UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Information Resource Management (IRM) Plan

2010 - 2013

A New Day for the Civil Service

Message From the
Chief Information Officer

Message from the Chief Information Officer

The Office of Personnel Management (OPM) is pleased to present the Agency's Information Resource Management (IRM) Plan for Fiscal Years (FY) 2010–2013. The Plan establishes a new direction for improving support to OPM's mission of recruiting, retaining, and honoring a world-class workforce to serve the American people.

The Office of the Chief Information Officer (OCIO), along with its IT partners, is responsible for the successful introduction of technology to support OPM's strategic goals, as well as the tools and infrastructure needed to deliver world-class services to the federal workforce and retirees. We will provide innovative technologies and IT services by: directing the implementation of the Agency's IT architecture to ensure integration of IT components with each other, including reviews to ensure design consistency and compliance with federal standards; managing compliance with oversight directives, including IT security and privacy programs for the Agency; managing government-wide and agency-specific programs in such areas as records management, forms management, and paperwork reduction, to ensure information and records under OPM's control are managed in the interests of the American public; working with other agencies on government-wide projects, such as e-Government; and leading the development of long-range IT human resource (HR) strategies for the Government as a whole.

The challenges currently facing OPM include the ever-growing need to adopt leading edge technologies while protecting the data with which the Agency is entrusted. In this IRM Strategic Plan, we outline how IT and information and records management will support the OPM Strategic Plan and goals. We also affirm our commitment to bring quality IT products and services and a state-of-the-art technology platform to OPM business operations and the American public.

The success of this IRM Strategic Plan will depend on the commitment at all levels of OPM to helping the Agency's IT staff achieve the goals and objectives of this plan. We will continue to assess our accomplishments and identify additional goals and measurements to advance OPM's mission.

Mathew Perry

Chief Information Officer (CIO)

OPM Mission Statement

Recruit, Retain and Honor a World-Class Workforce to Serve the American People

OPM Vision Statement

The Federal Government will Become America's Model Employer for the 21st Century

OPM Values

SERVICE

We pledge through our oath to encourage and support those who serve the wider public or community through their work as Federal employees.

RESPECT

We extend consideration and appreciation to employees, customers and stakeholders fostering a fair, open and honest workplace environment. We listen to the ideas and opinions expressed by others. We treat others as we would wish to be treated.

INTEGRITY

We uphold a standard of transparency, accountability, and reliability. We conscientiously perform our operations to promote a Federal workforce that is worthy of the public trust.

DIVERSITY

We honor our employees and customers through inclusiveness and respect for the various perspectives and backgrounds that each brings to the workforce.

ENTHUSIASM

We embrace our work and the challenges of the future with excitement, energy, and optimism. We are open to the myriad possibilities of change and eagerly unite in the spirit of "yes we can."

EXCELLENCE

We fulfill our mission by providing relevant and timely products and superior customer service that reflects our commitment to collaboration and the highest standards of quality.

INNOVATION

We constantly seek new ways to accomplish our work and to generate extraordinary results. We are dedicated to delivering creative and forward-looking solutions.

OCIO Mission Statement

We are committed to delivering innovative, cost-effective, and secure IT solutions and infrastructure that support OPM's programs and initiatives.

OCIO Vision Statement

We are model information and technology center recognized for strategic thinking, proactive leadership, collaborative partnerships, and innovative solutions advancing OPM's mission to recruit, retain, and honor a world-class workforce to serve the American people.

Contents

Purpose

The purpose of the Office of Personnel Management's (OPM) Information Technology (IRM) Strategic Plan for Fiscal Years (FY) 2010–2013 is to establish an agency-wide vision, a direction, and priorities for OPM's investments in information and records management, and IT operations so that they promote the achievement of OPM's mission and business outcomes. This Plan describes how OCIO strategies, goals, and objectives align with the mission, vision, values, and daily operations identified by the Director of OPM in the IRM Strategic Plan for 2010–2013. This IRM Strategic Plan identifies the implications outlined in OPM's business strategies and integrates them into implementable objectives associated with key performance indicators (KPI).

Several drivers—both internal and external to the Agency—have directly influenced the contents of this plan. Internal business requirements, internal technology requirements, open government requirements, and requirements mandated by the federal IT environment drives OPM's decisions. The development of this IT Strategy considered all aspects of IT, including decisions, investments, management, operations, technology selection, and implementation. The IRM Strategic Plan considers both OPM's current environment and future strategic objectives. The IT Plan provides OPM with a set of strategic guidelines for modernization and a high-level roadmap of objectives to support the business and OCIO strategies. It provides the strategic direction that OCIO has undertaken, along with details required to execute and implement the proposed strategies over the next 3 years.

Introduction

The Office of Personnel Management (OPM) works with the President of the United States, Congress, cabinet-level departments, agencies, and other stakeholders to implement human resource (HR) management policies to build a high-performing workforce that allows federal agencies to accomplish their missions. OPM's mission is to "recruit, retain, and honor a world-class workforce to serve the American people." OPM's strategic goals include recruiting and hiring talented and diverse citizens for federal service; supporting and developing the federal workforce though training, benefits, and work-life balance; ensuring the federal workforce is fully accountable; recognizing and rewarding exemplary performance; and honoring service. In addition, OPM provides a broad range of support services and products to the Federal Government, such as conducting background investigations; administering health benefits, life insurance, and retirement benefits; serving as a consolidated source of HR data; and overseeing merit systems accountability programs in the Federal Government.

OPM's IT assets are integral to the accomplishment of the Agency's mission. IT is managed at OPM through various management and governance processes: capital planning and investment control (CPIC); Enterprise Architecture (EA) planning; management of compliance and oversight directives, including IT security and privacy program management; and System Development Life Cycle (SDLC) management.

This IRM Strategic Plan encompasses information and records management services and activities across OPM and addresses a broad spectrum of technology services envisioned by OPM. It also describes the alignment between OPM's strategic goals and mission and the Agency's IT objectives.

Evolution of IT at OPM

OPM's IT infrastructure and architecture have evolved dramatically. In the mid-1990s, OPM, like many other agencies, was considered to be stove-piped and decentralized. OPM had multiple customer- or application-centric mainframe data centers, local area networks, and wide area networks managed by program organizations. These technologies were in need of coordination and consolidation.

In 1995, downsizing at OPM tied to budget reductions forced a re-evaluation of OPM's IT and resulted in the consolidation of data centers and infrastructure. This movement coincided with the enactment of the Clinger-Cohen Act in 1996, which established accountability for ensuring the use of IT to support the Agency's mission. The consolidation of IT management also coincided with the appointment of OPM's first Chief Information Officer (CIO). OCIO began its re-evaluation by developing an Architecture Vision, which later evolved into the Agency's EA. The OPM EA, guided by the Federal Enterprise Architecture (FEA), defined OCIO's IT management principals, goals, and objectives and established a roadmap to achieve the EA vision of centralizing and managing OPM's IT infrastructure for the benefits and efficiencies that can be realized through technology.

OCIO continues to implement its EA vision and has already achieved a high level of integration and standardization. OCIO has standardized its hardware and software environments, operating systems, office automation tools, and e-mail. OCIO has also centralized its help desk, network engineering, network administration, and technology refreshment management. In addition, OCIO has used its EA vision as the basis for developing an Agency-wide IT security program and Agency-wide SDLC management approach. OCIO has also developed IT and EA governance processes to oversee the

Agency's use of IT. For example, IT CPIC processes, which the CIO manages, engage OPM's most senior executives in IT oversight to ensure the investments support the Agency's mission.

