

# Strategic Goal 4

---

*Efficient and Effective Information Systems*

## **Strategic Goal: 4 Efficient and Effective Information Systems**

### **Strategic Goal Statement:**

#### **Manage information technology systems efficiently and effectively in support of OPM's mission.**

A significant portion of OPM's budget is spent on information technology (IT). For the most part, these expenditures are dedicated to the development and support of IT systems for specific Human Resource (HR) business functions, such as retirement, background investigations, hiring, etc. The remainder of the expenditures support OPM's workforce to include such tools as email, calendaring, remote access, internet access, file storage, etc. Through the development and implementation of the OPM-wide IT strategy, published in February 2014, OPM is taking steps to manage its IT systems more efficiently and effectively. By taking a corporate approach, OPM will leverage IT capabilities in one program area to support other program areas, benefitting the entire Federal Government.

Given the critical importance of information to HR management, OPM will have a clear, unified IT strategy so that scarce resources are spent wisely based on agency business priorities.

In addition to these actions, OPM has made progress in strengthening its cyber defense and will continue to make this a top priority in FY 2016 and FY 2017. Congressional support will be paramount in order for OPM to secure the Federal Government's data including health insurance information on over 5 million Federal employees, retirees and their families, and payroll records and the official personnel records for the entire Federal Government.

## **Strategy: 4.01 Commit to an enterprise-wide IT systems strategy based on the principle that business drives IT strategy**

### **Strategy Overview:**

OPM will continue to implement a sustainable IT program driven by business priorities, as published in its Strategic IT Plan. OPM will utilize and update the Human Resources Line of Business Reference Model as a framework for process and data standards across the HR life cycle. OPM will also implement its Open Data plan to openly share HR data, both publicly and with key Federal stakeholder communities, such as Federal agencies to the extent consistent with the Privacy Act and other applicable legal requirements. OPM will continue to refine its IT cost accounting, including a business perspective and a technology perspective, to align IT to OPM's mission priorities.

OPM commits to an enterprise-wide IT systems strategy based on the principle that business drives strategy by:

- delivering a framework for a set of standards that supports the entirety of the Human Resources life cycle as documented in the HR Line of Business, Business Reference Model that recognizes and synergizes the technology and tools within OPM, Shared Service Centers, and industry;
- establishing a culture of both openness and trust throughout the HR IT community and among key Federal stakeholder communities by, among other things, taking appropriate steps to safeguard personal information while appropriately using aggregate data; and
- establishing a practice of transparent IT cost accounting throughout OPM.

### **Next Steps:**

In FY 2016, OPM will continue to implement and refine robust service-level agreements for IT services with each stakeholder community to ensure transparency of costs and methods for measuring success. These service level agreements will serve as benchmarks by which costs can be managed and efficiencies can be analyzed. Additionally, OPM will continue to implement its Open Government/Open Data plan.

Further, OPM will build a Digital Service team of experts with modern digital product design, software engineering, and product management skills. The team will manage those OPM digital services that have the greatest impact to citizens and businesses, in alignment with our Strategic IT Plan commitments, to provide improved IT capabilities to agency stakeholders and enhanced IT leadership and governance. By dedicating the team to these services, OPM will not only provide improved services to stakeholders, but also identify practices and tools to improve other OPM services and design future services. OPM has plans to hire a Chief Technology Officer, and during FY 2016, we will identify the high impact, high value services to which the Digital Services team will lend its expertise.

U.S. Office of Personnel Management

In FY 2017, OPM will develop Government-wide HRIT function business requirements for performance management. These requirements will be used to approve performance management providers in category management “hallways.” These hallways will house everything from subject expertise and data, to tools and on-demand procurement assistance for Federal buyers.

