Office of the Chief Information Officer

IT Strategic Plan

FY 2007 – 2011

June 6, 2007

Draft Document Revision History

Version No.	Date	Description	Section	Author
15	June 6, 2007	Added: ▪ Asset Management ▪ Mobile device refresh cycle ▪ Information Security Policies, Standards, and Procedures ▪ Security Operations ▪ Security Training and Awareness	 3.1.6 3.3.1 3.4.1 3.4.3 3.4.7	David J. Cole

Message from the Chief Information Officer

June 2007

Upon joining the OPIC team in November, one of my first activities was to assess the Corporation's Information Technology capabilities. I performed this assessment from two points of view; internal to OCIO, and external with the OPIC users we support.

Internally, I looked at our applications portfolio, technology infrastructure, the enterprise architecture, and the way we govern and manage our IT resources, projects, and contracts. Externally, I looked at the perception of the services and support our end users receive from OCIO resources.

In meeting with those responsible for managing OPIC's lines of business and efforts at fulfilling our mission, I found that the overall perception of the support and services provided by the OCIO organization is good and has been improving.

In examining the current state of OPIC's technology infrastructure, information systems, and information technology (IT) management practices, I found several areas that could benefit from improvement. In order to correct these deficiencies, I requested that OCIO staff on both the operations and business solutions sides develop strategies to overcome the deficiencies and to generate plans of action and milestones (POA&M) to address the most critical shortcomings that represent the greatest risk to the sustainability of OPIC's business systems.

These strategies, along with other longer-term goals and objectives, are represented in this IT Strategic Plan. Over the past few months, the OCIO staff has been working to implement a number of these strategies and solutions. Over the next several months, we expect to see the completion of many of these efforts that will provide OPIC with more reliable systems, provide OPIC users with better system and data integrity, and will improve performance.

But these first few initiatives are just the start. I plan to implement a process of continuous improvement for OPIC's systems infrastructure and business systems that will maintain an improved level of service to the OCIO's business users. Many of these strategies are reflected in this plan, but there are more to be developed. This IT Strategic Plan is a living document that will be refreshed on a regular basis. With each update of the plan, we will introduce new strategies that employ new technologies and systems that respond to the business needs of the OPIC community.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Over the past few decades, Information Technology (IT) has changed dramatically. IT continues to rapidly change the way in which both industry and the federal government conduct their business. It is for this reason that attention to IT planning becomes critical to the achievement of an organization's mission, in terms of both business performance and management. As agencies' IT becomes increasingly complex, processes must be put into place to increase efficiency and reduce the cost of maintaining IT.

With regard to our IT strategic planning, the OCIO focused in the following areas:

- IT Governance and Program Management;
- Enterprise Business Solutions;
- Technology Improvement;
- Information Security; and,
- IT Operations.

The success of the OCIO depends on one core requirement, to provide the information technology leadership and governance that enables the programs and operations of OPIC to deliver their respective missions in an efficient, effective, and secure manner through the use of information technology solutions and services.

The OCIO's primary guiding principles which direct decision-making at different levels of the OCIO organization are the support of OPIC's mission by delivering information management solutions in a professional, effective, and prompt manner, and ensuring that all IT goals and investments are customer-focused, results-oriented, and cost-effective.

The strategies presented in this IT Strategic Plan can be placed in two categories; those that must be met in order to achieve our current mission, and those that need to be met in order to improve the way we meet our mission

Mission Achievement:

- Human Capital Management
- APPX Replacement
- Enterprise Web Portal
- Infrastructure Refreshment
- Information Assurance
- Continuity of Operations
- Certification and Accreditation
- Customer Service
- Performance Management

Mission Improvement:

- Develop an Enterprise Architecture
- Develop an IT Strategic Plan
- Provide oversight for IT policies
- Capital Planning
- Program Management Office
- T24 Development and Deployment
- Collaboration Toolset
- Interoperable Solutions
- Infrastructure Improvement

These strategies are presented in detail in Section 3 of this plan.

1.0 INTRODUCTION

This Information Technology Strategic Plan (ITSP) focuses on areas of the OPIC picture that are important to the ongoing success of OPIC. The topics included in this document cover a wide spectrum of interests, but together they provide an overview of the OPIC Strategic Plan for meeting the demands of an information- and technology-rich transformational environment.

This ITSP provides the roadmap for the OCIO organization's way forward in providing technological support to the OPIC lines of business. It describes our current IT environment, and addresses our goals and objectives to maintain and improve upon the current level of support that OCIO provides.

1.1 Current Environment

The OCIO is currently comprised of two organizations: Technical Services and Business Information Systems. The Technical Services group is responsible for operating and maintaining the IT infrastructure needed to deliver a variety of business applications to OPIC users. This includes the networks, hardware, software, and connectivity for all users' access, both locally and remotely, to the business applications needed to carry out their duties. The Business Information Systems group is responsible for business-specific applications OPIC users have as tools to help them carry out their assigned duties in support of the OPIC mission. An organization chart depicting the functional areas of the OCIO is provided in Figure 1-1, below.

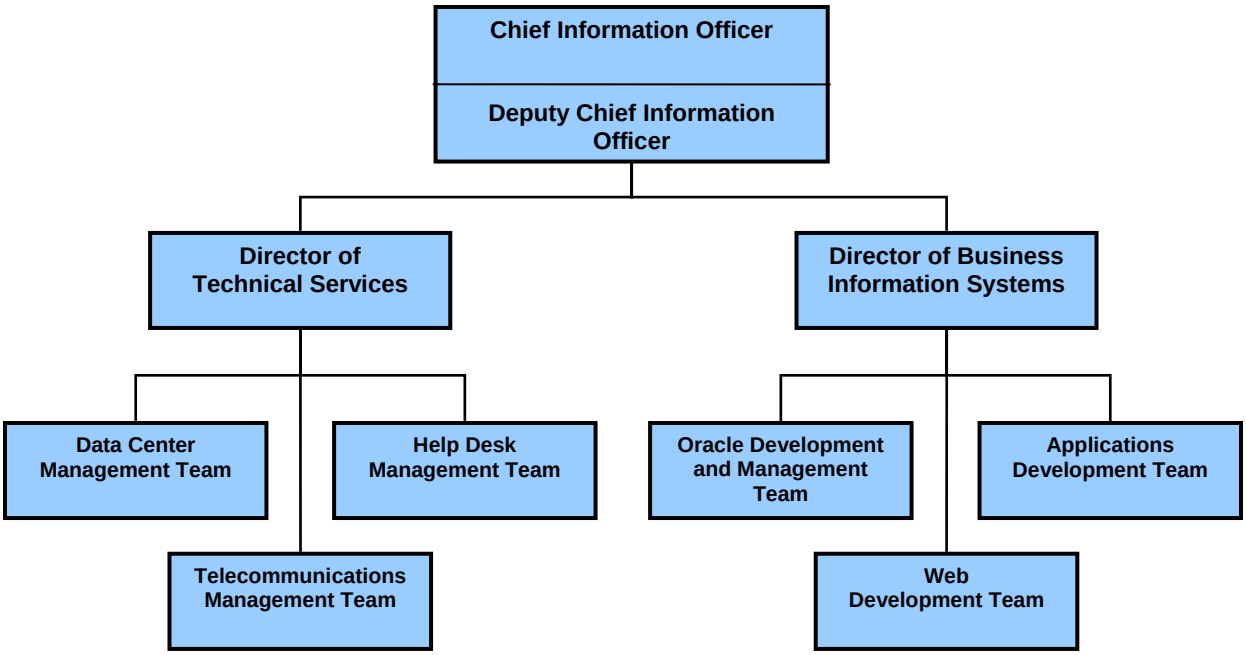

Figure 1-1: OCIO Functional Organization Chart

Functional Area	Responsibility
Technical Services	
Data Center Team (DCT)	Ensures continuous, reliable operation of all local and wide-area networks, connectivity to external networks such as the internet, the Department of the Interior (DOI) payroll system, and the various applications, data, and communications hardware needed to provision the business systems to OPIC users.
Help Desk	Provides support to OPIC users for their desktop and laptop workstations, locally run applications, and remote access services.
Telecommunications Services	Operates and maintains the voice telephone systems for OPIC users, both wired and wireless.
Business Information Systems	
Oracle Development and Management Team	Implements financial applications via the Oracle Government Financials (OGF) application.
Applications Development Team	Develops and maintains financial systems using the APPX system and the development of the T24 applications.
Web Development Team	Responsible for the OPIC enterprise web portal and the OPIC Intranet.

