FY 12 Outcome Goals

- Provide CFO with three-year budget forecasts for TechRep and OCIO support requirements
- Establish and maintain OCIO budget control sheets to track expenditures in a timely manner
- Process all credit card purchases in compliance with NTSB regulations and timelines
- Process all PRs in compliance with NTSB regulations and timelines
- Phased approach to achieve CPIC process maturity during FY08 – FY12
    - 80% of IT investments will be within 10% of the goals established in the cost, schedule, and performance baseline

    - 90% of IT investments will be within 10% of the goals established in the cost, schedule, and performance baseline
    - Synchronize Capital Planning activities with those of Enterprise Architecture and Information Security
    - 100% of IT investments will be reviewed and approved through the CPIC process
    - 95% of IT investments will be within 10% of the goals established in the cost, schedule, and performance baseline
- Achieve Level 2 of the GAO ITIM Maturity Model ***(FY08)****
- Achieve Level 3 of the GAO ITIM Maturity Model ***(FY10)****
- Achieve Level 4 of the GAO ITIM Maturity Model ***(FY12)****

*Based upon assessment by an NTSB team comprised of employees outside of the OCIO.

Stretch Goals

- Reach GAO ITIM Maturity Model benchmarks ahead of schedule

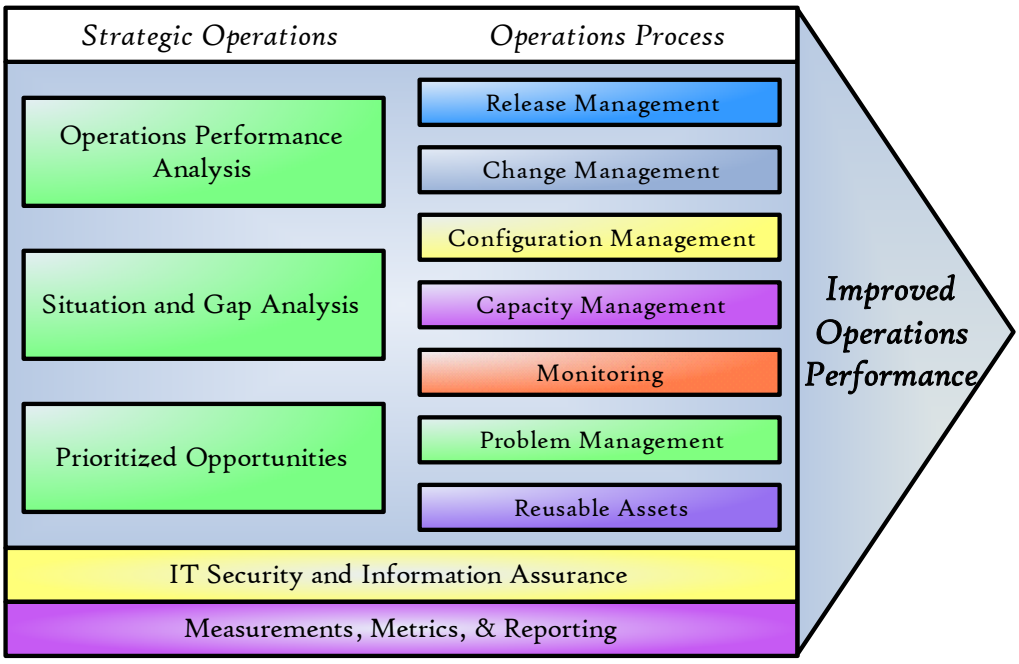
Focus Area 5: IT Infrastructure

The Safety Board acknowledges that standardizing operational capabilities, such as through standard desktop, laptop and server configurations, and secure wireless communications, is an essential component for attaining the desired level of maturity in the focus area of IT Infrastructure. A mature IT Infrastructure serves as a platform for continued standardization, and provides the capability to measure overall service level improvement. In an effort to increase the maturity level of the Safety Board's IT Infrastructure, the Office of the Chief Information Officer will continue to move toward infrastructure lifecycle planning, by factoring replacement costs into annual budgets as a continuing cost of doing business. The OCIO will also adopt the Information Technology Infrastructure Library (ITIL) framework to provide improved service quality to the Safety Board's customers.

Long-Term Strategic Goal

The goal of this focus area is to provide enhanced enterprise operations capabilities — improving the quality, accessibility, and sharing of data between NTSB and its customers. The overall goal of this focus area is to provide improved levels of service and security within a cost-effective, value-added operational structure.

Operations Performance Analysis will be applied to activities in this area. The analysis will identify opportunities for improvement. This approach will allow the Safety Board to provide continuous improvement in operations performance.



**ITIL was produced by the UK Office of Government Commerce.*

Process Maturity Model/Performance Measure

The Safety Board will use the **Information Technology Infrastructure Library (ITIL**) to track progress in this strategic area and to provide quality IT service in the face of budgetary constraints, skill shortages, system complexity, rapid change, current and future customer requirements, and growing customer expectations

FY07 Outcome Goals

- Asset Management
  - Install LANDesk to support IT Asset Management Program
- Customer Service
  - Install Heat system to provide enterprise support for incident, service, and change management processes
- Infrastructure Management:
  - Encrypt laptops used in Telework Pilot in compliance with OMB-06-16
  - Make encryption of laptops standard part of distribution process for new equipment
  - Initiate analysis of requirements to comply with OMB-07-11
  - Evaluate requirements to create fully operable development and test environments to support enhanced ISDLC activities
- Continuity of Operations (COOP)
  - Evaluate COOP capabilities at the NTSB Training Center facility
  - Identify additional resource needs to provide email and blackberry connectivity should the Safety Board's Headquarters site become inoperable
- Telecommunications:
  - Initiate upgrade of network capacity to field and headquarters locations
  - Evaluate tools to monitor and enhance network utilization
  - Initiate small scale pilot efforts to support wireless communication
  - Evaluate requirements to ensure compliance with IPv6 implementation schedules

FY08 –FY 12 Outcome Goals

- Asset Management
  - Initiate IT Asset Management Program
  - Explore option of expanding LANDesk to non-IT assets
  - Implement IT Asset Management Program (ITIL based)
  - Comply with requirements of IT Asset Management Program
- Customer Service
  - Develop FAQ page for common incidents and services
  - Place Heat system in production
  - Initiate phased-approach to reach ITIL process maturity FY08 – FY12
    - Service Level Agreements (SLAs) in place and met for 95% of cases for 20 most common incident and service request

        - SLAs in place for 100% of incident and service requests
        - SLAs met 98% or more of the time, documented reasons for all cases where SLA is exceeded
        - Meet network SLA provisions

- Infrastructure Management:
    - Encrypt all laptops in use at NTSB
    - Have standard configurations for laptops, desktops and servers
    - Achieve state where IT equipment is operating at no more than 2 releases behind on operating system software
    - Deploy Microsoft Operations Manager (MOM) to enhance infrastructure services and reduce costs
    - Implement fully operable development and test environments to support enhanced ISDLC activities

- Continuity of Operations (COOP)
    - Work with the Safety Board's senior management to prioritize IT resource requirements for COOP
    - Develop phased-plan to upgrade NTSB IT COOP capabilities
    - Deliver enhanced COOP capability to plan
    - Institute tests of COOP capabilities in place ***(annual)***
    - Update and integrate OCIO COOP Plan into overall NTSB COOP Plan ***(annual)***

- Telecommunications:
    - Mitigate deficiencies in IPv6 Program (i.e. obtain address block, etc.)
    - Ensure backbone devices are IPv6 capable ***(FY08 – June 30)***
    - Establish network SLAs
    - Provide enterprise solution to support secure wireless communication
    - Ensure agency-wide IPv6 capability ***(FY10)***
    - Meet network SLA provisions ***(annual)***

Stretch Goals

- Have ITIL compliant IT infrastructure environment by FY10

Focus Area 6: Information and Records Management

NTSB recognizes the importance of sound information and records management practices and has developed goals to drive improvements in support of the Information Management areas which include: Records Management, Privacy, Information Quality, and the Freedom of Information Act (FOIA).