In 2010, OPM is continuing to make effective use of IT despite the challenge of resource constraints. In recent years, OPM has encountered issues that, unless addressed, will be detrimental to the Agency over time. For example, key infrastructure (e.g., hardware and software tools) is aging and in need of modernization. Necessary funding to accommodate a refresh of technology, equipment, and staffing is severely lacking, delaying the required modernization of the agency's IT infrastructure. Several mandates and requirements remain unfunded. In addition, OPM continues to face a lack of personnel with the appropriate skill set to support the legacy technology. Although OCIO continues to effectively manage its IT spending, issues of adequate funding remain in the forefront of OCIO priorities. It is hoped that these will be resolved expeditiously.

In January 2010, OPM implemented an agency reorganization that shifted priorities toward a focus on business functions. OPM now comprises five core mission business lines:

- **Employee Services:** Provides policy direction and leadership in designing, developing, and promulgating government-wide HR systems and programs for recruitment, pay, leave, performance management and recognition, employee development, work-life/wellness programs, and labor and employee relations; provides technical support to agencies regarding the full range of HR management policies and practices, including veterans' employment and agency program evaluation; manages the operation of OPM's internal HR program.
- **Retirement and Benefits:** Is responsible for government-wide administration of the following: developing and providing federal employees, retirees, and their families with benefits programs and services that offer choice, value, and quality to help maintain the Government's position as a competitive employer; administering the Civil Service Retirement System (CSRS) and the Federal Employee Retirement System (FERS), serving 2.5 million federal retirees and survivors who receive monthly annuity payments; negotiating and administering health benefits contracts for the Federal Government; administering the Federal Employee Group Life Insurance (FEGLI) program covering employees, retirees, and their families; administering three voluntary, enrollee-pay-all programs: long-term care insurance program, flexible spending accounts for medical and dependent care expenses, and a group dental and vision insurance program.
- **Merit System Audit Compliance:** Ensures through rigorous oversight that federal agency HR programs are effective and meet merit system principles and related civil service requirements.
- **Federal Investigative Services:** Ensures the Federal Government has a suitable workforce that protects national security and is worthy of public trust; is responsible for providing investigative products and services for more than 100 federal agencies to use as the basis for security clearance or suitability decisions as required by Executive Orders and other rules and regulations (OPM provides more than 90 percent of the Government's background investigations).
- **HR Solutions:** Provides services that assist the Federal Government in achieving its missions by partnering with agencies to provide effective HR solutions that develop leaders, attract and build a high-quality public sector workforce, and transform agencies into high-performing organizations; offers services that enhance agencies' ability to attract and acquire specific talent.

OCIO will manage and implement IT investments that support the OPM Strategic Plan in a cost-effective and well-managed manner to support existing federal government initiatives, requirements and trends, such as recent transparency initiatives (e.g., Open Government, federal IT Dashboard reporting). OCIO will provide ongoing guidance in IT use and management through OPM's Strategic Plan, EA, Annual Performance Plan, and ongoing partnership with OPM program offices through the common services program.

Critical Success Factors

OCIO believes the following factors are critical to IT service delivery and achievement of strategic goals. These factors can help ensure the successful execution of the IRM Strategic Plan:

- Willingness of OPM staff to embrace openness and change
- Willingness of OPM senior executives to serve as stewards of IT and ensure IT supports OPM's mission
- Willingness to keep things that work and get rid of those that don't - whether it is a legacy software application, broken business process or failing project - reallocating resources to better investments
- Sufficient resources to support initiatives with skilled personnel, funding, and time
- Active and visible senior management support
- Well-defined and disciplined processes for information capture, stewardship, and quality and accuracy assurance of OPM information and records
- Education and training that enables employees and customers to adopt new technologies

Environmental Factors

The following are environmental factors that will inherently influence OPM IT services:

- **Aging Federal Workforce:** OPM must prepare for a significant increase in federal workforce retirees in the upcoming years because of the aging of the "baby boomer" generation. It will be the Agency's responsibility to roll out retirement benefits and claims for a greater population than that which OPM is accustomed.
- **Health-Care Reform Legislation:** OPM is closely monitoring the developments of health-care reform legislation. OCIO must be prepared to create and stand up a new health-care system for all uninsured citizens.
- **Presidential Initiatives:** OCIO is paying close attention to ever-emerging technology-related Presidential initiatives. OCIO will prepare to address any technology initiatives that may arise. Currently, OCIO is addressing transparency and accountability in its IT strategic approach because both have been identified as essential regarding the intersection of IT and modern government organizations.
- **Increased emphasis on Cyber Security and PII:** OCIO will effectively utilize cyber security, privacy, and information security measures (i.e. Firewall establishment, data encryption, anti-virus software, etc.) as they relate to the protection of OPM infrastructure containing Federal employee and citizen Personally Identifiable Information (PII). OCIO is working to continue to avoid the unauthorized exposure of OPM sensitive employee data and information.

Guiding Principles

The following guiding principles were utilized during the creation of the IT IRM Strategic Plan, ultimately driving the creation of the IT strategic goals and objectives. These principles form the common themes embraced by OCIO and provide broad guidance for the IT planning process:

- **Shared Services:** Centralize OPM functions and services into cloud computing or virtualized environments resulting in improved processes and cost savings. Pursue the consolidation of like IT functions across the Agency into shared service pools.
- **Efficiency and Economies of Scale:** Provide streamlined services to the Federal Government and citizens by effectively utilizing resources; leverage economies of scale in acquisition, design, and implementation of IT assets to serve OPM and the public.
- **Reliability/Uniformity:** Streamline OPM processes into common or shared processes leading to significant increases in interoperability, information sharing, and knowledge management.
- **Transparency:** Collaborate and share information across OPM and externally to increase accountability and promote informed participation by the public.
- **Customer Service:** Service is implicit in OPM's name and mission; a major principle of OPM is instilling and maintaining the spirit of customer service in every employee, and it is the job of every employee to deliver exceptional customer service.
- **Time to Market:** Reduce the time OPM employees have to wait for the benefits of IT solutions by utilizing consumer technologies, agile methodologies and iterative implementation.
- **Managed Diversity:** Provide the tools that knowledge workers need to be productive, allowing those workers to choose from a broad pool of client devices and software applications while maintaining a commitment to cost savings for the Agency.

IRM Strategic Goals

"Achieving Strategic goals…may be easy, but doing so is absolutely necessary to make the Federal Government the model employer in the United States, and OPM its model agency".

John Berry, Director of OPM

To realize the IT mission and vision, OCIO has identified four strategic goals that will guide IT decision-making processes and IT personnel as they perform their mission in support of Agency business. The goals are the following:

INNOVATION

Enable the 21st Century workforce by providing the tools that inspire innovation, promote learning and make collaboration seamless

OPERATIONAL EXCELLENCE

Develop and implement comprehensive IT governance and management practices

MISSION FOCUS

Deliver IT solutions that are customer-focused and driven by the needs of OPM

WORLD-CLASS WORKFORCE

Recruit and develop the best information and technology management workers in the Federal government

CIO Organization

The *Chief Information Officer* (CIO) advises the OPM Director on the design, development, and implementation of information technology investments. In that capacity, the CIO is responsible for information technology (IT) management, software development and maintenance, as well as records management, forms management, and information dissemination and disclosure programs of the Agency.