1.2 Opportunities and Challenges

While the current OCIO organization provides an acceptable level of service and support to the OPIC user community, there are areas with room for improvement that have the potential to greatly increase the level of service and support, as well as enhance the reliability of OPIC's technology infrastructure. Among these areas are:

- Business applications software – OPIC's current portfolio of financial business applications needs updating to bring it into line with the latest releases of the vendors' packages. By upgrading these packages and consolidating some of them to a suite system, we can ensure the reliability of the performance of the applications with the required support from the software vendors.

- Technology refreshment – at both the data center server and the desktop level, much of OPIC's hardware resources are nearing the end of their useful lives. By implementing a

technology refreshment program, we can ensure that OPIC's users have up-to-date hardware resources at their disposal to enhance their work experience.

- Network redundancy – the availability and reliability of technology resources will be greatly improved through the implementation of redundant network connectivity at the data center server level.

- Program management – the chances of success of OCIO development, implementation, installation, and service delivery programs will be greatly improved through the development of project management processes, tools, and techniques that subscribe to industry-accepted standards.

- Information security – the protection and integrity of OPIC financial and privacy data can be ensured through the implementation of a rigorous information security program.

Taken together, these areas provide opportunities for improving the quality of technology support and service that the OCIO can deliver to the OPIC user community and enhance the OPIC mission.

1.3 OCIO Strategic Planning Process for 2007

The OCIO followed a very basic process in developing this ITSP. The process was initiated through obtaining a thorough understanding of the requirements and needs of OPIC's lines of business, and then identified goals that the OCIO might achieve in order to best fulfill those requirements. Since this is our first ITSP, we will closely monitor our progress against the goals and objectives outlined in this plan, and regularly update the ITSP to reflect changes in mission, scope, goals and objectives, and technology. The basic strategic planning process is depicted in the following figure.

Figure 1-2: IT Strategic Planning Process

Identify Purpose – This is the statement that describes why OCIO exists, i.e., its basic purpose. The mission statement describes which OPIC needs are intended to be met and with what services. This mission statement may evolve somewhat over time, as the mission of OPIC changes.

Select Goals – The OCIO goals are general statements identifying what needs to be accomplished to meet our mission, and address major issues facing OPIC in general, and the OCIO specifically.

Identify Objectives – The objectives are the means to meeting the stated goals. These objectives will be the agent of change for the OCIO organization, and may change often as each set of objectives are met and new ones identified by closely examining the external and internal environments of the Corporation.

Define Actions – These are the specific activities that OCIO will undertake, or is currently undertaking, to ensure the effective implementation of each strategy. The actions, per se, are not detailed in the ITSP, but are contained in related project plans for each of the OCIO initiatives.

Monitor and Update the Plan – Using the performance measures identified for each of the goals, the OCIO will monitor progress against the ITSP, and update it when necessitated by a changing environment. Perhaps the most important indicator of our success is positive feedback from our OPIC customers in how well we are meeting their needs and requirements.

The ITSP is a living document, and the ITSP process is a continuous effort that will help the OCIO maintain our vision in meeting the expectations of the OPIC user community.

2.0 IT MISSION, VISION, AND GUIDING PRINCIPLES

OCIO provides the information technology leadership and governance that enables the programs and operations of OPIC to deliver their respective missions in an efficient, effective, and secure manner through the use of information technology solutions and services.

We envision IT at OPIC as having a proactive role, not only as a business partner, but also as an integral part of the Corporation's overall business. Our focus on an integrated enterprise approach will leverage benefits for OPIC offices and improve mission performance. Implementing IT as an integrated and vital component within all of OPIC's lines of business is also a means of business transformation. It supports meeting the Corporation's mission and goals through developing modernization blueprints, implementing data sharing opportunities, and providing enterprise integration services.

The following guiding principles direct decision-making at different levels of the OCIO organization. These principles form the common values embraced and demonstrated by the OCIO, and provide broad guidance for IT planning and architecture decisions into the future:

- Support OPIC's mission by delivering information management solutions in a professional, effective, and prompt manner;
- Use the Enterprise Architecture (EA) to make informed business decisions;
- Ensure that all IT goals and investments are customer-focused, results-oriented, and cost-effective;
- Provide a high-quality, innovative, and secure IT infrastructure that proactively assures confidentiality, integrity, and accessibility, and protects OPIC data and information systems; and,
- Attract, develop, and retain a competent, creative, and highly motivated workforce.

The OCIO support of the OPIC mission was paramount in developing the ITSP. IT exists to enable OPIC's mission and programs, and to support the accompanying business and performance requirements. IT can provide breakthrough opportunities for accomplishing business requirements better, faster, and/or cheaper. Conversely, opportunities for restructuring and streamlining agency programs and business functions often provide the basis for rethinking IT strategy, goals, and priorities. The OPIC Strategic Goals and Objectives, as presented in the OPIC Strategic Plan, include:

- Goal #1: Maximize OPIC's Impact on Economic Development;
- Goal #2: Support U.S. Foreign Policy;
- Goal #3: Mobilize Investments by Small and Medium Enterprises; and,
- Goal #4: Efficiently Serve Investors.

Based on our understanding of the OPIC Strategic Goals and Objectives, the OCIO developed the IT Strategic Goals and Objectives to assist us in providing the required levels of support and service to OPIC users. The OCIO Strategic Goals include:

- Goal #1: IT Governance and Program Management;
- Goal #2: Enterprise Business Solutions;
- Goal #3: Technology Improvement;
- Goal #4: Information Security; and,
- Goal #5: IT Operations.

In order to ensure that the IT Strategic Goals and Objectives align with those of the Corporation, we developed a cross-walk of the two. The results of that cross-walk are presented in the following table which provides a brief description of how each of the IT Strategic Goals meets the OPIC Strategic Goals.

OPIC Strategic Goals / **OCIO Strategic Goals**	**Goal #1: Maximize OPIC's Impact on Economic Development**	**Goal #2: Support U.S. Foreign Policy**	**Goal #3: Mobilize Investments by Small and Medium Enterprises**	**Goal #4: Efficiently Serve Investors**
Goal #1: IT Governance and Program Management	Provides the management discipline to ensure that OCIO projects are fiscally responsible and meet the business needs of the OPIC lines of business.			
Goal #2: Enterprise Business Solutions	Provides the financial, management, information sharing, and collaboration tools needed to meet OPIC's Strategic Goals.			
Goal #3: Technology Improvement	Ensures that the OPIC user community has the advantage of the most current technologies to help them perform their duties to meet the OPIC mission.			
Goal #4: Information Security	Protects the financial and project information needed to carry out the OPIC mission.			
Goal #5: IT Operations	Provides the technology infrastructure and support to OPIC users.			