Long-Term Strategic Goal

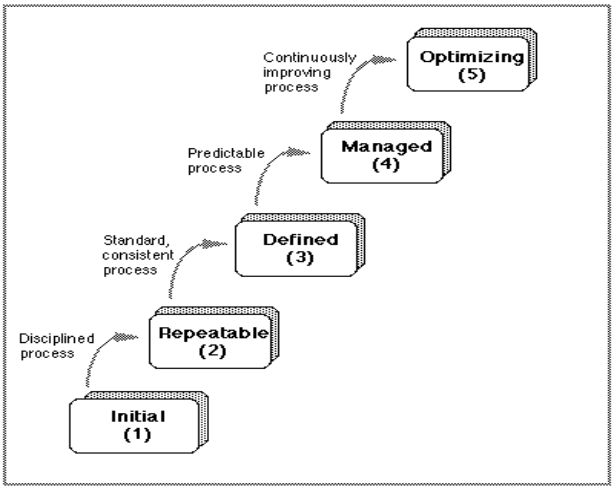
The goal of Information and Records Management is to provide the information needed to make thoughtful decisions, to inform our stakeholders and provide appropriate public access to information, and to protect sensitive information from inappropriate release.

Information and Records Management must support the Safety Board's workforce in managing an ever-increasing volume of information and provide for the retention of institutional knowledge despite a growing numbers of retirees from Federal service. Information and Records Management that follows mandatory standards is a keystone for ensuring an effective and responsible knowledge-sharing environment and provides assurance to E-Government customers that the Safety Board is serious about its role of steward of their information.

The Safety Board also recognizes the need to provide timely and accurate information to a broad customer base through an effective FOIA Program. As a result, the Safety Board has moved aggressively to bring its FOIA Program into full compliance with the E-FOIA Act of 1996 and other Federal mandates. Specific metrics have been set over the life of this strategic plan to ensure that compliance is achieved and maintained.

Process Maturity Model/Performance Measure

The maturity model shown below is used to track progress in this focus area.



**This maturity model was based on the* (CMM®) *developed by the Software Engineering Institute at Carnegie-Mellon University.*

FY07 Outcome Goals

- Initiate use of FOIAXpress system in support of the Safety Board's FOIA Program
- Set and publish rates and exclusions for FOIA charges
- Execute all FY07 milestones in the Safety Board's FOIA Improvement Plan, which is designed to improve the overall effectiveness and efficiency of the FOIA Program as well as customer service.
- Update NTSB Internet FOIA site to comply with requirements of E-FOIA Act of 1996
- Eliminate backlog of simple FOIA requests
- Complete FOIA training for non-modal offices

FY08 –FY 12 Outcome Goals

- Review the Safety Board's FOIA Improvement Plan and adjust as required
- Eliminate FOIA backlog
- Evaluate capability to add additional documents (i.e., DMS) to the Safety Board's website to reduce FOIA requests
- Initiate addition of documents to the Safety Board's website based upon analysis of IT infrastructure capabilities
- Initiate planning for development of NTSB Records Schedule
- Complete NTSB Electronic Record Schedule
- Meet the E-Government Scorecard requirements for "Maintaining Green"
    - Demonstrated for 90% of applicable systems a Privacy Impact Assessment has been conducted and publicly posted
    - Demonstrated for 90% of systems with personally identifiable information a system of records notice has been developed and published
- Refine Records Management Capability Maturity Model
- Complete Action items in FOIA Plan
- Gain National Archives and Records Administration (NARA) approval of NTSB Electronic Record Schedule
- Ensure compliance with Federal laws relating to Records Management, Privacy, Information/Data Quality, and FOIA ***(annual)***
- Maintain backlog of FOIA requests of 50 or fewer cases for simple and complex requests ***(annual FY09 and later)***
- Conduct FOIA training events to increase the visibility of the Safety Board's FOIA Program ***(periodic)***

Stretch Goals

- Achieve rating of "E-Star Agency" in FOIA by The National Security Archive ***(FY09)***
- Establish a records schedule one or more fiscal years ahead of schedule

Focus Area 7: IT Workforce Management

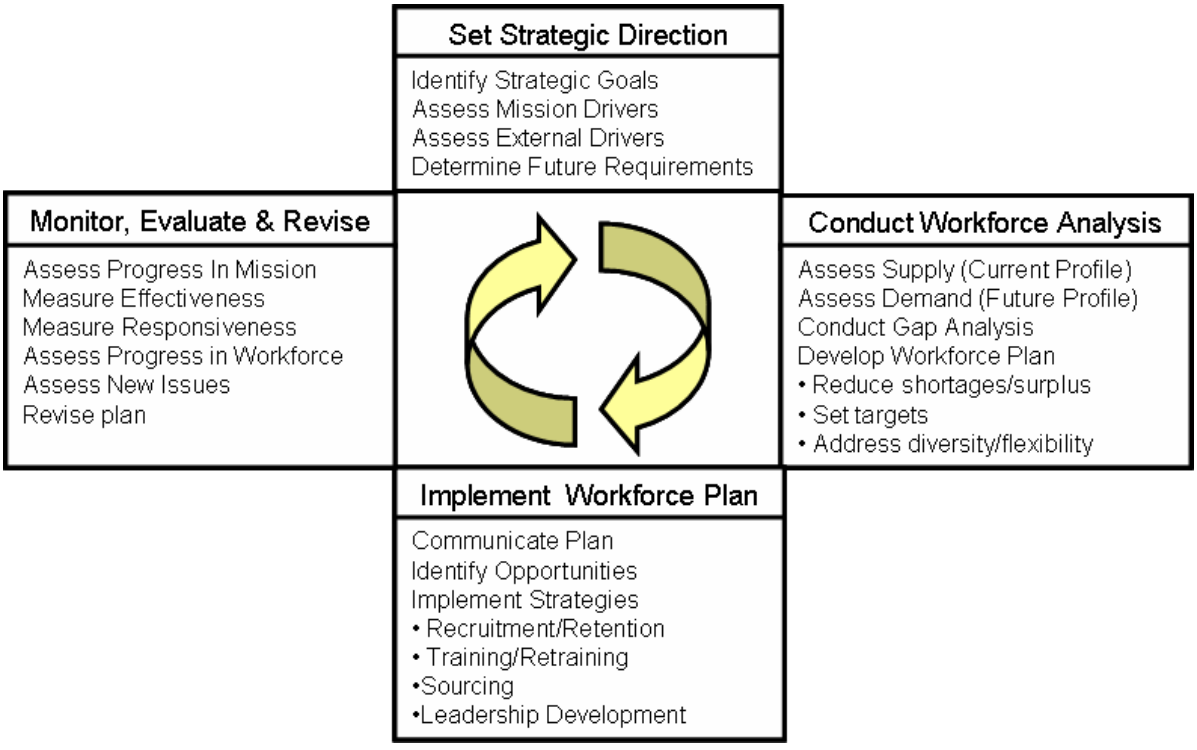
A well-trained, experienced workforce is vital to providing excellence in IT services. Key focus areas include staffing, IT skills and competencies, role-based training, and succession planning. The Safety Board's IT workforce management will build on known human capital management successes to leverage the capabilities of this critical resource.