The CIO monitors and evaluates the performance of information resources investments through an IT capital planning and investment control process, and advises the agency head on whether to continue, modify, or terminate IT investments. The CIO also advises the agency head on budgetary implications of information resource decisions, and is an active participant throughout the annual agency budget process in establishing investment priorities for agency information resources. Therefore, the CIO develops the Agency's IT Strategic Plan and defines the IT vision and strategy of OPM.

The CIO develops information management policy and manages the IT security and privacy program of the Agency. The CIO shapes the application of technology in support of the Agency's Strategic Plan and establishes an IT Architecture that outlines a long term Strategic Architecture and Systems Plan. The CIO provides oversight of major IT acquisitions to ensure they are consistent with Agency business needs and monitors investments for compliance with federal standards. The CIO also works with other agencies on government-wide programs through the Federal CIO Council, and performs long range planning for IT Human Resource Strategies.

The OCIO is organized into two major divisions to streamline internal operations and to effectively address the goals discussed above. Following figure presents the OPM OCIO organization chart.
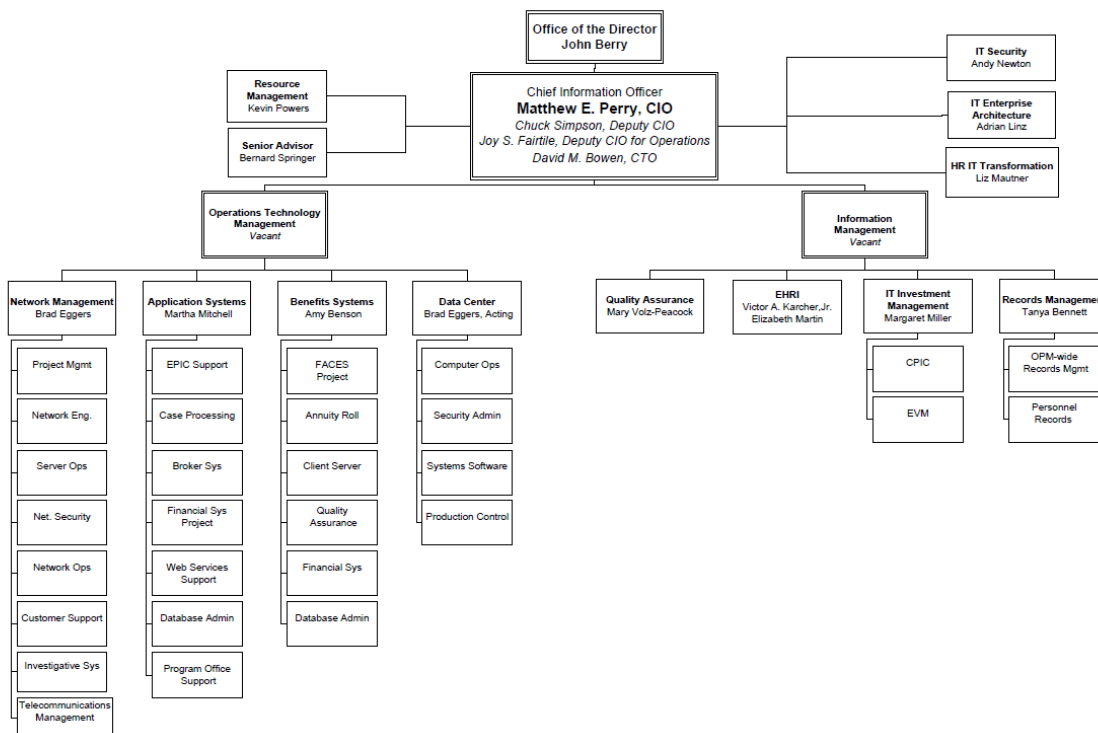

Figure 1 OPM OCIO Organization Chart

The Operations Technology Management area supports core IT operations to include the Network Management, Application Systems, Benefits Systems, and Data Center within OPM.

The CIO Information Management area supports the management of information in multiple interrelated OPM areas, including: Human Resources Information Technology Transformation (HRITT), Enterprise Human Resources Integration (EHRI), IT Investment Management, and Records Management

IT Enterprise Architecture, HR IT Transformation, IT Security (ITS), and Resource Management report directly to the CIO.

Following sections describe the key activities of each of the CIO program areas or sub-divisions.

Network Management: Network Management (NM) supports the CIO goals by managing and operating OPM's Information Technology (IT) infrastructure. This includes the implementation, management and maintenance of local and wide area networks (LAN/WAN), data communications, servers, SANs, IT security initiatives, and Help Desk support.

Application Systems: Applications Systems designs, develops, and maintains mainframe, distributed, and browser-based systems to support OPM programs that are not related to Retirement and Insurance Services. The group comprises 3 teams and 4 branches:

Web Systems Support Team

- Develops agency and intra-agency large or small-scale websites and web applications
- Manages and supports OPM's shared web host environments
- Develops 508-compliant PDF and HTML documents
- Provides web standards, best practices, and technical assistance for web related functions

Case Processing Branch

- Develops and enhances functionality of end-to-end automated support for the processing of personnel security investigations
- Designs, develops, and supports government-wide database of security clearance information for Federal employees and contractors
- Integrates generation of payable and receivable transactions into case processing and supports the interfaces with financial systems

EPIC Support Branch

- Develops functionality to enable the storage, retrieval, and sharing of electronic personnel security investigation case files
- Develops workload management and dashboard reporting of key performance indicators for the personnel security program
- Provides tracking systems for administrative functions in the Federal Investigative Services

Broker Systems Branch

- Develops front-end Portal access for the personnel security suite of systems
- Develops and enhances systems that submit data to the case processing system
- Develops and enhances interfaces with other investigative entities

Program Office Support Branch

- Provides administrative systems using COTS and browser-based applications within OPM

- Systems include Central Personnel Data File, the Executive and Schedule C System, numerous tracking systems, and system development portals

Financial Systems Project Team

- Provides management oversight for the contract staff conducting the independent verification and validation of the CBIS Project

Database Administration Team

- Provides database administration services for server and mainframe based applications
- Services include Systems Architecture, Data Model Review, Capacity Planning, Application Server Administration, Database Administration

Benefits Systems: Benefits Systems is responsible for developing solutions and managing systems that support Retirement and Benefits business processes. Benefits Systems support the Office of the Chief Financial Officer (CFO) and the Office of the Inspector General (IG) in their retirement and benefits-related missions.

These systems perform a broad range of functions and serve a diverse group of consumers and customers, including:
- 2.5 million Federal retirees and survivors who receive annuity payments totaling $64 billion annually;
- 8 million Federal retirees, survivors and dependents who receive health benefits;
- Providing an online Health Benefits Plan comparison tool for use by 8 million Federal employees, annuitants, and survivors;
- 4 million employees, retirees and family members who receive life insurance;
- Establishing 100,000 new retirement cases each year;
- Accounting, receiving, tracking and reporting financial transactions related to voluntary contributions, refunds and other payments;
- Working with 36 State agencies, 6 major Federal Unions and numerous Federal Agencies to withhold taxes and other payments, and coordinate benefits;
- Accumulating withholdings on behalf of nearly 4 million Federal employees across the Federal government to pay hundreds of Health Benefit carriers;
- Supporting actuarial, audit and statistical work.