Table 2-3: Strategic Goals Matrix

Finally, we categorized the IT Strategic Objectives into two groups; those that help us achieve our current mission and those that will help us improve upon how well we can assist the Corporation in meeting its mission, goals, and objectives.

2.1 Mission Achievement Strategic Objectives

The following OCIO strategic objectives fall into the area of objectives that must be met in order to achieve our current mission:

- Human Capital Management
- APPX Replacement
- Enterprise Web Portal
- Infrastructure Refreshment
- Information Assurance
- Continuity of Operations
- Certification and Accreditation
- Customer Service
- Performance Management

2.2 Mission Improvement Strategic Objectives

The following OCIO strategic objectives fall into the realm of objectives that need to be met in order to improve the way we meet our mission:

- Develop an Enterprise Architecture
- Develop an IT Strategic Plan
- Provide oversight for information technology and information management policies
- Capital Planning and Investment Control
- Program Management Office
- T24 Development and Deployment
- Collaboration Toolset
- Interoperable Solutions
- Infrastructure Improvement

The IT Strategic Goals and Objectives are presented in detail in the following section.

3.0 IT STRATEGIC PLAN GOALS

The OCIO has identified objectives within five strategic goals:

1) IT Governance and Program Management;
2) Enterprise Business Solutions;
3) Technology Improvement;
4) Information Security; and,
5) IT Operations.

The following sections of this document provide the details of how the OCIO plans to meet these strategic objectives.

3.1 IT Governance and Program Management Goals

OPIC will face many challenges in the years to come. It has become clear that resources, including funding and people, are limited, so it is vital to make smart investments, integrate architectures, ensure secure IT environments, ensure an adequate IT workforce to meet these challenges, and leverage resources through enterprise solutions and increased partnerships. Our ultimate commitment is to sustain and improve performance within our mission areas and guarantee efficient and effective customer-oriented business operations. We want to ensure success through viable goals and performance measures that are applied to a value chain that moves from effective management of Inputs (i.e., investment in IT resources, and maintenance of effective IT governance and control mechanisms) through the Work processes (implementation of procedures to meet rigorous standards to supply the targeted services or systems required by our customers) to accountable Results that provide successful outcomes supporting our mission. These results ultimately determine if our processes and structures can deliver the "bottom line." Meeting these challenges requires new thinking and new ways of doing business; and it requires focus: Are we fulfilling our mission? Are we delivering anticipated outcomes? Are we efficient in how we manage our programs? How do we know? Can the public review our progress?

3.1.1 Enterprise Architecture

The OCIO recognizes that the OPIC Enterprise Architecture (EA) is much more than a static document produced to meet regulatory requirements. Properly positioned and utilized, the EA is first and foremost a management and governance tool.

The EA provides a comprehensive view into the various layers of OPIC. The foundation of the EA is made up of the Federal Enterprise Architecture Framework (FEAF) layers. These layers include the Business Reference Model, Applications Reference Model, Data Reference Model, Technical Reference Model, and Performance Reference Model. These layers are further categorized by domains. There are: external portions of the architecture (usually national or federal); common/enterprise OPIC-wide portions; and organizational portions. The FEAF is represented in the following figure.

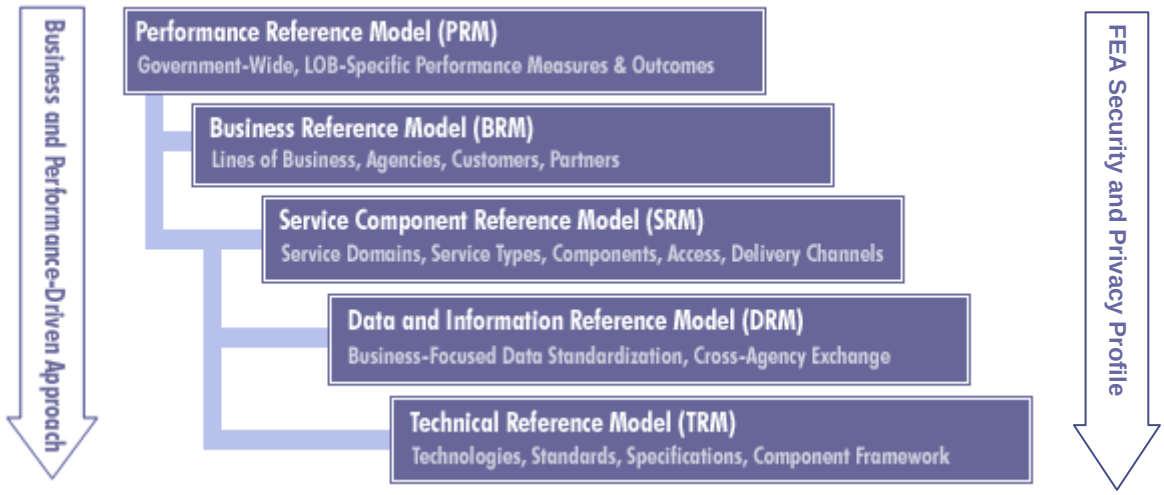

Figure 3-1: Federal Enterprise Architecture Framework

Alignment of IT resources to the business requirements of OPIC is derived from addressing both business and technology models and establishing clear linkage between business strategies and enabling technology. The importance of the EA lies in its ability to highlight the impact a business change may have on the underlying technologies, and vice versa. As such, the EA can be used to predict the impact of both IT and business decisions. EA Program emphasis is on investment support systems, security, and e-Government projects. The EA can also be used to measure progress on attaining business and technology performance goals, as required by the Federal Enterprise Architecture (FEA) Performance Reference Model. The OPIC EA will go deeper and become integrated with the Corporation's strategic planning, CPIC process, software development, and COTS/ GOTS evaluation and selection processes.

To position the EA to be used as a management tool, OCIO will:

- Define and implement an EA action plan to improve the maturity level of the architecture discipline within OPIC;
- Establish EA configuration controls and strategies;
- Identify and recommend changes regarding new enterprise-wide standards;
- Integrate capital planning and EA; and,
- Ensure transition plans are aligned with changing business needs and strategic priorities.

Along with this IT Strategic Plan, the EA becomes the direction for all IT initiatives needed to meet OPIC mission’s technology needs.

3.1.2 Strategic Planning

Strategic planning is an organization's process of defining its strategy, or direction, and making decisions on allocating its resources to pursue this strategy, including its capital and people.

Looking ahead is what makes planning strategic. OPIC's IT strategic planning effort started with a single goal: Imagine the desired future state of OPIC. With that vision, the OCIO was then able to analyze the present state, compare the two to identify gaps, and start to draw a road map for closing those gaps and getting the Corporation to the goal. Project prioritization, risk analysis, and an analysis of the likelihood of changes in technology were also considered in the strategic-planning process.

While there are many approaches to strategic planning, the OCIO followed a typical three-step process:

1) Evaluate the Situation - evaluate the current situation and how it came about.

2) Determine the Target - define goals and/or objectives.

3) Define the Path - map a possible route to the goals/objectives.

The end result of that process is this OPIC IT Strategic Plan, containing directions for each of the five strategic IT objectives.

3.1.3 Policy Oversight

In order to ensure that computer systems are used in an effective and productive way, it is important that the owners, operators, and users of these systems have a clear understanding of acceptable standards of use. Such an understanding can be gained through an established set of OPIC technology policies.