Long-Term Strategic Goal

The goal of this focus area is to ensure the availability of IT human capital capable of meeting IT goals and NTSB mission challenges. This focus area includes:

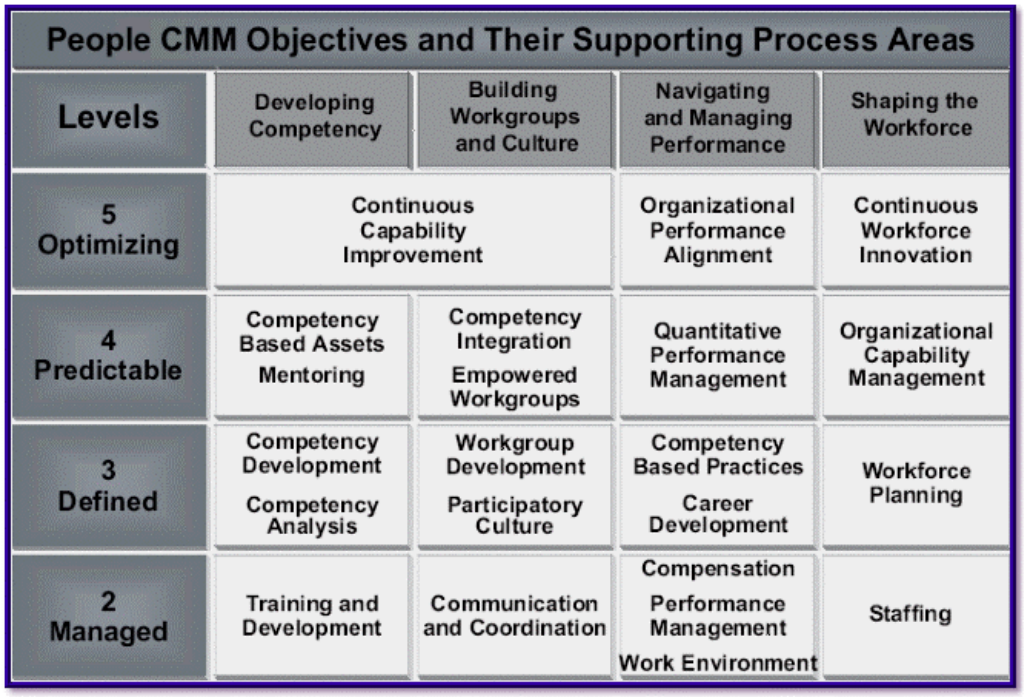
- improvement of IT workforce identification, assessment, and reporting capabilities;
- ensuring that robust IT professional development programs are available; and
- strengthening and leveraging IT project management skills.

Success in this area must also take into account changes to business processes, workloads, and required skill sets that will result from implementation of enterprise initiatives, modernization blueprints, and E-Government initiatives. A graphic representation of this multi-source iterative process is presented below.



Process Maturity Model/Performance Measure

The "People Capability Maturity Model" is used to measure the Safety Board's progress in the Skilled Workforce focus area.



People CMM Objectives and Their Supporting Process Areas				
Levels	Developing Competency	Building Workgroups and Culture	Navigating and Managing Performance	Shaping the Workforce
5 Optimizing	Continuous Capability Improvement		Organizational Performance Alignment	Continuous Workforce Innovation
4 Predictable	Competency Based Assets Mentoring	Competency Integration Empowered Workgroups	Quantitative Performance Management	Organizational Capability Management
3 Defined	Competency Development Competency Analysis	Workgroup Development Participatory Culture	Competency Based Practices Career Development	Workforce Planning
2 Managed	Training and Development	Communication and Coordination	Compensation Performance Management Work Environment	Staffing

**The People Capability Maturity Model* (CMM®) *was developed by the Software Engineering Institute at Carnegie-Mellon University.*

FY07 Outcome Goals

- Develop baseline IT Human Capital and Training Plans

FY08 –FY 12 Outcome Goals

- Refine and integrate baseline IT Human Capital and Training Plans with emerging agency-wide Human Capital and Training Plans
- Make Human Capital development part of performance plans for supervisors, managers, and employees
- Complete IDPs for 95% of OCIO staff
- Evaluate staff developmental progress against Human Capital and Training Plans ***(annual)***

Stretch Goals

- No current stretch goal(s) for this focus area

Stretch Goal(s) will be developed based upon input from the agency-wide Human Capital Plan schedule for release in FY08.