The Benefits Systems provides the following services:

- Assisting the customer with identifying and defining business requirements;
- Providing analytical support for developing Needs Statement and the use of the Information Technology Systems Manager (ITSM) methodology;
- Conducting systems analysis;
- Making feasibility and technology-related recommendations;
- Doing custom application development and maintenance;
- Coordinating and providing support for user acceptance testing, documentation, training and operational support;
- Assisting Designated Security Officers (DSO) with validating that production systems are secure through the certification and accreditation (C&A) authorization process;
- Providing project management support;
- Conducting ad hoc query and reporting.

Data Center: The Data Center (DC) manages the Enterprise Servers consisting of IBM Z9s running the z/VM; zOS; and z/Linux operating systems. The Data Center comprises two branches and two teams organized to provide IT services for the various program offices within the Office of Personnel Management. The Data Center functions in a 7 x 24 environment and has staff in Washington, D.C., Boyers, PA, and Macon, GA.

- The Computer Operations Branch operates the Enterprise Servers, Data Center network, printers, and peripheral systems which serve all OPM program areas.
- The Production Control Branch manages production software libraries, provides support to application development projects, manages the production processing schedules on Enterprise Servers and Windows servers, executes production and test programs, monitors application software performance, diagnoses and corrects application problems, and distributes reports.
- The Security Administrator Team develops Data Center security policies, controls security administration, and provides auditing support for the Enterprise Server platform.
- The System Software Team performs selection, testing, installation, implementation, and maintenance of all Enterprise Server operating system software and program products and performs system tuning to ensure optimal performance. This team is responsible for developing the Data Center backup and recovery procedures, including disaster recovery, and is responsible for executing the platform recovery procedures when necessary. Also, this team works with internal and external customers to convert systems to the use of electronic data transmission techniques and make other improvements to the applications, and it provides Enterprise Server related training to other organizations.

The Data Center provides a full spectrum of IT services including operating system support, computer operations, production application processing and development support, security administration, computer facilities management and customer support. While all OPM program areas use these services, there is a particularly high level of support provided to Federal Investigative Services (FIS), the Retirement Services, and OPM administrative offices. The Data Center contains large scale Enterprise Server systems performing both legacy tasks and web-enabled server tasks, and it houses associated network equipment to provide connectivity to customers and business partners nationwide. The systems and services are protected by a world-class disaster recovery plan that is fully exercised annually.

Human Resources IT Transformation: Human Resources IT Transformation (HR IT) leads the government-wide transformation of HR Information Technology by focusing on modernization, integration, and performance assessment. It manages the Human Resources Line of Business (HR LOB) initiative through active collaboration with agencies and service providers and focuses on improving the strategic management of human resources by overseeing government-wide systems and services employed by agencies and service providers, improving integration and interoperability of HR systems, and promoting innovative technologies.

Policies and guidance related to Human Resources IT Transformation can be found at
http://theo.opm.gov/References/it/

Enterprise Human Resource Integration (EHRI): Enterprise Human Resources Integration (EHRI) supports the strategic management of human capital by providing agency customers with access to timely and accurate Federal workforce data. In support of this objective, EHRI provides following services:

- Streamline and automate the exchange of Federal employee human resources (HR) information Government-wide;
- Provide comprehensive knowledge management and workforce analysis, forecasting, and reporting across the Executive Branch;
- Maximize cost savings captured through automation; and
- Enhance retirement processing throughout the Executive Branch.

IT Investment Management: IT Investment Management provides oversight of OPM's investments in information technology (IT). Examples of IT Investment Management's responsibilities include, but are not limited to:

- Developing and supporting executive level governance processes related to the management of OPM's IT investments.
- Developing and managing OPM IT portfolio management policies and procedures, including those for:

  o IT capital planning and investment control (CPIC)
  o Earned Value Management (EVM), a methodology for projecting and evaluating IT investment cost and schedule performance
  o OPM's system development life cycle standard, IT System Manager (ITSM)

- Providing independent assessments of IT investments to the CIO and other senior executives.
- Administering IT project manager certification processes jointly with OPM's contracting office.
- Managing OPM's participation in the Federal IT dashboard and submission of IT investment status information to it.
- Managing OPM's development and submission of budget requests for IT, and advising on the development and coordinating the review of Exhibit 300s and Exhibit 53 for inclusion in OPM's budget request.
- Evaluating trends in IT spending and, with OPM's Enterprise Architect, performing IT investment planning and analysis.

Records Management: Records Management performs governance processes related to the management of OPM's internal and government wide records programs and related forms in compliance with federal records and personnel data management standards. Records Management also does the following:

- Manages OPM's forms program.
- Manages the Agency's Paperwork Reduction Act information collection program, provides guidance to OPM program offices in their development of information collection approval requests under the Paperwork Reduction Act, and coordinates the approval of such requests with OMB. Develops and manages implementation of directives standards and guidelines for the Directives Management program of the Office of the CIO.
- Leads OPM's Freedom of Information Act (FOIA) program.
- Leads the development and implementation of personnel data policy and standards for the Federal Government

Records Management Responsibilities

This unit manages the agency's records program. In that capacity, Records Management:

- Develops and maintains the agency's Records Management Handbook.
- Develops and maintains the governmentwide Guide to Personnel Recordkeeping.
- Manages the agency's agreement with the National Archives and Records Administration (NARA) for governmentwide services and storage related to OPM administrative records and federal personnel recordkeeping.

- Administers funds related to the NARA agreement, monitors trends in usage, and advises other agencies on ways to minimize spending on personnel recordkeeping.

IT Enterprise Architecture: The OPM Enterprise Architecture (EA) is a strategic business information asset intended to guide the agency-wide business and technology evolution. OPM business and technology leaders use the EA to analyze and improve the support of information technology (IT) to OPM's mission.

The EA program provides services that include promoting business process improvements; developing and maintaining agency-wide business models and processes, applications and technology architecture; and collaborating with program offices in developing their Project/Program Architectures.

OPM has instituted several activities and services in support of the EA program. The following items highlight those activities:

- **Cost Reduction**: The EA enables high-level views of OPM's business priorities and guides the cost-effective application of IT in support of those priorities. The EA helps to eliminate stovepipe operations and systems, highlight needless duplication and incompatible technologies, as well as reduce or eliminate additional - and unnecessary - costs.
- **Architecture Modernization Blueprint Process**: Individual project/program architectures enable OPM to improve discovery and re-use of business processes, service components, and technologies across the Agency, as well as E-Gov and Line of Business (LOB) initiatives. By conducting this 'blueprinting' process, project/program architecture fosters comprehensive definition, validation, and refinement of OPM's baseline and target EA. Several project/program architectures have been developed and others are in-process with the goal of completing project/program architectures for all major OPM business functions, IT infrastructure and eGov programs.
- **Redundancy Reduction**: OPM continues efforts to institutionalize EA as an element of the strategic IT decision making in order to eliminate redundancies, focus on citizen services, and integrate information for improved decision-making. Further, continuing the Agency's efforts to evolve the EA will allow OPM to take advantage of information integration and sharing across all levels of government.
- **IT Communications**: OPM is advancing an EA Communications Strategy to ensure consistency in IT management messages and themes communicated to project and program managers, staff, and stakeholders throughout the agency.
- **IT Governance**: All OPM program offices and divisions must adhere to the most current approved version of the OPM EA Program Management Plan in their IT solutions and implementations. This plan and related documents drive the EA and how it is managed, used, and governed to achieve the maximum results towards program business/mission outcomes.
- **Quality Assurance**: OPM maintains an EA Configuration Management Plan that defines the procedures for developing, implementing, and editing EA information. This plan identifies the individuals responsible for and tools used in maintaining OPM EA.