The OCIO has formulated, and will continuously review, revise and augment, policies governing the management of all technology resources throughout the Corporation, establish processes and procedures that carry out these policies, and provide oversight and review on the implementation of these policies, processes, and procedures. The OCIO will also assist in the preparation of OPIC positions on proposed legislation or proposed Government-wide policies affecting IT governance, and represent the Corporation in interagency technology councils. OCIO will develop and maintain the OPIC training and development program, and provide management oversight across the Corporation for implementation of these policies, processes, and procedures. An example of OPIC training includes the Information Security training that is given to all new employees and contractors.

3.1.4 Capital Planning

The creation of an IT capital planning and investment control process is essential to the proper management of IT investments. IT capital planning is a rigorous process for planning, selecting, controlling, and evaluating IT investments. It engrains proper project management philosophies to assist project managers in staying on target with regard to cost and schedule performance.

Additionally, it ensures that procedures are implemented to identify, monitor, and mitigate risks that could potentially affect project performance. An overview of the OCIO capital planning process is presented in the following figure.

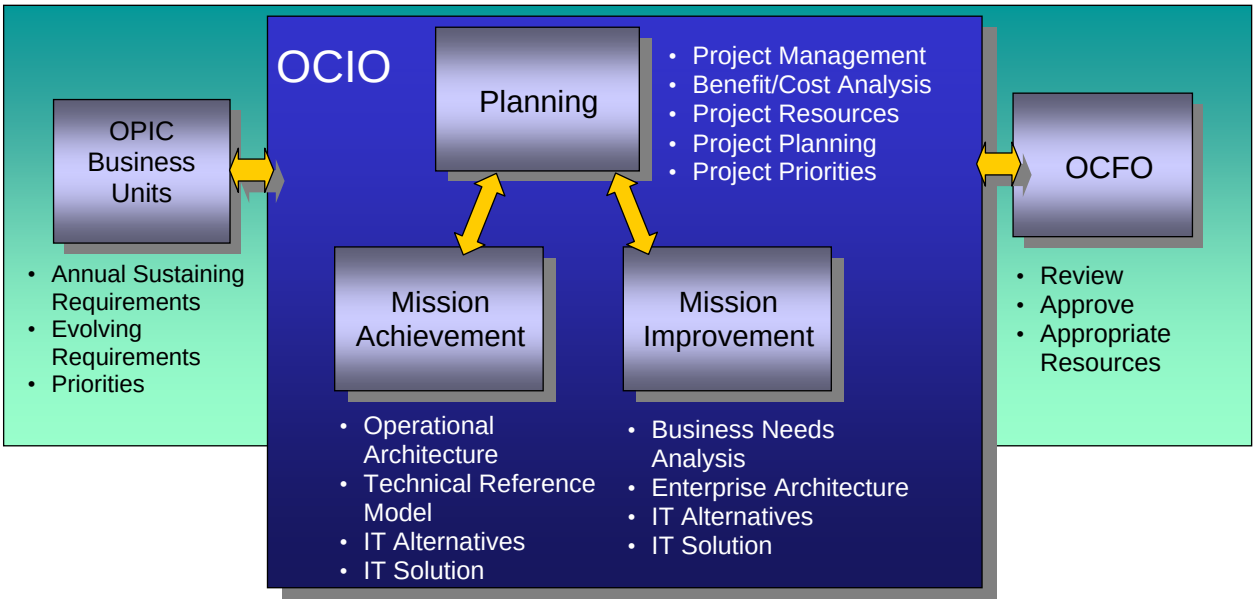

Figure 3-2: OCIO Capital Planning Process Overview

To initiate the annual process, each OPIC line of business (LOB) identifies its technology resource requirements for the coming fiscal year. These requirements are forwarded to OCIO as part of the annual budget process. The OCIO reviews the requirements and the programs they represent to determine whether the requirements are still valid and the programs are still consistent with the overall OPIC IT strategies and architecture. OCIO then consolidates all of the LOB requirements and allocates the appropriate budget amounts to each of the programs as part of the annual IT spend plan. The allocations are presented to the OCFO for review and approval, and where necessary, prioritization of the requirements and resources.

3.1.5 Program Management Office

The OCIO will implement a Program Management Office (PMO). The objective of the PMO is to deliver strategic IT projects with more consistency and efficiency. The PMO will rely on three metric areas to determine its effectiveness: (1) accuracy of cost estimates, (2) accuracy of schedule estimates, and (3) project stakeholder satisfaction.

Responsibilities of PMOs will range from providing a clearinghouse of project management best practices to conducting formal portfolio management reviews, but the management of the

individual IT projects will continue to lie with the project managers in each section. The responsibilities of the PMO will include:

- Provide project management guidance to project managers in each OCIO section.
- Develop and implement a consistent and standardized project management process and methodology. Methodology refers to the processes, procedures, templates, best practices, standards, guidelines, policies, etc., that project managers use to perform certain aspects of work. The methodology provides the framework that your project managers use to manage the work.
- Conduct training programs. Training is one of the premiere services offered by PMOs and involves putting classes together to create an overall project management curriculum. The curriculum can include internal classes, vendor classes, computer based training, etc.
- Advise employees about best practices through internal consulting and mentoring. Mentoring refers to working with individual project managers or project teams to transfer knowledge and teach new skills. Mentoring is different than training in that training implies a formal teacher-pupil relationship and the formal instruction of material.
- Select and maintain project management tools for use by OCIO project managers in each section.
- Establish portfolio management processes to manage multiple projects that are related, such as infrastructure technologies, desktop applications, etc., and allocate resources accordingly.
- Implement common roll-up reporting on the state of all the projects being executed within the OCIO. This service will also extend to keeping metrics on historical projects to the successful execution of projects over time. The PMO will also track the backlog of projects that have not yet begun to provide OCIO management with a complete, portfolio-wide view of all active, pending, and historical projects.
- The PMO will perform periodic project audits. Project audits are one way for the PMO to validate that the project teams are utilizing the appropriate project management processes.
- Develop a project management repository. One of the value propositions for deploying common project management processes is the ability to reuse processes, procedures, templates, etc. This reuse also extends to the level of being able to reuse specific documentation from prior projects. The PMO will establish and manage a document repository to facilitate process and document reuse.

Overall, the PMO will help ensure that the OCIO can deliver its infrastructure, technology, and business applications projects on time, within budget, and to the satisfaction of the OPIC community.

3.1.6 Asset Management

Asset management involves the entire organization and is a cross-functional task. Asset management is a process that involves tracking information about agency assets, including purchase dates, maintenance, software licensing and distribution, auditing, and change management through the asset life cycle. IT asset categories include: hardware, software, mobile and telecommunication devices. The OCIO is responsible for ensuring the establishment of an effective IT asset management tool that will reduce government waste, make more efficient use of warranties and maintenance, reduce legal exposure for or over-purchase of software licenses, optimize equipment use, strengthen internal controls and increase the overall efficiency of helpdesk operations.

The OCIO is in the process of implementing an Asset Management System (AMS) and the associated policies, procedures and processes.

3.1.7 Human Capital Management

To achieve the overall goals of the OPIC IT Strategic Plan, the OCIO must work in concert with other OPIC Offices and its contractors to ensure that the IT workforce has the knowledge, skills, and abilities to make those goals a reality.

Key to the success of this goal is the development of an IT Human Capital Management Plan. This plan will outline the goals, objectives, and timelines to ensure consistency in individual skill levels, with special emphasis on customer service and service delivery. The IT Human Capital Management Plan will focus primarily on these areas:

- Strategic alignment/human capital planning;
- Workforce planning and deployment;
- Accountability system;
- Talent management; and,
- Leadership development and succession planning.