Section 5: Conclusion

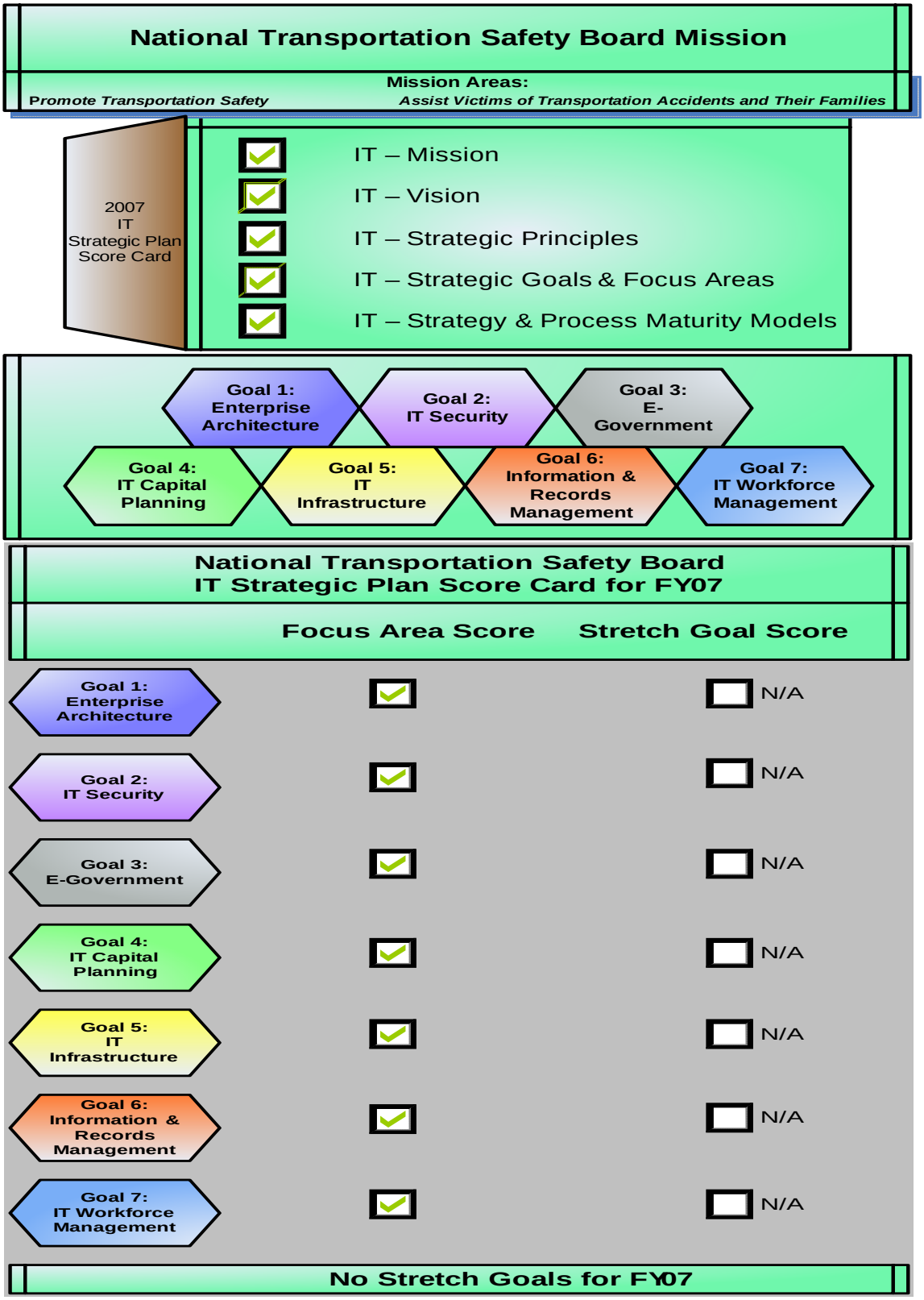
The National Transportation Safety Board's IT Strategic Plan provides a strategic framework for the coordinated development, implementation, operation, and integration of information technology within the Board. The Safety Board's IT Strategy will enhance the efficiency and effectiveness of the organization as well as support the successful delivery of Mission results.

Additionally, this document provides an organizational framework for the continued development of an architecture that can support more levels and types of electronic interactions. It outlines the Safety Board's IT Strategic Principles, establishes specific IT Strategic Goals with corresponding Focus Areas, and directs IT resources to utilize Maturity Models to measure performance. The Safety Board will strive for these collective approaches to improve performance, reduce inefficiency and duplication, and provide the support needed to achieve our important Mission.

The Safety Board will continue the migration of its IT portfolio toward integrated, agency-wide business processes and technologies to maximize the innovative and effective use of technology. Through leadership in customer service, strategic planning, intelligent management of IT resources and investments, and continual improvements in securing our IT environment, the OCIO will provide high-speed reliable services that meet customer expectations and create savings.

As a key component in achieving the Safety Board's Mission, the Office of the Chief Information Officer will provide a viable means for ensuring that the Board receives the best value for its precious resources.

IT STRATEGIC PLAN CHECK LIST & SCORE CARDS



Appendix A: NTSB's Response to M-06-02 Improving Public Access to and Dissemination of Government Information Using the FEA Data Reference Model

Web Component of the National Transportation Safety Board's Information Dissemination Program

NTSB Mission

The transportation industry accounted for 10 percent—more than $1.2 trillion—of U. S. Gross Domestic Product [GDP] in 2005. We are proud to play a key role in maintaining the viability of this industry by investigating accidents and promoting safety.
Our mission is:

to promote transportation safety by

- maintaining our congressionally mandated independence and objectivity;
- conducting objective, precise accident investigations and safety studies;
- performing fair and objective airman and mariner certification appeals; and
- advocating and promoting NTSB safety recommendations. And

to assist victims of transportation accidents and their families.

The National Transportation Safety Board is an independent Federal agency charged by Congress with investigating every civil aviation accident in the United States and significant accidents in the other modes of transportation -- railroad, highway, marine and pipeline -- and issuing safety recommendations aimed at preventing future accidents. The Safety Board determines the probable cause of:

- all U.S. civil aviation accidents and certain public-use aircraft accidents;
- selected highway accidents;
- railroad accidents involving passenger trains or any train accident that results in at least one fatality or major property damage;
- major marine accidents and any marine accident involving a public and a non-public vessel;
- pipeline accidents involving a fatality or substantial property damage;
- releases of hazardous materials in all forms of transportation; and
- selected transportation accidents that involve problems of a recurring nature.

The Board derives its authority from Title 49 of the United States Code, Chapter 11. The rules of the Board are located in Chapter VIII, Title 49 of the Code of Federal Regulations.

The NTSB is responsible for maintaining the government's database of civil aviation accidents and also conducts special studies of transportation safety issues of national significance. The NTSB provides investigators to serve as U.S. Accredited Representatives, as specified in international treaties for aviation accidents overseas involving U.S.-registered aircraft, or involving aircraft or major components of U.S. manufacture.

The NTSB also serves as the "court of appeals" for any airman, mechanic or mariner whenever certificate action is taken by the Federal Aviation Administration or the U.S. Coast Guard Commandant, or when civil penalties are assessed by the FAA. For more information about this NTSB function, see the pages regarding the Administrative Law Judges and General Counsel.

Information Dissemination across NTSB Offices

The NTSB is organized into many Offices. Each fulfills one or more key elements of the NTSB mission. Each Office disseminates information to the general public and to unique customer communities that relates to each Office's mission.

There are four key goals supported by all Offices for which information is provided across various programs. These include:

Strategic Goal #1 – Accomplish Objective Investigations of Transportation Accidents to Identify Issues and Actions that Improve Transportation Safety

Strategic Goal #2 – Increase our Impact on the Safety of the Transportation System

Strategic Goal #3 – Outstanding Stewardship of Resources

Strategic Goal #4 – Organizational Excellence

A summary of NTSB Data and information products is provided below:

DATA & INFORMATION PRODUCTS

The following is an alphabetical list that describes information available from the NTSB, much of which is on the NTSB website. The Government Information Locator Service (GILS) also offers a standard description format - see GILS Records for more information. Almost all factual information about an accident and all final documents issued by the Board are available to the public in some form. Information products distributed by the Board adhere to quality assurance guidelines. Keep in mind that other transportation-related information may be available from related sites.

To obtain any of this information, use the online links provided with each description, or see Information Sources & Contacts.