IT Security: The mission of the OPM IT Security (ITS) Office is to implement and maintain an agency wide information security program that safeguards information assets against unauthorized use, disclosure, modification, damage or loss. This is done by providing oversight over the implementation of management, operational and technical security controls to protect agency resources. The ITS Office also manages security risks by educating the OPM user community about security related issues, assessing current policies, developing new policies and establishing mechanisms to respond to incidents and events that endanger information assets.

The ITS administrative responsibilities include establishing and maintaining an IT security organization that is

compliant with OPM's strategic goals and priorities, the Federal Information Security Management Act (FISMA) of 2002, the Privacy Act of 1974 and the Clinger-Cohen Act of 1996.

Resource Management: Resource Management provides enterprise-wide support to various CIO functions including information technology (IT) budgeting, IT procurement management and oversight, liaison to OPM offices and external agencies for inter/intra-agency agreements, human capital support, administrative support, space management, and budget and performance reporting activities.

Following section presents the goals and objectives of the CIO organization as well as the performance measures that form the basis of the CIO scorecard.

INNOVATION

Goal 1: Enable the 21st Century workforce by providing the tools that inspire innovation, promote learning and make collaboration seamless.

This goal is focused on modernizing OPM's IT solutions and infrastructure because these components have a significant impact on information and service delivery. OCIO will continue to expand its enterprise-wide approach to modernize its IT environment, which will improve Agency IT asset utilization, system reliability, and availability and achieve cost savings. Presidential initiatives outline the need for transparency and accountability (as a recent example, OMB M-10-06 states that Government must be transparent, participatory, collaborative and accountable). Therefore, OCIO will strengthen its IT security management and data storage as OPM examines and implements new information sharing methods. Data center optimization will continue to be a high priority to reduce the overall cost of operations and energy consumption by OCIO, resulting in effective asset utilization and execution of processes. OCIO will implement innovative practices, such as green IT and cloud computing, to ensure the successful modernization of OPM's IT solutions and infrastructure.

Goal 1 will directly assist OPM modernization programs, such as the Consolidated Business Information System (CBIS), in the review and assessment of 80 legacy systems used to support retirements and trust fund administration. To reduce costs and gain other efficiencies, OCIO will leverage the best of OPM's existing systems while promoting new ideas, such as OPM's Open Government Flagship Initiative, needed to deliver business services across the Agency.

Benefits

- Streamlined operations
- Improved collaboration
- Improved disaster recovery capability

- Cost reductions
- Increased system performance reliability
- Knowledge worker

- Improved information security and privacy
- Energy conservation and environmental awareness
- More informed public and agencies

The following objectives support the achievement of Goal 1:

- **1.1 Data Center Optimization:** Streamline data center operations and infrastructure to eliminate costly redundancies; minimize servers, storage, and application sprawl; simplify day-to-day management and maintenance.

Key Performance Indicator(s)	• Physical to Virtual ratio on servers
	• % data center utilization

- **1.2 Cloud Computing:** Leverage cloud computing technologies, such as on-demand-capacity, to achieve scalability, cost efficiencies, and improved system utilization; tailor technology to business line needs through an appropriate blend of internal and external cloud platforms.

Key Performance Indicator(s)	• # of applications hosted in external cloud(s)
	• O&M dollar savings from previous year due to cloud computing

- **1.3 Platform Modernization:** Minimize and upgrade software versions and develop standardized platforms, including hardware, that result in a more reliable and stable IT environment.

Key Performance Indicator(s)	• % reduction in Hardware/Software/OS platforms
	• # of legacy systems

- **1.4 Shared Services:** Increase agility, modularity, and reuse of systems using open standards and modular architecture to enable more rapid deployment of IT capabilities, such as service-oriented architecture (SOA).

Key Performance Indicator(s)	• Time to Market
	• # of shared services
	• # of systems per shared service

- **1.5 Network:** Improve the performance of OPM's communication/network resources to ensure OPM personnel can access systems whenever and wherever they need.

Key Performance Indicator(s)	• Bandwidth per port (Internal Buildings Only)
	• Bandwidth available into OPM
	• Bandwidth available out of OPM
	• % network availability

- **1.6 Green IT:** Reduce power consumption through the appropriate blend of equipment by implementing green IT practices.

Key Performance Indicator(s)	• Power Usage Efficiency
	• % of IT equipment using "green" settings
	• % of IT equipment that is 'green' certified

- **1.7 OPM Labs:** Implement a highly focused innovation team to develop systems and applications using emerging technologies.

Key Performance Indicator(s)	• # active projects in OPM Labs
	• % of OPM Labs projects brought to market

OPERATIONAL EXCELLENCE

Goal 2: Develop and implement comprehensive IT governance and management practices.

OCIO will continue to develop and strengthen its IT governance processes to ensure that OPM's IT infrastructure supports its mission and the implementation of its strategic goals. OCIO will work to: develop an integrated IT Portfolio Management program; strengthen the Agency's Enterprise Architecture and integrate its use more fully with IT Capital Planning and Investment Control (CPIC); and update its cost estimation and assessment, project management, performance assessment and acquisition processes. OCIO will provide guidance in planning, budgeting, managing, and implementing IT investments and evaluating their cost, status, and effectiveness. OCIO will identify improvements to its IT portfolio in relation to OPM's business needs. OCIO will continue to manage and improve OPM's IT infrastructure, defining technical standards to ensure IT systems are interoperable, leverage existing IT resources where possible and eliminate costly redundancies.

In addition, a number of practices are underway in OCIO business lines that also demonstrate a continued commitment to comprehensive IT governance and management practices. For example, OPM has established a team to review the *Guide to Cost Estimating and Assessment* published by the Government Accountability Office and to establish the processes and tools for using the *Guide* for program cost estimation and budget planning in accordance with OPM policy.

Benefits

• Accountability for ensuring IT initiatives support the Agency's strategic mission	• Standardization of governance procedures for seamless execution of initiatives	• Integrated processes that affect IT planning and implementation
• Clear direction for and expectations of OPM workforce	• Cost savings and avoidance; less redundancy	• Well-informed decision making
• Improved OCIO management function integration and program collaboration	• Successful IT investments	• Achievement of program goals
• Improved information security and privacy		

The following objectives support the achievement of Goal 2:

- **2.1 Governance:** Improve IT governance processes, linking IT investments to the Agency mission and strategic goals with a view to define decision-making processes clearly and assign proper accountability within OPM.

Key Performance Indicator(s)	• % of major IT investments approved by executive steering group

- **2.2 IT Portfolio Management:** Apply integrated planning, budgeting, project management, cost estimation, performance measurement and other information resource management processes to OCIO's IT portfolio to achieve project success.