Although the OCIO will continue to outsource delivery of some IT services, those services will always be managed by OPIC federal employees. In order to execute those management responsibilities, OCIO is working diligently to ensure that OPIC employees with management and contractual oversight duties are well trained and well prepared to execute those duties. Creating clear direction, efficiency, timely response, and quality outcomes requires project managers who are agile -- adept at change. The OCIO will seek certification of OPIC program managers by the Project Management Institute (PMI), the world's leading association for the project management profession. It administers a globally recognized, rigorous educational, and/or professional experience and examination-based professional credentialing program.

The OCIO will develop a plan to ensure a group of employees is targeted each year to attend PMI training so that succession planning in the area of project management does not become an issue. While this is a positive step forward, leadership is committed to ensuring that all

employees have a project management mentality in terms of completing projects on time and within budget. Therefore, the OPIC IT employees will be coached on Earned Value Management (EVM) and the Clinger-Cohen Act project management regulations, as well as the ramifications that a missed project deadline or cost overrun has on other projects in the IT portfolio. Furthermore, the PMI's Organizational Project Management Maturity Model (OPM3) will be considered for utilization for assessment and guidance on prioritizing and planning increased maturity in this area.

The requirement for technical and effective Contracting Officer's Technical Representatives (COTRs) is ever increasing in the Government workplace. As the OCIO outsourcing increases, the requirement for highly trained COTRs increases to ensure a fair and equitable contract management program exists to produce efficient resource investments.

3.1.8 Performance Measures

The following represents the performance measures for the IT Governance and Program Management Goals:

- On an annual basis, ensure the OPIC IT Strategic Plan is aligned with the OPIC Strategic Plan. If there are any revisions, ensure the OPIC IT Strategic Plan accommodates those revisions as appropriate in the next update to its OPIC IT Strategic Plan.

- In FY 2007, begin marketing and communicating the final OPIC IT Strategic Plan for exposure and awareness of the IT vision and direction for IT at OPIC.

- Beginning in FY 2007, develop an action plan to mature the current level of the OPIC EA. Update the plan on an annual basis to ensure consistency with OMB guidance and progression of technology throughout the Corporation.

- Integrate the components of the IT Strategic Plan into IT employee performance standards.

- Develop a Human Capital Management Plan.

3.2 Enterprise Business Solutions Goals

OPIC's Enterprise Business Solutions (EBS) are comprised of our applications portfolio and our internet and intranet presence. The primary focus of our applications portfolio is on the financial systems that support OPIC's projects. These systems include our legacy APPX applications, Oracle Financials, our current development efforts in Temenos/T24, as well as current efforts to deploy electronic versions of the agency's Insurance and Finance application forms. A secondary focus is on internal web-based workflow systems to facilitate personnel processing, leave requests, etc., which utilize Lotus Notes and Active Server Page technology. Our EBS also utilizes Microsoft's Active Server Pages (ASP) environment for web development, and has responsibility for OPIC's externally hosted public web site.

The OCIO goals in the EBS area includes improved automated workflow tools, replacement of the legacy APPX applications, identification and implementation of a collaboration toolset that is

consistent with OPIC's Enterprise Architecture, a more robust Content Management solution for intranet, a refresh of the development environments for currency, and improvements in the areas of data governance and enterprise reporting. These goals are described in more detail in the following paragraphs.

3.2.1 Automated Workflow

Automated workflow is the automatic routing of work documents to the users responsible for working on them. Workflow is concerned with providing the information required to support each step of the business cycle. The documents may be physically moved over the network or maintained in a single database with the appropriate users given access to the data at the required times. Triggers can be implemented in the system to alert managers when operations are overdue. Integrating workflow into existing software applications may require some reprogramming, because although independent workflow software can launch a whole application, a workflow system must be able to invoke individual routines within the application. Workflow standards can provide interoperability between workflow software and the applications as well as between different workflow systems.

OPIC's first attempt to automate financial workflow is the implementation of T24 in the loans line of business (LOB). Current plans have the deployment of T24 for Loan Origination in the February 2008 timeframe. The workflow processes for T24 will include all activities that are not related to accounting entries, i.e. approvals, document repository, etc. Information generated in T24 will automatically interface to APPX for "back end" processing.

OCIO is considering a Commercial-Off-the-Shelf (COTS) product, Oracle Loans, as a possible "Back End" (budgeting and accounting) solution. OCIO will be configuring Oracle Loans for demonstration in the OPIC environment. OCIO will be work closely with the lines and with functional experts to review the system capability, to map the capability to OPIC's documented functional requirements, and to assist in determining if this product meets OPIC's needs.

Over the long term, the OCIO strategy is to use integrated workflow to automate the LOBs' customer pipeline, capture required statutory documents, and feed work information into an integrated Oracle Financial environment.

3.2.2 APPX Replacement

The APPX legacy environment is comprised of the departmental systems and the database of record that manages OPIC business transactions. APPX data serves as a primary source of data for the OPIC Oracle Government Financials (OGF) core financial system. APPX data is interfaced to OGF with a conversion operation called the daily interface. Given the maturity of the APPX system in the software development lifecycle (SDLC) and the on-going implementation of the T24 application, there are no planned expansions to the APPX system. APPX is at the end of the development and support lifecycle. As such, OPIC's goal is to sustain the usability of the system until all capability is replaced with new systems. OCIO has developed a high-level approach for maintaining the viability of APPX by:

- Mitigating the risks associated with the current APPX hardware and software platform,
- Planning for future hardware and software refresh until decommissioning, and

- Defining the requirements for continued access to the historical data, post-decommission.

OCIO is currently planning to perform an initial and sequential upgrade to the APPX hardware and software environments. The current lifecycle of APPX will require continued operation through 2011 and beyond for historical data purposes. As a result, the initial upgrade will make APPX compliant with current technology standards. The sequential upgrade will ensure future compatibility with OPIC systems.

Over the longer term, OCIO plans to migrate the backend processes for Loans to Oracle Loans, and investigate the development of a custom Oracle application for the Insurance functions.

3.2.3 Collaboration Toolset

Project teams today move faster and work under more pressure than ever before. To expedite information sharing and to accelerate decision making, teams are using new tools – tools that are changing our definition of the workplace. These knowledge management tools include:

- Document collaboration,
- Web-based file and document sharing,
- Online whiteboards,
- Internet presentations,
- Chat and instant messaging,
- Discussion groups and Bulletin Boards, and
- Distance learning for education and training.

These tools fall under the general heading of collaboration tools or knowledge management software.

OPIC is moving to a more Oracle-centric environment. OPIC must select a collaboration toolset that will fully support the Oracle E-Business Suite. The toolset must also support the Oracle E-Business Suite middle-tier software. A review of all appropriate toolsets will be performed in 2008 and the toolset will be selected based on this review.

3.2.4 Interoperable Solutions

Currently OPIC uses a series of disparate systems with manual “daily interfaces” to transfer sub-sets of information. This disjointed approach provides no visibility from one system to the details of another, and does not allow for a cross-system reporting capability.

Interoperability is the ability of different information technology systems and software applications to communicate, to exchange data accurately, effectively, and consistently, and to use the information that has been exchanged. Making information systems interoperable will contribute to more effective and efficient work processes and can reduce costs.

The goal of the OCIO is to provide a more integrated and accessible environment. To that end, OPIC business software is being transitioned to Oracle-based and Oracle E-Business Suite-

based solutions. This will allow for common toolsets and routine access to OPIC data resources. We will also need to expand on our Oracle E-Business Suite investment to drive systems interoperability across multiple areas and departments: HR, finance, accounting, budget, and PMD.