- Accident Reports
- Annual Report to Congress
- Annual Review of Aircraft Accident Data - U.S. Air Carrier Operations
- Annual Review of Aircraft Accident Data - U.S. General Aviation
- Aviation Accident Database
- Initial Decisions of the Administrative Law Judges
- Investigation Guides and Procedures
- NTSB 2006 Federal Human Capital Survey (PDF, 44 KB)
- NTSB Directives
- NTSB Seal (GIF format, 331x335 pixels)
- Opinions & Orders
- Pamphlets
- Press Releases
- Public Records and Files, including Accident Dockets
- Regulations of the NTSB
- Safety Recommendations
- Safety Studies
- Special Investigations
- Speeches & Testimony of the Board Members and Staff
- We Are All Safer

To achieve the goals of organizing and categorizing government information to make it readily searchable across agencies so as to improve public access and dissemination the Safety Board is engaged in the following initiatives:

- Developing Web Standards – The Office of the Chief Information Officer has established a Web Guild to develop organizational roles and responsibilities, web standards, and to ensure compliance with requirements mandated by Federal laws and regulations, policies on authenticity and branding; document type definition standards; and customer focus.

- Taxonomy – In keeping with the practice of using standard practices the Safety Board intends to adopt the ISO 11179 standard to consistently organize and describe data in its formal information models. The Safety Board's Data Reference Model will be developed in accordance with the milestones identified in the Enterprise Architecture (EA) focus area. The use of ISO 11179 standard taxonomies will enable NTSB customers to locate a particular type of content more easily, based on its categorization through Metadata and enabling Key Word searches.

- RSS feeds – The Safety Board is in the process of implementing Really Simple Syndication (RSS) as a method to inform the customers of pertinent information on new or updated content on a real-time basis.

- Content Management

    - Content Management Systems – the Safety Board is in the process of implementing a content management system to make it easier for web information content providers to maintain web pages without having to learn web programming.

    - Templates – the Safety Board will develop Web page templates in order to promote a common interface, and to simplify navigation for customers so that customers will not need to spend time "learning" a new interface.

- P3P - Implementing the Platform for Privacy Preferences Project (P3P) that enables websites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents such as Web browsers and other software to access Web content.

- Consumer Identification – the Safety Board is in the process of more accurately identifying the consumers of information and the needs of such consumers. This information will enable the Safety Board to more accurately provide the right types of information to the right consumer through the right channel in the right amount of time.

- Web Review and Certification – An annual review of NTSB websites ensures that the public has access to up-to-date, accurate information.

- Search – Key to discoverability is the customer's ability to locate the exact type of information they are interested in. The Safety Board is examining improvements to its search engine to provide greater relevancy, increased content, and reduced search times.

- Website and Server Consolidation –As technology matures, the Safety Board is actively consolidating and streamlining websites to drive efficiency, reduce costs, and simplify information discovery and dissemination. Servers are also being consolidated and relocated to centralized data centers for efficiency, security, and reliability.

Results of NTSB's Information Dissemination Program Review

Information Dissemination takes place at many levels at the National Transportation Safety Board. As noted above, the Safety Board's broad, multi-modal mission and geographically dispersed Offices are responsible for maintaining and improving the safety of the Nation's transportation systems. Information pertaining to these programs and services is varied and our approximately 400 employees and volunteers deliver programs through partnerships and cooperative relationships that engage key stakeholders to participate.

The Safety Board is committed to ensuring the public has access to the information it is entitled to under the law. Content of materials published via the Internet is managed at the office level. Office Web Guild representatives and the NTSB Web Guild Manager work in partnership to ensure that material posted on the Web is examined to avoid posting any non-public information on individuals. Web pages are developed according to E-Government Act of 2002 privacy requirements and OMB web privacy guidelines (see OMB Memoranda M-03-22, M-00-13, and M-99-18, and OCIO Directives), and are scanned routinely for compliance. Web scans also review compliance with Section 508 of the US Rehabilitation Act, Freedom of Information Act requirements, and other web maintenance standards.

With respect to quality of information standards, the Safety Board is in compliance with the February 2002 guidance issued by OMB requiring all Federal agencies to issue and implement Information Quality Guidelines. These guidelines ensure the quality, objectivity, utility, and integrity of information disseminated by the Safety Board's offices. In compliance with the guidelines, the Safety Board and its offices provide a venue for the public to challenge and seek correction of information disseminated, and offices have a procedure in place to address these challenges.

The OCIO is responsible for developing regulations, guidelines, procedures, and for coordinating standards developed by the NTSB Web Guild. The Web Guild meets routinely, with representation from the majority of NTSB offices. The Web Guild provides a forum for sharing best practices, evaluating Web tools and providing oversight and technical assistance for the Safety Board's Web programs.

The Public Affairs Division provides oversight and guidance regarding press releases and information disseminated to the public directly and is responsible for developing procedures that pertain to maintaining the continuing responsibility of keeping constituencies and the general public informed of the Safety Board's programs and activities (including news releases, speeches, audio visual productions, publications and articles). The overall responsibility for assuring adherence to information dissemination policies and procedures rests with the Public Affairs Division, which coordinates the general information activities of all offices of the Safety Board.

NTSB Plan to Reduce the Gaps in the Performance and Results of its Information Dissemination Program

Through this management and oversight structure, the Safety Board maintains the information dissemination standards established through the processes outlined above. The review processes

established for each of these areas provides a means of determining gaps in performance and recommendations to address key issues. For example, the NTSB Web Guild currently plays an active role in addressing matters of pressing concern and bringing recommendations to the attention of the IT Management.

The NTSB web manager monitors the Safety Board's presence on the web through the various means noted above and conducts customer usability studies or surveys that may also highlight areas for attention or remedial action. The Web Guild continuously review the requirements in this area as issues arise and will establish working groups or teams as required to provide guidance and ensure compliance. Accordingly, the Safety Board plans to continue use of scanning, inventory, compliance monitoring, and other Web management techniques as well as continued oversight by the Public Affairs and business program managers over content as appropriate to maintain the performance and results in the overall information dissemination process.

Appendix B: Architecture Principles for the US Government

Preamble

These principles support a single Federal Enterprise Architecture to achieve operational excellence for the American public.

The Federal Enterprise Architecture is a mission-focused framework for federal agencies, OMB and Congress to improve government performance. By aligning organizations, business processes, information flows, and technology consistently across and throughout the Federal Government, the FEA builds a blueprint for improving programs.

The Federal Government focuses on citizens

Citizens' needs determine how government functions are defined and delivered. Functions include direct services and regulating society to serve the public.

Rationale

The Federal Government exists to serve the American public who want simpler, faster, better and cheaper access to government services and information.

Implications

- Agencies will design and apply their business processes and services to benefit citizens, even when the services cross lines of business and agency missions.
- The Federal Government offers citizens a single, "unified" face, reducing duplicate, needlessly complex, inconsistent ways of using government services.
- Citizens can access government services through various means.

The Federal Government is a single, unified enterprise

The Federal Government operates as a single enterprise with decision-making flexibility at the agency level.

Rationale

A single enterprise with shared strategic objectives, common governance, integrated management processes and consistent policies improves the implementation of government-wide strategies and the coordination of the delivery of agency citizen services.

Implications

- Government optimizes resource allocations across the enterprise to achieve common goals.
- Government optimizes information across the enterprise to support services and processes.
- Architectural designs integrate services for efficiency and keep autonomy of operations for effectiveness.
- Architectural designs identify and accommodate distinctive (non-homogenous) approaches to maintain important policy objectives.