Key Performance Indicator(s)	• % of major IT investments receiving an overall Green rating on the Federal IT Dashboard (monthly indicator)
	• % of major IT investments evaluated utilizing a "Value vs. Health" criteria

- **2.3 Enterprise Architecture (EA):** Utilize the EA as a management and governance tool to strengthen decision making and standard setting. Coordinate with OPM business lines to ensure technology decisions and implementations for new systems align with the Agency's as well as the Federal government's EA.

Key Performance Indicator(s)	• % of major IT investments compliant/noncompliant with EA
	• # of business/ service capability gaps as identified in the agency EA

- **2.4 IT Acquisition:** Identify opportunities and develop strategies for obtaining IT acquisition cost savings (SmartBuys, optimization, cloud computing, etc).

Key Performance Indicator(s)	• % savings from previous year through "OPM Smart Buyer" program

- **2.5 Risk Management:** Guide modernization activities with sound risk management principles to ensure proper risk mitigation.

Key Performance Indicator(s)	• % of risks avoided or mitigated that are identified on major IT investment risk registers

- **2.6 Compliance:** Establish and maintain IT policies and standard operating procedures (SOP) to ensure compliance with evolving federal legislation and OMB regulations relating to information resources management.

Key Performance Indicator(s)	• % POAMs resolved by the due date
	• % "Maintaining Green" under FISMA quarterly reporting
	• % of systems Certified and Accredited (C&A) under FISMA Annually reporting
	• % FOIA responses that are defined as "backlogged"

- **2.7 Information Security and Privacy:** Sustain a robust information security and privacy management program by implementing and enforcing policies and guidelines. Implement next-generation security tools.

Key Performance Indicator(s)	• % of remote users using 2-factor authentication
	• % of systems with a green status on security ops

| | • All external internet connects are routed through an OMB approved TIC |
| | • Extent of policy deployment and adoption across the organization (e.g.: % of employees signing security policy/attending security training) |

- **2.8 System Development Life Cycle (SDLC):** Upgrade and enhance OCIO's IT System Manager (ITSM) life-cycle framework and tool set (agile development methodologies) to help standardize software and hardware development and management practices.

| **Key Performance Indicator(s)** | • % of system development projects compliant with SDLC framework/standards |
| | • # of systems developed using agile methodology |

- **2.9 Disaster Recovery:** Enhance disaster recovery capabilities for critical OPM business line systems to ensure reliability and accessibility to the OPM community.

Key Performance Indicator(s)	• % of systems recoverable within Recovery Time Objective (RTO)
	• % of critical systems whose DR plans are tested annually
	• % of OPM systems with a Business Impact Assessment as prioritized to OPM missions

MISSION FOCUS

Goal 3: Deliver IT solutions that are customer-focused and driven by the needs of OPM.

OCIO will ensure that all of its IT systems and services are customer-focused. OCIO will address the needs of citizens, federal employees, business, academia and

> *"…Technology for technology's sake is useless. It needs to enable a core mission."*
>
> *Vivek Kundra, Federal CIO*

the Government alike in delivering information effectively across all of OPM's lines of business and program areas. To ensure this, OCIO will make information more readily available and accessible to federal employees and citizens through the implementation of information sharing, knowledge management and collaborative technologies such as portals and social media. OCIO will increase system reuse to eliminate redundancy and excess costs. By improving information sharing across OPM programs, such as the Enterprise Human Resource Integration (EHRI) data warehouse and other RSM retirement data repository, OPM will be able to continue providing excellent service to the federal workforce wherever they may be working. By taking this approach, OPM will enable the efficient use and collaboration of information and data by all OPM customers.

Benefits

• Cohesion between IT and program areas	• Increased efficiency of information delivery	• Increased employee productivity
• Increased accountability	• Increased availability of information	• Modernization of application development tools
• Supports mobile workforce	• Transparency	• Civic Engagement

The following objectives support the achievement of Goal 3:

- **3.1 Mission-Focused Solutions:** Work with program areas to understand business needs, priorities and areas where technology enablers will enhance the performance, value provided and service to customers. Prioritize mission investments based on their alignment and support of OPM strategic goals.

Key Performance Indicator(s)	• Customer satisfaction score

- **3.2 Open Government:** Leverage dashboards, knowledge management systems, Data.gov and social media (wikis, blogs, instant messaging, etc.), among other technologies, to enable transparency, increase accountability and promote informed participation by the public and other Federal agencies on OPM business activities. Improve OPM web presence through external website (opm.gov/open) and internal intranet (THEO).

Key Performance Indicator(s)	• # of data feeds on data.gov
	• Average feed rating on data.gov
	• # of data feed downloads

- **3.3 Mobility:** Implement technology that enables telework and flexible work schedules, increasing employee work-life balance and job satisfaction.

Key Performance Indicator(s)	• # of remote logins per day
	• % of mobile staff
	• % of OPM systems available remotely

- **3.4 Training:** Ensure all OPM employees can effectively use technology tools by implementing a robust, high-quality training program for all OPM employees.

Key Performance Indicator(s)	• # of training classes offered
	• # of employees attending training

WORLD-CLASS WORKFORCE

Goal 4: Recruit and develop the best information and technology management workers in the Federal government.

For OCIO to succeed, it must have a world-class, diverse workforce. This is as true for IT, information management and records management professionals as it is for other areas of the Agency. It is typical for IT shops both in the private and public sectors to fail to put in place the right policies and practices to attract and retain great employees. For example, contractors are procured rather than hiring full-time employees because of the time it takes to hire or because of a perception that certain skills will not be found inside the Federal government. Or, contractors may be given "plum assignments" instead of FTEs who may require additional training or skills development. An organization can sometimes lose valuable employees because there is no perceived career path without leaving the organization altogether.

OCIO must ensure that it is able to attract and retain innovative, highly skilled workers in order to take the Agency to the next level.

Benefits to the OPM Community

- Cost savings and avoidance
- Job satisfaction
- Retention of key knowledge

The following objectives support the achievement of this Goal 4:

- **4.1 Increase Workplace Diversity:** A commitment to hiring a diverse workforce, bringing additional perspectives to OPM and benefiting the broader community.

Key Performance Indicator(s)	• # of non-traditional recruiting channels

- **4.2 Career Advancement:** Structuring the OCIO to allow for career paths (vertical and horizontal), creating positions at many different pay grades and giving current employees opportunities to lead.

Key Performance Indicator(s)	• # of "career ladders"
	• # of leadership opportunities

- **4.3 Professional Development:** A clear and persistent commitment to raising the capabilities of employees, including training opportunities, job rotation and stretch goals to broaden his/her exposure to the full range of knowledge, skills and type of work required to staff an IT organization in order to fulfill its mission.

Key Performance Indicator(s)	• Training dollars ($) per employee
	• # of training hours per employee
	• % of IDP goals met

- **4.4 Internship Opportunities:** Working with the communities in which OPM is located, create opportunities for college and high school kids to learn from and work for OCIO.

Key Performance Indicator(s)	• # of Presidential Management Fellows and interns in OCIO

- **4.5 Engagement with the Broader Community:** Both within the Federal government and outside of it, OCIO will find ways to collaborate with IT and records management professionals. This can include cross-agency projects, work with nonprofits like Code For America and contests that entice civic-minded IT people to help OCIO meet its many challenges.