3.2.5 Enterprise Reporting

OPIC's lines of business have a need to transform the large amounts of data collected from its financial management and other systems into meaningful reports that different types of workers in multiple lines of business can use to better do their jobs. Currently, OPIC users must use separate Excel spreadsheets, Access databases, and reports from the various business systems in combination to obtain their required report solution. Unlike ad hoc query reports developed by business analysts and other computer-savvy users, enterprise reports are developed by IT for broader audiences. Reports generally take the form of spreadsheets, PDF files, or even just rows and columns of data disseminated through the Web or by E-mail.

Building on the development of interoperable solutions, OCIO plans to develop a reporting solution that can be used to provide standard reports to their user base regardless of which business system houses the data needed to generate the report.

3.2.6 Data Governance

Currently at OPIC, some data and information is duplicated across multiple business systems. Data governance can provide the ability to better manage this business data by identifying the data owners and data users, and providing a process for data integrity.

Data governance refers to the overall management of the availability, usability, integrity, and security of the data employed in an enterprise. A data governance program would include defining the custodian of the data, defining a set of procedures for its capture, storage and use, and planning to execute those procedures.

The initial step in the implementation of a data governance program involves defining the owners or custodians of the data assets in the enterprise. A policy would be developed that specifies who is accountable for various portions or aspects of the data, including its accuracy, accessibility, consistency, completeness, and updating. Processes must be defined concerning how the data is to be stored, archived, backed up, and protected from mishaps, theft, or attack. A set of standards and procedures must be developed that defines how the data is to be used by authorized personnel. Finally, a set of controls and audit procedures must be put into place that ensures ongoing compliance with government regulations.

Over the longer term, the OCIO envisions implementing data governance through an operational data store. An operational data store (ODS) is a type of database often used as an interim area for a data warehouse. Unlike a data warehouse, which contains static data, the contents of the ODS are updated through the course of business operations. An ODS is designed to quickly perform relatively simple queries on small amounts of data (such as finding the status of a customer loan), rather than the complex queries on large amounts of data typical of the data warehouse. An ODS is similar to your short term memory in that it stores only very recent information.

3.2.7 Enterprise Web Portal

OPIC's current web and intranet environment is a combination of Lotus Notes, HTML, and Microsoft's ASP. The web content is manually created and maintained with no framework for ease of development, deployment or maintenance of the content.

The OCIO will work toward developing a standard content management framework for development and deployment of web content that puts information management in hands of departments without the need for OCIO staff to post all web content, and without requiring the departments' business users to learn complex development tools. OPIC will explore Microsoft Sharepoint and similar COTS software as a means of providing the content publishing framework that will enhance the utility of the intranet as a sharing and collaboration location and which could be managed by departmental business users rather than OCIO.

The OPIC application software environment is moving to a service-oriented architecture due to the movement of the Oracle E-Business Suite. OPIC will leverage this new capability to provide more access and services via our developing Enterprise Web Portal.

3.2.8 Performance Measures

The following represents the performance measures for the Enterprise Business Solutions Goals:

- Deployment of the Temenos/T24 loan initiation application by the end of FY07, to include testing and user training.

- Successful upgrade of APPX software to the most current version.

There will be a number of additional performance measurements implemented in 2008 and beyond. Project metrics will be established to monitor new projects. Software and databases will be performance baselined so advances in software and hardware can be quantified against our baselines.

3.3 Technology Improvement Goals

The OCIO has undertaken a structured regimen of maintaining and improving the technology infrastructure within OPIC. This approach takes two forms: Technology Refreshment and Technology Improvement. Technology Refreshment aims to maintain our current technology infrastructure at industry-standard levels through a program of regular replacement of aging technology elements. Technology Improvement identifies new technologies that can be introduced to OPIC to assist in applying emerging technology solutions to OPIC's business requirements.

3.3.1 Infrastructure Refreshment

The OCIO team is in the process of implementing a Technology Refreshment Plan to bring how often we replace our hardware and software into line with the current guidance. The plan calls for replacing all desktop and laptop computers every three years. In order to avoid spikes in capital expenditures, this will be accomplished by replacing one-third of the PCs each year. The net result is that no OPIC staff should have a computer on their desk that is over three years

old. In the Data Center, we plan to maintain our servers and network equipment so that none are outside of support by the hardware vendor. As a general rule, that means we will replace servers every five years, again on a cycle of replacing approximately one-fifth of the servers every year. The OCIO also supports the OPIC community's mobile communications needs for the issuance and support of mobile devices. OCIO plans to refresh mobile devices every two years based on the original purchase date.

For software, the plan calls for maintaining our software at not more than one release behind the current versions released by the software vendor. For example, now that Microsoft has released Windows Vista, we are in the process of upgrading all of our current PCs that are running Windows 2000 to Window XP, approximately 100 PCs. We also are upgrading those machines from Microsoft Office 2000 to Microsoft Office 2003.

In addition, we are undertaking efforts to bring all hardware and software current with maintenance contracts, so that our entire IT infrastructure is supported by the manufacturer or software vendor.

These changes will increase the reliability and maintainability of all of OPIC's technical infrastructure, thus providing a better computing environment to all OPIC staff.

3.3.2 Infrastructure Improvement

The OCIO will implement a Technology Improvement Program (TIP) to provide for the orderly and systematic acquisition of information technology improvements to support the OPIC Strategic Plan. The TIP will be the OCIO's principal tool for identifying new and emerging technologies that can be applied to the variety of business requirements within the OPIC lines of business. The TIP will also be instrumental in communicating and coordinating information technology strategic planning.

The TIP is a significant part of the information technology strategic planning process established to formulate strategic direction, prioritize major initiatives, address strategic issues, and provide recommendations. The TIP will be responsible for constantly scanning the industry journals and publications to keep abreast of the latest developments in technology that is currently in use within OPIC, or that has the potential to be applied to OPIC's business requirements. When the TIP identifies a potential new technology, that technology will be examined for its possible uses within OPIC, and its fit within the OPIC IT enterprise architecture and strategic plan. Once the technology is deemed appropriate for use within OPIC, it will be applied through the capital planning process, and a program plan developed for its implementation.

3.3.3 Performance Measures

The following represents the performance measures for the Technology Improvement Goals:

- Annually, identify the number of technology elements that have been refreshed through the OCIO technology refreshment program to ensure that the goals of the program are met each year.
- Account for the number of new technologies that have been examined for application against OPIC business requirements, and the number that have been selected for implementation.

3.4 Information Security Goals

Information Security covers a broad spectrum of programs designed to ensure the integrity of all data and information stored within OPIC's information systems. These areas are broken down into Information Assurance (IA), Continuity of Operations, Disaster Recovery, and Certification and Accreditation. Information Assurance protects information to ensure that it is reliably available to users as needed. Continuity of Operations deals with the ability to reconstitute OPIC information systems in the event of any form of a systems failure or disaster. Certification and Accreditation is a program that assesses information systems to operate within security standards and accredits them to safeguard the business information of the Corporation.

3.4.1 Information Security Policies, Standards, and Procedures

The Policies, Standards, and Procedures element will establish the framework for the overall Information Security program through the development, documentation, and maintenance of policies, standards, and procedures. The compilation of these documents is essential to the overall effectiveness of OPIC working towards similar security solutions and implementing them in accordance with a defined security architecture.

The collection of security policies establishes foundational IA requirements and rules for OPIC to protect the confidentiality, integrity, and availability of information assets. This element will document policies, standards, and procedures that will instruct Department staff on the specifics of the IA program and on safeguarding the program and specific systems. These documents will draw source materials from authoritative sources, including NIST, OMB, and public laws, and will ensure that these materials are distributed or otherwise made available to OPIC staff. The Policies, Standards, and Procedures element will also establish a framework for consistently collecting, analyzing, and distributing guidance materials. These documents will be developed and compiled in a manner that fulfills OPIC regulations and guidelines.