Federal agencies collaborate with other governments and people

Federal Government agencies, other government entities, and private companies work together using commonly accepted open standards to improve services' quality, consistency, and cost-effectiveness.

Rationale

The Federal Government operates within a larger government ecosystem that includes state, local, foreign governments and the private sector. This operation takes advantage of collaboration while reducing duplication.

Implications

- Requires agencies to strengthen collaborative partnerships with other agencies, state, local and foreign governments and the private sector.
- Requires agencies to adopt agreed-on standards and industry's best practices. The standards must be open and voluntary, not proprietary, and must meet the market's needs.

The federal architecture is mission-driven

Government core mission needs and priorities are the primary drivers for architecture.

Rationale

A business-led architecture is more successful in meeting strategic goals, responding to changing mission needs and serving citizens' expectations.

Implications

- Business-approved architecture is a prerequisite for investment, so CIOs and architects must ask program leaders to say how it should look and work. Architecture is driven by program mission needs and enabling technology.
- Agencies will first seek to optimize business processes, and then use performance standards to define automation requirements.
- Systems and processes will use an architecture that responds quickly to events, including a "push" model for delivering information.
- The Federal Government and agencies will use their enterprise architectures to guide their capital planning, budget and investment decisions.
- Agencies will manage change in government operations with enough security to keep services flowing.
- Government solutions must be agile and flexible to meet business needs.

Security, privacy and protecting information are core government needs

Security, privacy and protecting information are integral to government operations, and are part of the architecture. Government must protect information against unauthorized access, denial of service, and both intentional and accidental modification.

Rationale

Government must protect confidential information to increase public trust and improve the security of its resources.

Implications

- The business context defines security and privacy requirements, which integrate into the entire architecture throughout the business lifecycle.
- Architectures must reflect policies to minimize improper use of data and security violations.
- Government must apply security and privacy consistently and monitor compliance.
- Information security controls need to be clearly defined so cost and risk are balanced and managed.

Information is a national asset

Information is an asset needed by citizens and leveraged across the government to improve performance.

Rationale

A well informed citizenry is necessary to our constitutional democracy. Further, accurate information is critical to effective decision making, improved performance, and accurate reporting.

Implications

- The Federal Government will improve its information sharing environment to better disseminate information to the public.
- This requires Government to identify authoritative sources of high quality information, and agencies to provide access to specified data and information.
- Authoritative data sources may need to be restructured and catalogued for easy dissemination, access and management.
- To realize this principle requires a Federal Government strategy to promote cost effective data sharing with other levels of government.

The federal architecture simplifies government operations

Federal Architecture is designed to reduce complexity and enable integration to the maximum extent possible.

Rationale

Complex processes and systems with tightly coupled modules are difficult to manage, risk failure, are inflexible to changing agency mission needs, and are expensive to maintain. Highly modular, loosely coupled systems and processes take advantage of shared services and reusable components within government and available commercially.

Implications

- This requires loosely coupled software components shared as services and compatible application development.
- Agencies must share their best practices and reusable business and technical components.
- Building and integrating reusable components must become a common development method.

Appendix C: 2007 President's Management Agenda - Standards of Success

Expanded E-Government

GREEN Standards for Success

Agency:

- Has an Enterprise Architecture with a score of 4 in both the "Completion" section and 3 in both the "Use" and "Results" sections;
- Has acceptable business cases for all major systems investments and no business cases on the "management watch list";
- Has demonstrated appropriate planning, execution, and management of major IT investments, using EVM or operational analysis, and has portfolio performance within 10% of cost, schedule, and performance goals;
- Inspector General of Agency Head verifies the effectiveness of the Department-wide IT security remediation process and rates the agency certification and accreditation process as "Satisfactory" or better;
- Has 90% of all IT systems properly secured (certified and accredited); **AND**
- Adheres to the agency-accepted and OMB-approved implementation plan for all of the appropriate E-Gov/Lines of Business/SmartBuy initiatives rather and has transitioned and/or shut down investments duplicating these initiatives in accordance with the OMB-approved implementation plan.

Standard for Success to MAINTAIN GREEN

Agency:

- Has ALL IT systems certified and accredited;
- Has IT systems installed and maintained in accordance with security configurations;
- Has demonstrated for 90% of applicable systems a Privacy Impact Assessment has been conducted and publicly posted; **AND**
- Has demonstrated for 90% of systems with personally identifiable information a system of records has been developed and published.

YELLOW Standards for Success

Agency:

- Has an Enterprise Architecture with a score of 4 in the "Completion" section and 3 in either the "Use" or "Results" sections;
- Has acceptable business cases for more than 50% of its major IT investments;
- Submits security reports to OMB that document consistent security improvement and either:
    - 80% of all IT systems are properly secured; **OR**
    - Inspector General of Agency Head verifies the effectiveness of the Department-wide IT Security Plan of Action and Milestone Remediation Process;
- Has demonstrated appropriate planning, execution, and management of major IT investments, using EVM or operational analysis, and has IT portfolio performance operating within 30% of cost, schedule, and performance goals; **AND**

- Has an up-to-date agency-accepted and OMB-approved implementation plan for all of the appropriate E-Gov/Lines of Business/SmartBuy initiatives rather than creating redundant or agency unique IT projects.

Appendix D: NSTB IT CPIC Procedures

INFORMATION TECHNOLOGY (IT)
CAPITAL PLANNING & INVESTMENT CONTROL (CPIC)

1. BACKGROUND. Information Technology (IT) is integral to the National Transportation Safety Board (NTSB/Safety Board). IT must be effectively managed and used in support of business goals and objectives. An effective IT Governance structure is critical for ensuring enterprises effectively acquire and manage their IT priorities and make IT investment decisions directly in support of their business mission, strategic objectives and goals.

2. PURPOSE AND SCOPE. This document establishes the Safety Board's structure for ensuring that IT investments and expenditures are aligned with Safety Board mission and strategic objectives. Capital Planning and Investment Control (CPIC) is the framework process by which governance of IT is achieved.

3. POLICY. It is the policy of the Safety Board to implement and comply with the requirements of the:

- Information Technology Management Reform Act (ITMRA/Clinger-Cohen),
- Government Performance and Results Act (GPRA),
- Federal Information Security Management Act of 2002 (FISMA), and
- OMB Circulars A-11 and A-130.

4. REFERENCES.

a. The Information Technology Management Reform Act of 1996.
b. Federal Information Security Management Act of 2002.
c. OMB Circular A-11, "Preparation, Submission and Execution of the Budget," updated annually.
d. OMB Circular A-130, "Management of Federal Information Resources," Nov 2002.