Key Performance Indicator(s)	• # of cross-agency collaborative projects/ partnerships
	• % increase in collaboration tools

Key Performance Indicator (KPI) Measurement Targets

Table 1 highlights OCIO's IT Strategic Plan objectives and KPIs with designated targets for FY10 – FY13. Each objective directly aligns to one or more KPI. Table 1 demonstrates how OCIO will measure results of the IT Strategic Plan.

Table 1: Key Performance Indicator (KPI) Measurement Targets

Objective: Key Performance Indicator (KPI)	FY10	FY11	FY12	FY13
1.1 Physical to Virtual ratio on servers	1:1	1:5	1:10	1:20
1.1 % data center utilization	30%	50%	75%	75%
1.2 # of applications hosted in external cloud(s)	1	10	20	35
1.2 O&M $ savings from previous year due to cloud computing	5%	10%	10%	10%
1.3 % reduction in Hardware/Software/OS platforms	10%	20%	20%	10%
1.3 # of legacy systems reduced	7	8	11	12
1.4 Time to Market	60d	30d	30d	30d
1.4 # of shared services	10	20	30	30
1.4 # of system per shared service	10	20	20	30
1.5 Bandwidth per port (Internal Buildings Only)	100Mbps	100Mbps	1Gbps	5Gbps
1.5 Bandwidth available into OPM	1Gbps	1Gbps	5Gbps	10Gbps
1.5 Bandwidth available out of OPM	1Gbps	1Gbps	5Gbps	10Gbps
1.5 % network availability	99.95%	99.95%	99.95%	99.95%
1.6 Power Usage Efficiency	1.94	1.8	1.7	1.6
1.6 % of IT equipment using "green" settings	50%	100%	100%	100%
1.6 % of IT equipment that is 'green' certified	50%	75%	90%	95%
1.7 # active projects in OPM Labs	10	50	50	50
1.7 % of OPM Labs projects brought to market	50%	25%	25%	25%
2.1 % of major IT investments approved by executive steering group	100%	100%	100%	100%
2.2 % of major IT investments receiving an overall Green rating on the Federal IT Dashboard (monthly indicator)	90%	100%	100%	100%
2.2 % of major IT Investments evaluated utilizing a "Value v. Health" criteria	90%	100%	100%	100%
2.3 % of investments compliant/noncompliant with EA	100%	100%	100%	100%
2.3 # of business/ service capability gaps as identified in the agency EA	100	80	50	30
2.4 % savings from previous year through "OPM Smart Buyer" program	20%	15%	10%	10%
2.5 % of risks avoided or mitigated that are identified on major IT investment risk registers (updated and monitored monthly)	90%	100%	100%	100%
2.6 % POAMs resolved by the due date	90%	95%	100%	100%
2.6 % "Maintaining Green" under FISMA quarterly reporting	97%	98%	99%	100%
2.6 % of systems Certified and Accredited (C&A) under FISMA Annually reporting	80%	85%	90%	95%

Objective: Key Performance Indicator (KPI)	FY10	FY11	FY12	FY13
2.6 % FOIA responses that are defined as "backlogged"	5%	2%	2%	2%
2.7 % of remote users using 2-factor authentication	30%	90%	100%	100%
2.7 % of systems with a green status on security ops	95%	100%	100%	100%
2.7 All external internet connects are routed through an OMB approved TIC	75%	90%	100%	100%
2.7 Extent of policy deployment and adoption across the organization (e.g.: % of employees signing security policy/attending security training)	90%	95%	100%	100%
2.8 % of system development projects compliant with SDLC framework/standards	90%	100%	100%	100%
2.8 # of systems developed using agile methodology	5	10	20	40
2.9 % of systems recoverable within Recovery Time Objective (RTO)	75%	90%	100%	100%
2.9 % of critical systems whose DR plans are tested annually	75%	90%	100%	100%
2.9 % of OPM systems with a Business Impact Assessment as prioritized to OPM missions	10%	50%	100%	100%
3.1 Customer satisfaction score	85%	90%	95%	95%
3.2 # of data feeds on data.gov	50	100	200	300
3.2 Average feed rating on data.gov	85%	90%	95%	95%
3.2 # of data feed downloads	50	100	150	200
3.3 # of remote logins per day	2000	3000	4000	5000
3.3 % of mobile staff	25%	50%	75%	80%
3.3 % of OPM systems available remotely	95%	100%	100%	100%
3.4 # of technology training classes offered	10	50	100	100
3.4 # of employees attending training	200	2000	2500	3000
4.1 # of non-traditional recruiting channels	2	10	15	20
4.2 # of "career ladders"	5	10	10	10
4.2 # of leadership opportunities	50	100	150	200
4.3 Training dollars ($) per employee	$750	$1,500	$1,500	$1,500
4.3 # of training hours per employee	50	100	150	200
4.3 % of IDP goals met	50%	75%	80%	85%
4.4 # of Presidential Management Fellows and interns in OCIO	5	10	15	20
4.5 # of cross-agency collaborative projects/ partnerships	5	20	25	30
4.5 % increase in collaboration tools	50%	50%	25%	25%

Strategic Alignment

IRM Objectives Alignment to OPM Strategic Goals

Table 2 illustrates the alignment between OPM's IRM Plan goals and objectives. Each objective directly aligns to and assists in the achievement of a specific OPM strategic goal. Table 1 demonstrates how OCIO will strategically enable execution of the Agency mission and vision.

Table 2: IRM Objectives Alignment to OPM Strategic Goals.

OPM IRM Plan Objectives	OPM Strategic Plan Goals			
	1. Hire the Best: Recruit and hire the most talented and diverse federal workforce possible to serve the American people.	**2. Respect the Workforce:** Provide the training, benefits, and work-life balance necessary for federal employees to succeed, prosper, and advance in their careers.	**3. Expect the Best:** Ensure the federal workforce and its leaders are fully accountable and fairly appraised and have the tools, systems, and resources to perform at the highest levels to achieve superior results.	**4. Honor Service:** Ensure comparable recognition and reward for exemplary performance of current employees and honor the careers of federal retirees.
1.1 Data Center Optimization	X			X
1.2 Cloud Computing		X		X
1.3 Platform Modern.	X	X	X	X
1.4 Shared Services			X	
1.5 Network		X	X	
1.6 Green IT			X	
1.7 OPM Labs			X	
2.1 Governance	X	X	X	X
2.2 IT Portfolio Mgt.				X
2.3 EA	X	X	X	X
2.4 IT Acquisition	X			X
2.5 Risk Management			X	X
2.6 Compliance	X	X	X	
2.7 Information Security and Privacy	X	X	X	X
2.8 SDLC	X	X	X	X
2.9 Disaster Recovery			X	X
3.1 Mission-Focused Solutions	X	X	X	X
3.2 Open Government		X	X	X
3.3 Mobility		X	X	X

4.1 Increase Workplace Diversity	X	X	X	X
4.2 Career Advancement	X	X	X	X
4.3 Professional Develop.		X	X	
4.4 Internship Opportunities	X			
4.5 Engagement with Broader IT Community	X	X	X	X

33

IRM Objectives Alignment to Top Management Challenges

Table 3 outlines the top management challenges, both internal and external, as outlined by the Inspector General (IG) for OPM for FY09. OPM's IG Report on management challenges identifies program areas where improvements in IT could help address these challenges. The challenges are mapped to OPM's IT goals and objectives in Table 2.