The overall objective of this element is to develop the policies, standards, and procedures that will serve as the foundation for a robust IA program. To meet this objective, OPIC will undertake a series of tasks that will support a more effective application of security. The Policies, Standards, and Procedures element will meet the following objectives:

- Establish and maintain an integrated security policy and metric framework including policies, standards, and guidelines
- Validate the existing security standards or identify the need for new security standards
- Ensure baseline security standards fulfill requirements set forth by current and future legislation, regulations, and federal guidance
- Provide guidance for disaster recovery planning for all IT systems
- Provide guidance for continuity of support planning for all IT systems

3.4.2 Information Assurance

The U.S. Government's National Information Assurance Glossary defines Information Assurance (IA) as:

Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Assurance is closely related to information security, and the terms are sometimes used interchangeably; however, IA's broader connotation also includes reliability, and emphasizes strategic risk management over tools and tactics. In addition to defending against malicious hackers and viruses, IA includes other corporate governance issues such as privacy, compliance, audits, business continuity, and disaster recovery. Further, while information security draws primarily from computer science, IA is interdisciplinary and draws from fraud examination, forensic science, military science, management science, systems engineering, security engineering, and criminology, in addition to computer science.

The OCIO is in the process of refining our IA plans and tools, which currently consist of an IA directive and handbook, IA training for users, owners, and custodians, annual IA refresher training, and security baselines for OPIC's business systems.

OCIO is in the process of identifying and implementing IA auditing and logging tools and processes to analyze the output of those tools. OCIO also have plans to implement improved security systems including proxy/reverse proxy, and changes to our current DMZ approach. In the future, the OCIO will focus on protecting financial system data and insider threat scanning and analysis.

3.4.3 Security Operations

Information Security management has become an area of complexity in protecting the confidentiality, integrity, and availability of systems and data. With system interconnections across OPIC and its external partners, protection and response capabilities must be centrally managed. Preventive and reactive IA services will ensure that a baseline of system security is maintained across interdependencies. Integrated solutions will focus on establishing a framework to effectively identify, evaluate, test, and implement new security solutions in addition to ensuring standard security configurations are implemented across OPIC. Incident Management (IM) will integrate all incident-related services into a single, comprehensive capability that focuses on OPIC-wide incident preparedness and readiness.

The Security Operations element will establish a capability to centrally manage OPIC-wide security integration initiatives and IM initiatives. The goal is to build and maintain IA capabilities to effectively manage OPIC-wide system assurance efforts from a central location and efficiently implement security solutions that map to the OPIC's mission, business requirements, and IA requirements. The comprehensive Security Operations capability will meet the following objectives:

- Promote and enforce the implementation and integration of baseline security standards throughout Principal Office lines of business
- Monitor and react to potential disruptions impacting Department assets
- Develop an operational capability to provide decision support under all conditions

3.4.4 Continuity of Operations

Continuity of Operations Planning (COOP) is responsible for the preparing, documenting, and testing required to ensure the ability to reconstitute the OPIC core business systems in the event of a catastrophe. There are three main criteria in COOP planning: recovery point objective (RPO), recovery time objective (RTO), and cost.

RPO is defined as the point to which you need to be able to recover, that is the state to which the system needs to be recovered, and the systems that need to be reconstituted.

RTO is defined as the time limit within which the systems need to be recovered. This can vary by system and nature of the failure.

Both the RPO and RTO have to be balanced against a budget, documented business need, and technical capability of the OPIC systems.

The OCIO is participating with OPIC's DR/COOP committee to understand the business impact of any failure or disaster, and to plan our technology response to an event. OPIC has a draft BIA and COOP document that is in the review and approval process. OCIO will develop its COOP capability against the approved documented plan.

3.4.5 Disaster Recovery

Disaster recovery (DR) is the process of regaining access to the data, hardware and software necessary to resume critical business operations after a natural or human-caused disaster. A good plan takes into account many different factors. The most important are:

- Communication
- Backup and Restore capability
- Facilities - having backup hot sites or cold sites
- Training
- Testing

OCIO is in the process of implementing several new technologies that will improve OPIC's DR capability. These include an improved backup/restore technologies and processes, a storage area network (SAN), network redundancy and documented procedures for failover processes.

Over the longer term, OCIO is exploring the value of using additional server clustering and considering the possibility of obtaining remote hosting services. We are also reviewing restoration capability with system owners for impact analysis, expectation gap analysis and implementation of improved fault tolerance at the system and sub-system level. The OCIO DR plan is a sub section of the OPIC COOP plan.

3.4.6 Certification and Accreditation

Certification is the comprehensive assessment of the technical and non-technical security features and other safeguards of a system associated with its use and environment to establish the extent to which a particular system meets a set of specified security requirements. Certification is in support of accreditation. Certification is an integral part of risk management and should be continually reviewed and updated throughout the system life-cycle. The Certification Phase of the C&A process includes a system analysis to identify weaknesses in operating the system with specified counter-measures in a particular environment, as well as an analysis of the potential vulnerabilities of these weaknesses through a rigorous systems test and evaluation (ST&E). Planning for accreditation should be implemented at the beginning of the system life-cycle to ensure that security protection mechanisms and safeguards are designed and integrated into the system and/or subsystems that security decisions are not delayed leading to costly retrofits and delays in operationally fielding the system, and that adequate resources are provided for C&A activities.

Accreditation is the formal declaration by the Designated Approving Authority (DAA) that an automated information system (AIS) is approved to operate in a particular security mode using a prescribed set of safeguards, and should be strongly based on the residual risks identified during certification. The Accreditor has the formal responsibility in authorizing operation of the system. Since the risk to a system changes over the life of the system, the Accreditor must remain actively involved in the accreditation/reaccreditation process during the entire system life-cycle. The level of risk the Accreditor is willing to accept should be based upon the degrees of assurance.

The C&A process allows the DAA, Program Manager, and User Representative to tailor the certification efforts to the particular system mission, threats, environment, degrees of assurance, and criticality of the system, as necessary, as long as they comply with network connection rules. With a standard approach established, reuse of both the technical and nontechnical analyses from the certification effort for recertification or certification of a similar system might be possible. The C&A process should encourage and preserve commonality in understanding, be consistent in application, be open to evolution and growth, employ feedback, and be applied continuously. This process should be scalable to the size of the system, repeatable, and predictable.

The OCIO is in the process of certifying and accrediting all OPIC systems, both the systems infrastructure and the business systems that support OPIC users. This will provide the initial C&A for OPIC's systems. In addition, OCIO plans to implement a continuous monitoring plan to ensure security and compliance between C&A refreshes, a repeatable process for conducting ST&Es, and future C&A at the network and system levels.

3.4.7 Security Training and Awareness

A Security Training and Awareness program has been established that must be enhanced and continually refined to ensure that OPIC staff is provided with specialized training and security awareness that allows them to successfully fulfill their specific job duties, to develop professionally in their careers, and to alert them to important information regarding their security

responsibilities. A Security Training and Awareness program that includes training, awareness, and outreach must be implemented that delivers a multitude of security messages through various means to all employees. The Security Training and Awareness program will include a comprehensive and integrated approach to delivering security-related training content and awareness initiatives that will promote, raise, and sustain the security culture and goals of the Department.

The Security Training and Awareness program will target the general population and the specific functional roles within the Department. The specific mission assurance objectives are:

- Improve security awareness and communications throughout the Department
- Establish a professionalization and retention program for personnel with security responsibilities.