5. SUPERSESSION. None.

6. DEFINITIONS.

a. **Capital Planning and Investment Control (CPIC)** is a decision-making process for ensuring IT investments integrate strategic planning, budgeting, procurement, and the management of IT in support of agency missions and business needs. The term comes from the Clinger-Cohen Act of 1996 and generally is used in relationship to IT management issues.

b. **Life Cycle Costs**. The life cycle costs of an asset include all direct and indirect initial costs associated with the acquisition of an asset including planning, procurement and other costs; all periodic or continuing costs associated with the operation and maintenance of the asset; and the decommissioning and disposal costs required to retire the asset. For IT investments, the life cycle can be measured and separated by major version number, meaning that a version 1.x of an IT investment can have a different life

cycle than version 2.x. Life cycle costs include both Development/Modernization /Enhancement (DME) and Steady State (SS) cost components.

c. **Development/Modernization/Enhancement (DME)** means the program cost for new investments, changes or modifications to existing systems to improve capability or performance, changes mandated by the Congress or agency leadership, personnel costs for project (investment) management, and direct support. For Major IT investments, this amount should equal the sum of amounts reported for planning and acquisition plus the associated full time equivalent (FTE) costs reported in the exhibit 300.

d. **Steady State (SS)** means maintenance and operation costs at current capability and performance level including costs for personnel, maintenance of existing information systems, corrective software maintenance, voice and data communications maintenance, and replacement of broken IT equipment. For Major IT investments, this amount should equal the amount reported for maintenance plus the associated FTE costs reported in the Exhibit 300.

e. **Capital Assets.** Structures, equipment and intellectual property, including software, which the Federal Government uses: costing more than $250,000, either individually or aggregately; and have an estimated useful life of two years or more.

f. **Major IT Investments** are those projects that meet at least one of the following OMB-specific criteria (per OMB Circular A-11):

   i. Requires special management attention because of its importance to the mission or function of the agency, a component of the agency or another organization;
   ii. Is for financial management and obligates more than $500,000 annually;
   iii. Has significant program or policy implications;
   iv. Has high executive visibility;
   v. Has high development, operating, or maintenance costs;
   vi. Is defined as "Major" by the agency's capital planning and investment control process; or
   vii. Agency (NTSB) Specific Criteria:
      1. Total life cycle costs (10 year) exceeds $50 million; or
      2. Has an annual budget of $5 million or higher.

g. **Non-Major IT Investments** – Investments that are not Major IT Investments.

h. **Pre-Select Phase** – Key NTSB decision-makers assess each proposed IT investment in terms of how it supports the Safety Boards mission and strategic objectives. Requesting business owners compile information necessary for supporting a proposed investment.

i. **Select Phase** – Investment analyses are conducted and approved that best support the mission of the organization. Investments that are Major IT Investments must be promoted to the Office of Management and Budget (OMB) for review and approval.

j. **Control Phase** – The Safety Board ensures, through timely management oversight, quality control, and executive review, that IT initiatives are developed and executed in a disciplined, well-managed, and consistent manner.

k. **Evaluate Phase** – After the system or investment has been implemented and becomes operational (or after the roll-out of a major sub-component), actual results are compared to expectations to assess investment performance. The goal of Evaluate Phase is to gather lessons learned and identify potential candidates for modification, acceleration, replacement or retirement.

l. **Steady State Phase** – Once an investment has been in place is deemed to have met or exceeded performance goals the natural tendency is to keep the investment in place with minor changes. The role of the steady state review is to ensure that the investment is continuing to return best value for the Safety Board. Items such as advances in technology, functionality provided by a center of excellence, mission changes, etc., should be considered in determining if the investment should be continued, reconstituted in another form, or retired.

m. **New Investment** - The introduction of a completely new capability.

n. **Modified Investment** – The enhancement of a current investment where it is reasonable and/or feasible that the performance increase or change relates to an existing capability. Additionally, "child systems" are considered modifications to existing systems.

7. OBJECTIVES. The Safety Board's primary objectives for IT CPIC are to:

a. provide a framework for making NTSB IT decisions and to ensure clear alignment between IT initiatives and NTSB strategic goals and objectives;
b. establish and implement guidelines for reviewing and assessing projects to address identified requirements, and for selecting and prioritizing viable projects for funding;
c. provide a structure and process for NTSB executive and managerial involvement in IT decision-making, project oversight, and review; and
d. resolve IT issues of enterprise importance.

8. IT GOVERNANCE STRUCTURE.

Table 1: New NTSB Investment Thresholds and Approval Levels specify the NTSB strategy for approving new IT investments and the level(s) of approval required. (see Section 10 – Implementation of CPIC Phases)

Table 2: Modified NTSB Investment Thresholds and Approval Levels specify the NTSB strategy for approving modifications to IT investments and the level(s) of approval required. (see Section 10 – Implementation of CPIC Phases)

9. ROLES AND RESPONSIBILITES. The roles and responsibilities for various individuals and groups are defined below:

a. **NTSB Business Owner.** This is the individual who establishes the requirement for IT services and is responsible for development of supporting documentation, as required for the investment.
b. **NTSB Business Owner's Management.** This is a manager in the chain of command of the requesting NTSB Business Owner. See Tables 1 and 2 for additional detail on manager approval levels.

c. **Chief Information Officer Staff.** This staff is responsible for collecting and maintaining financial information related to IT investments.
d. **OCIO Project Manager.** This is the individual assigned to manage the development of the approved investment.
e. **NTSB IT Investment Executive Committee.** Is comprised of the Managing Director (Chair), Deputy Managing Director, Chief Financial Officer, Chief Information Officer, and General Counsel.

10. IMPLEMENTATION OF CPIC PHASES.

a. **Pre-Select Phase**. During this phase, the NTSB Business Owner documents the business need for the investment and describes its anticipated alignment with NTSB, E-Gov and the President's Management Agenda (PMA) strategic goals. The NTSB Business Owner obtains management concurrence from within the Business Owner's functional area. Documentation requirements are defined in Table 1 and 2, depending on if the proposed investment is new or a modification to an existing investment. *Note: Pre-Select concurrence is not approval to begin work or expend funds; it simply signifies management's agreement with a requested activity.*

The investment Business Owner is responsible for providing the information necessary for an investment to be promoted for review in the Select Phase.

The following documentation and approval levels are in effect at the Safety Board for new IT investments Table 1 and modifications to IT investments Table 2:

Table 1: New NTSB Investment Thresholds and Approval Levels

Investment Type	Threshold	Documentation Required	NTSB Approval	OMB Approval
New Major IT Investment	OMB and NTSB established thresholds	Request for Service via Heat System OMB 53 and 300	NTSB Executive Committee	Requires submission to OMB for Funds Appropriation
New Non-Major IT Investment	OMB and NTSB established thresholds	Request for Service via Heat System NTSB Business Case For Non-Major IT Capital Investment (see Appendix D)	CIO and requesting Office Director (if applicable). Include NTSB CFO if additional funding is required Notify NTSB Managing Director if expenditure will exceed $250K.	None