Table 3: IT Strategic Objective Alignment to Top Management Challenges

	Top Management Challenge	OPM IT Goal(s)	OPM IT Objective(s)
External	Strategic Human Capital	Goals 1, 3 & 4	• 1.4 Shared Services • 3.1 Mission-Focused Solutions • 4.1 Increase Workplace Diversity • 4.2 Career Advancement • 4.3 Professional Development • 4.4 Internship Opportunities
	Federal Employees Health Benefits Program	Goals 1, 2 & 3	• 2.4 IT Acquisition • 1.1 Data Center Optimization • 1.5 Network • 3.3 Mobility
	Wellness and Work-Life Balance	Goal 3	• 3.1 Mission-Focused Solutions • 3.3 Mobility
	IT Security	Goal 2	• 2.1 Governance • 2.7 Information Security and Privacy
Internal	Retirement Systems Modernization	Goals 1, 2 & 3	• 2.6 Compliance • 2.3 EA • 1.5 Network
	Background Investigations	Goals 1, 2 & 3	• 2.1 Governance • 1.5 Network • 3.1 Mission-Focused Solutions
	Financial Management System and Internal Controls for the Revolving Fund and Salaries and Expenses Accounts	Goals 1, 2 & 3	• 2.2 IT Portfolio Management • 1.1 Data Center Optimization • 3.1 Mission-Focused Solutions

IRM Objectives Alignment to Federal Government IT Priorities

Table 4 outlines the Federal Government IT priorities as outlined in the President's Budget. The Federal Government IT priorities are mapped to OCIO's IT strategic objectives. Table 4 is intended to demonstrate how OCIO will strategically address the Federal Government's IT priorities.

Table 4: IRM Objectives Alignment to Federal Government IT Priorities

Priority Area	Federal Government IT Priority	OPM IT Objective
Managing IT Federal Portfolio	Federal Spending on IT	2.2 IT Portfolio Management
	Federal Enterprise Architecture	2.3 Enterprise Architecture
Modernizing Federal and National IT Infrastructure to Be Efficient and Effective	Centralized Provision of IT Services for Non-Military Agencies	1.4 Shared Services
	Cloud Computing	1.2 Cloud Computing
	Data Center Consolidation	1.1 Data Center Optimization
	Leveraging the Federal Government's Buying Power and the Federal E-mail	2.4 IT Acquisition
	Building a Strong Federal IT Workforce	4.1 Increase Workforce Diversity, 4.2 Career Advancement, 4.3 Professional Development, 4.4 Internship Opportunities
	An Efficient Federal Workforce	4.2 Career Advancement, 4.3 Professional Development
	Health Information Technology (HIT)	N/A
	Smart Grid	1.6 Green IT
	Focus on Customer Service	3.1 Mission-focused Solutions, 3.2 Open Government
Transparency and Participation	USASpending.gov	2.4 IT Acquisition, 2.2 IT Portfolio Management, 3.3 Mobility
	Data.gov	3.2 Open Government; 3.3 Mobility
	Geospatial Platform	N/A
	Citizen Services Dashboard	3.2 Open Government, 3.3 Mobility
	Challenge Platform	1.3 Platform Modernization
	Transparency of Research and Development Information	N/A
	Broadband Access for Americans	N/A
Security and Privacy	Securing Government Systems	2.7 Information Security and Privacy
	Identity Management	2.7 Information Security and Privacy
	Protecting Privacy	2.7 Information Security and Privacy

Appendix A: Glossary

1. Capital Planning and Investment Control (CPIC) Process - a management process for ongoing identification, selection, control, and evaluation of investments in information resources. The process links budget formulation and execution, and is focused on agency missions and achieving specific program outcomes. (See OMB Circular A-130, Section 6 at http://www.whitehouse.gov/omb/Circulars_a130_a130trans4/#6.)

2. Government Information - information created, collected, processed, disseminated, or disposed of by or for the Federal Government. (See OMB Circular A-130, Section 6 at http://www.whitehouse.gov/omb/Circulars_a130_a130trans4/#6.)

3. Information - any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms. (See OMB Circular A-130, Section 6 at http://www.whitehouse.gov/omb/Circulars_a130_a130trans4/#6.)

4. Information Management - the planning, budgeting, manipulating, and controlling of information throughout its life cycle. (See OMB Circular A-130, Section 6 at http://www.whitehouse.gov/omb/Circulars_a130_a130trans4/#6.)

5. Information Resources - includes both government information and information technology. (See OMB Circular A-130, Section 6 at http://www.whitehouse.gov/omb/Circulars_a130_a130trans4/#6.)

6. Information Resources Management (IRM) - the process of managing information resources to accomplish agency missions. The term encompasses both information itself and the related resources, such as personnel, equipment, funds, and information technology. (See OMB Circular A-130, Section 6 at http://www.whitehouse.gov/omb/Circulars_a130_a130trans4/#6.)

7. Information System – a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual. (See OMB Circular A-130, Section 6 at http://www.whitehouse.gov/omb/Circulars_a130_a130trans4/#6.)

8. Information Technology - any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. The term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. The term "information technology" does not include national security systems as defined in the Clinger-Cohen Act of 1996 (40 U.S.C. 1452). (See OMB Circular A-130, Section 6 at http://www.whitehouse.gov/omb/Circulars_a130_a130trans4/#6.)

9. Major Information System - an information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources. (See OMB Circular A-130, Section 6 at http://www.whitehouse.gov/omb/Circulars_a130_a130trans4/#6.)

10. Major IT Investment (OPM criteria) – an investment that meets the following criteria:
   a. Is the investment managed by an OPM project manager? (Yes or No) If no, it is not an OPM-

      designated major IT investment.
   b. AND Does it require special OPM management attention for <u>all</u> three of the following reasons? (Yes or No)
         i. The nature of the investment is complex [See Note, below.]
        ii. AND it is important to an OPM policy or program
       iii. AND the investment is a high priority of the OPM Director, the President, Congress or

            OMB
   c. OR does the Exhibit 53 show more than $30 million in DME, steady state or both types of funds over a 3-year period for the investment? (Y/N)
   d. OR is it for financial management and, if so, does it obligate more than $500,000 annually? (Y/N)
   e. Summary: Is it an OPM Major IT investment based on the criteria in a through e, above? (Y/N) If yes, then it is a Major IT Investment.
   f. Is it an OMB-designated Major IT Investment for OPM? (Y/N) If yes, then it is a Major IT Investment, regardless of the answer to question e, above.

11. Records - all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the government or because of the informational value of the data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included. (44 U.S.C. 3301) (See OMB Circular A-130, Section 6 at http://www.whitehouse.gov/omb/Circulars_a130_a130trans4/#6.)

12. Records Management - the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations. (44 U.S.C. 2901(2)) (See OMB Circular A-130, Section 6 at http://www.whitehouse.gov/omb/Circulars_a130_a130trans4/#6.)

13. Legacy System – a system can be considered "legacy" if it meets one of the following criteria:
   a. It consists of one or more components that are no longer supported by a manufacturer.
   b. It is based on a platform or technology that OCIO has made a stated decision to move away from (through EA standard-setting or other means).