3.4.8 Performance Measures

The following represents the performance measures for the IT Security Goals:

- All OPIC information systems are under the guidance of a comprehensive Information Assurance plan that is regularly updated to reflect the latest trends and threats;
- A complete, tested information technology COOP plan that identifies three levels of failure and the OCIO response to each to reconstitute OPIC information systems; and,
- A complete, approved C&A document for all OPIC information systems.

3.5 IT Operations Goals

IT operations are the heart of the OCIO's support to OPIC users. Operations comprises the day-to-day business tools that OPIC users utilize in performing their duties to meet the OPIC mission and strategic goals. Operations consists of our help desk which provides service to OPIC users and our data center which provides the infrastructure on which OPIC business systems operate.

3.5.1 Customer Service

A help desk is an information and assistance resource that troubleshoots problems with computers and similar products. The OCIO provides help desk support to OPIC users via telephone, and/or e-mail.

The OPIC help desk performs several functions. It provides the users a central point to receive help on various computer issues. The help desk manages its requests via the HEAT help desk software, which includes a trouble ticket tracking system. The OCIO is also implementing procedures to use the help desk software to find, analyze, and eliminate common problems and trends in OPIC's computing environment. This gives the help desk the ability to monitor the OPIC user environment for issues from technical problems to user preferences and satisfaction. This information is valuable in planning and preparation for other IT programs.

The OCIO is in the process of upgrading the HEAT trouble ticket system to the latest release of the HEAT software. This upgrade will provide the OCIO with a more robust reporting capability

with the ability to track the level of service provided by the help desk and better identify user and technology trends.

3.5.2 Performance Management

Performance management is a relatively new concept to the field of management. Performance management reminds us that being busy is not the same as producing results. The major contribution of performance management is its focus on achieving results -- useful products and services for customers inside and outside the organization. Performance management also helps to ensure that systems and processes in the organization are applied in the right way to the right things: to achieve results needed to meet the OPIC strategic goals and mission.

The OCIO is in the process of implementing a performance management plan for the data center. Software has been implemented that monitors the performance of all OPIC systems and reports on that performance on a regular basis. Performance reports are currently being examined to identify the normal performance range of each monitored element and the out-of-limits metrics for each. By having these metrics established, the OCIO will be able to closely watch the performance of the IT infrastructure and identify any anomalies before they have a major impact on system performance. The performance management plan will also provide the OCIO with the ability to identify performance trends that may indicate that a system element may need improvement.

An additional goal of the OCIO performance management plan is the development of established service levels for the support and services that we acquire from our hardware and software vendors, as well as the support and services that the OCIO provides to OPIC users. These established service levels will provide the OCIO with a mechanism to track how well our vendors meet our needs, and how well the OCIO meets the need of the OPIC user community.

3.5.3 Performance Measures

The following represents the performance measures for the IT Operations Goals:

- Implementation of the upgraded HEAT software package with an established set of reports that are being regularly monitored by OCIO management;
- Establishment of service level agreements (SLA) for all OCIO vendors and management scrutiny of the vendors performance against the SLAs; and,
- Performance metrics for the IT infrastructure support and service provided to OPIC users.

4.0 CONCLUSION

This IT Strategic Plan outlines the OCIO vision and approach to addressing measures to gain improvement in the areas of:

- IT Governance and Program Management;
- Enterprise Business Solutions;
- Technology Improvement;
- Information Security; and,
- IT Operations.

These improvements are needed to not only maintain OPIC's systems, but also to improve the way OCIO supports our OPIC community and the services and support we are responsible for delivering to our users.

These strategies are just the starting point. Underlying each of the strategies are initiatives that will implement technology solutions that will help in reducing risks to OPIC systems, data and information. Each of these initiatives are either currently underway, through a well thought out, planned approach, or are in the planning stages.

In the future, the OCIO staff will continue to maintain and refresh the IT Strategic Plan as new business requirements surface that call for additional technology solutions.

APPENDIX A – BUSINESS DRIVEN OPIC IT STRATEGIC PLANNING FRAMEWORK DETAIL

The OPIC IT Strategic Plan is based on helping to meet OPIC strategic goals.

Strategic Goals	Strategic Objectives
Goal #1: Maximize OPIC's Impact on Economic Development	(a) Ensure that OPIC supported projects are highly developmental. (b) In the priority sectors of housing, micro finance and access to credit by Small and Medium Enterprises: achieve a significant aggregate development impact in selected countries.
Goal #2: **Support U.S. Foreign Policy**	(a) Proactively channel U.S. private investment to the foreign policy priority regions, e.g. (Broader Middle East, Sub Saharan Africa and Central America/ Mexico/Brazil). (b) Mobilize U.S. private capital to jumpstart economic growth in countries in economic crisis due to armed conflict or natural disasters. (c) Ensure that OPIC supported investments go to countries that have good relations with the United States.
Goal #3: Mobilize Investments by Small and Medium Enterprises	(a) Continue targeted support for Small and Medium Enterprises. (b) Implement projects sponsored by Small and Medium Enterprises owned by women and minorities.
Goal #4: Efficiently Serve Investors	(a) Operate in a business-like, self-sustaining manner. (b) Make access to OPIC products and services as user friendly as possible

Table 2-1: OPIC Strategic Goals and Objectives

IT Strategic Goals	IT Strategic Objectives
Goal #1: IT Governance and Program Management	(a) Develop an Enterprise Architecture (b) Develop an IT Strategic Plan (c) Provide Oversight for Information Technology and Information Management Policies (d) Capital Planning and Investment Control (e) Program Management Office (f) Human Capital Management
Goal #2: Enterprise Business Solutions	(a) Automated Workflow (b) APPX Replacement (c) Collaboration Toolset (d) Interoperable Solutions (e) Enterprise Reporting (f) Data Governance (g) Enterprise Web Portal
Goal #3: Technology Improvement	(a) Infrastructure Refreshment (b) Infrastructure Improvement
Goal #4: Information Security	(a) Information Assurance (b) Continuity of Operations (c) Disaster Recovery (d) Certification and Accreditation
Goal #5: IT Operations	(a) Customer Service (b) Performance Management

Table 2-2: OPIC OCIO Strategic Goals and Objectives

APPENDIX B – OPIC IT STRATEGIC PLANNING LEGISLATION

Over the past few years, Congress passed an unprecedented amount of legislation aimed at improving agency performance through implementation of more effective strategic, financial, and acquisition management policies. The Clinger-Cohen Act (CCA) of 1996, the Government Information Security Reform Act (GISRA) of 2000, the Government Performance and Results Act (GPRA) of 1993, the Chief Financial Officer's Act (CFOA) of 1990, the Paperwork Reduction Act (PRA) of 1995 and the E-Government Act of 2002 are relevant legislation that direct agencies to improve the uses and efficiency of IT within their organizations. The table below provides a summary description of each act.

Legislation	Description
Clinger-Cohen Act, 1996	Improves the productivity, efficiency, and effectiveness of federal programs through improved acquisition, use, and disposal of IT resources.
Government Information Security Reform Act, 2000	Focuses on the program management, implementation, and evaluation aspects of the security of systems.
Government Performance and Results Act, 1993	Holds federal agencies accountable for achieving program results and requires them to clarify their missions, set program goals, and measure (and report) performance related to meeting those goals.
Paperwork Reduction Act, 1995	Ensures that operations and decisions are integrated with organization planning, budget, financial management, human resources management, and program decisions.
E-Government Act, 2002	Codifies the President's Management Agenda (PMA) to expand E-Government initiatives, sets new OMB reporting requirements and codifies the existence of the CIO Council.
Chief Financial Officer's Act, 1990	Manages the strategy for developing and integrating individual agency accounting, financial information and other financial management systems to ensure adequacy, consistency, and timeliness of financial information.