Table 2: Modified NTSB Investment Thresholds and Approval Levels				
Investment Type	**Threshold**	**Documentation Required**	**NTSB Approval**	**OMB Approval**
Modified Major IT Investment	OMB and NTSB established thresholds	Request for Service via Heat System Updates to OMB 300 as required	NTSB Executive Committee	Requires submission to OMB for Funds Appropriation
Modified Non-Major IT Investment	OMB and NTSB established thresholds	Request for Service via Heat System NTSB Business Case For Non-Major IT Capital Investment (see Appendix D)	Division Manager level (GS-15) in both the OCIO and requesting Office Director (if applicable). Include NTSB CIO and CFO approval if implementation involves purchasing a Capital Asset. Notify NTSB Managing Director if expenditure will exceed $250k.	None

b. **Select Phase**. In the Select Phase, the Safety Board ensures that only IT investment activity that best support the Safety Board's mission, investment principles and technical approaches are chosen and prepared for success (i.e., have a good project manager, are analyzing risks, etc.). Prior to entering the Select Phase, IT investments must have obtained management concurrence from within the NTSB Business Owner's functional area. *Note: the Office of the Chief Information Officer may reclassify a request initially designated as "new" to "modified" and vice-versa depending on the parameters of the request and technologies involved.*

The process for the Select Phase provides a framework for selection of investments in an objective and consistent manner; reviewed at the appropriate level of authority and either approved or disapproved. The Select process applies to new (including significant changes thereto) investments seeking funding. Approval of investments depends on:

- A broad understanding of the environment and the Safety Board's need in identifying which investments produce the maximum return.
- Considers public and Congressional interest in IT investment decisions.
- Determines which investments are of particular interest to the Safety Board through its strategic goals and policies, the Administration and Congress.
- Considers Enterprise Architecture and e-Government.
- Considers the impacts of not selecting the investment.
- Evaluates mandatory investments in terms of the overall portfolio and whether the investment must be made now or in the future.

The proposed IT investment is reviewed and is either:

- Returned for more data analysis
- Approved
- Denied

Approval of an investment is signified when all of the required documents per Tables 1 and 2 have been signed. However, execution of this plan (via the Control Phase) is contingent upon the availability of funding and resources.

c. **Control Phase.** The objective of Control is to ensure, through timely oversight, quality control, and executive review, that IT investments are managed in a disciplined and consistent manner. The Control Phase can also be thought of as the acquisition/development process where a capability is bought and/or built. An assigned OCIO Project Manager typically executes the Control Phase once funding and resources become available. Adherence to developmental processes, oversight, security, testing, documentation and training are done during the Control Phase.

The Control Phase is also characterized by conducting reviews which focus on ensuring that projected benefits are being realized, cost, schedule and performance goals are being met, risks are minimized and managed, and the investment continues to meet strategic needs. These reviews promote the delivery of quality products and result in investments that are completed within scope, on time, and within budget.

The Control Phase usually concludes with a decision to place the system in a production environment commensurate with proper security certification and accreditation approvals in accordance with the Federal Information Security Management Act (FISMA).

As an IT investment exits the Pre-Select Phase, the OCIO Project Manager (PM) establishes milestones against which performance is measured throughout the Control Phase. During Control, the PM gathers cost and schedule data, updates performance measures, revisits risks and PM data, and updates the security status. The ability to adequately monitor IT investments relies heavily on effective project management. Project Managers are required to certify the accuracy of the quarterly Earned Value management (EVM) (EVM required for major IT investments only) and performance data.

d. **Evaluate Phase.** Is the phase in which the agency will conduct its Post Implementation Review (PIR). The purpose of the PIR is to capture and document lessons learned from the development process though the implementation of the system. The Safety Board will accomplish this review by completing an assessment that compares actual to expected results after an investment is fully implemented, or after a Major functionality is rolled out. Findings, recommendations and lessons learned are shared in a manner that preserves the integrity of the lessons learned without revealing the source investment. The Post Implementation Review (PIR) process is required for all IT investments as they exit the acquisition (build/buy) phase and move into operations and maintenance (O&M) of the life cycle. The PIR targets new investments that have been placed into O&M within the past 6-18 months. The PIR will be conducted by the OCIO PM and the Business Owner with oversight by the NTSB IT Investment Executive Committee.

e. **Steady State Phase.** An annual process conducted in the first quarter of the fiscal year to examine IT investments that are in their 2nd or greater year of operation. It is an Operational Analysis (OA) of the system. The purpose of the OA is to identify investments that are potential candidates for modification, acceleration, replacement or retirement. The Safety Board can fulfill this purpose by assessing the ability of a mature investment to continue meeting user needs and performance goals based upon the performance of the system relative to the cost of replacing the system with a more modern or alternate solution.

Appendix E: Non-Major IT Business Case Template

BUSINESS CASE FOR NON-MAJOR IT CAPITAL INVESTMENTS
(Project Name)

AMOUNT REQUIRED: (dollar amount)
(Must include all allocated costs including security and installation)

DESCRIPTION OF INVESTMENT: (brief description of investment and why it is being made)

PROGRAM/BUSINESS REQUIREMENT SUPPORTED: (select from options below)

___ Aviation ___ Highway ___ Marine ___ Railroad, Pipeline & Hazardous Materials
___ Safety Recommendations & Communication ___ Research & Engineering
___ Administrative (Specify Office: _____)

TYPE OF INVESTMENT: (select from options below)

___ New Technology Investment
___ Mandate Requirement Support
___ Modification to Existing Investment
___ Reengineering, Business Process Change

STRATEGIC GOALS SUPPORTED: (select one or more applicable goals and describe how the investment supports the goal)

_____ **Strategic Goal #1** – Accomplish Objective Investigations of Transportation Accidents to Identify Issues and Actions that Improve Transportation Safety

_____ **Strategic Goal #2** – Increase our Impact on the Safety of the Transportation System

_____ **Strategic Goal #3** – Outstanding Stewardship of Resources

_____ **Strategic Goal #4** – Organizational Excellence

PERFORMANCE MEASURES: (list and describe qualitative and quantitative performance measures (single measure for mandate, 3 – 5 measures for non-mandate).

COST/BENEFIT ANALYSIS: (value of quantitative and qualitative benefits, ROI point, etc.)

PROJECT MANAGEMENT

Project Sponsor(s): (office directors)

OCIO Project Manager:

Business Owner: (manager from requesting office)

RISK – (list the most significant risks associated with this project, and the plans to mitigate such risks: (risk categories: schedule, costs (both initial and life cycle), technical obsolescence, feasibility, reliability of systems, interoperability, surety (asset protection) considerations, risk of creating a monopoly for future procurements, capability of agency to manage the project, overall risk of project failure, organizational and change management, business, data/info, technology, strategic, security, privacy, and project resources))

STAKEHOLDERS BENEFITED: (identify internal and external stakeholders, which stakeholders receive most benefit.)

IT COMPLIANCE – Is this project in compliance with the following:

Enterprise Architecture Y__ N__ N/A__ IT Security Requirements Y__ N__ N/A__
IT Privacy Requirements Y__ N__ N/A__ C&A Requirements Y__ N__ N/A__

How is compliance addressed?

If the answer is NO for any of the above, provide a brief explanation as to why compliance has not been met. (For example, if IT Certification & Accreditation Requirements are not met, what IT Security Requirements have been addressed, such as Risk Assessment, Security Plan, etc.?)

Approval by:

Sponsors:

_____ _____
Business Office Director **Date**

_____ _____
Chief Information Officer **Date**

CFO: (if additional funding is required)

_____ _____
Chief Financial Officer **Date**

Managing Director: (as required by dollar threshold)

_____ _____
Managing Director **Date**