OPM will also develop a Government-wide HRIT function Service Component Reference Model for Compensation Management. This model will define standard service offerings for approved compensation management providers in Category Management hallways

Further, OPM will propose updates to the OMB Federal Enterprise Architecture and budget guidance to align with the HR Business Reference Model v3.0 sub-functions, which is expected to lead to increased HRIT spending transparency at agencies and assist in identifying HRIT investments that should leverage shared services.

**Contributing Organizations:**

Chief Information Officer (CIO)

Performance Measure	FY 2013 Result	FY 2014 Result	FY 2015 Result	FY 2015 Target	FY 2016 Target	FY 2017 Target
Percent of HR life cycle for which National Information Exchange Model data standards are published	N/A*	0%	1.37%~	≥5%	≥15%	≥25%
<p><b>Progress Update:</b> In FY 2015, OPM published National Information Exchange Model (NIEM) data standards for 24 of 1,757 data elements in the HR life cycle. While OPM did not achieve this target, the agency is positioned to increase the percentage in FY 2016. The agency needed additional time at the beginning of this project to familiarize the staff with the NIEM standards and implementation process. The team completed the analysis of the HR grouping. With each grouping the process will become more efficient. Data elements not identified in the NIEM Core will be included in other NIEM Domain standards. OPM is working with NIEM to create the NIEM HR Domain, which OPM will oversee.</p>						
Percent of HR lifecycle examined for automation opportunities	N/A*	N/A*	60.0%^	≥5%	≥60%	Discontinued
<p><b>Progress Update:</b> OPM examined 6 of 10 parts of the HR life cycle for automation opportunities. OPM far exceeded the goal of five percent, reaching 60 percent in January. The HR Line of Business reviewed six of the 10 HR life cycles. The agency identified a number of automation opportunities from these reviews. During the first half of FY 2015, HR Line of Business met with the stakeholders and customers, resulting in a decision to focus on updating the Business Reference Model Framework. As a result, OPM shifted focus and the Business Reference Model 3.0 Framework will be published in the first quarter of FY 2016. OPM also defined a new measure to track the publication of standards for the Business Reference Model 3.0 that will replace this measure for FY 2016, as the current measure is of limited use due to the constant change in technology.</p>						

\*N/A - Not Available - no historical data available for this period.

## **Strategy: 4.02 Implement enabling successful practices and initiatives that strengthen IT leadership and governance**

### **Strategy Overview:**

OPM will implement enabling successful practices and initiatives that strengthen IT leadership and governance by:

- enhancing the OPM Director's ability to establish strategy and policy across the HR life cycle;
- enabling the Chief Human Capital Officers Council to work with the OPM Director to translate the HR strategy and policy into business and policy requirements for HR IT systems;
- positioning the OPM CIO as the Federal HR CIO responsible for setting Government-wide HR IT strategic direction and standards for HR IT service providers;
- establishing a flexible capital planning and investment management process within OPM that provides transparency of IT expenditures and IT program/project performance;
- establishing client and stakeholder engagement practices focused on measuring the cost, quality and compliance of Shared Service Center IT capabilities;
- developing an enterprise architecture that supports the HR life cycle as documented in the HR Line of Business, Business Reference Model;
- establishing standards for managing OPM IT programs / projects and providing oversight to measure their performance;
- identifying qualified and trained/certified IT customer relationship managers for each OPM business unit to ensure partnership and collaboration between the OPM CIO and the Associate Directors and Office Heads;
- establishing service level agreements and program plans that document expectations of the CIO and business unit leaders to achieve affordable, responsive HR IT capabilities;
- establishing a data management program that provides greater access to HR data and enables data analytics that informs policy and decisions; and
- incorporating portfolio goals into SES performance management system.

**Next Steps:**

In FY 2016, OPM will refine the CIO organization and IT program focusing on accountability, responsiveness, engagement, transparency, and innovation, to ensure OPM’s IT staff has updated technical and management skills necessary for addressing OPM’s technology opportunities. The agency will also refine the IT governance model to engage more stakeholders, including agencies, in planning of Government-wide HR solutions. OPM will continue to implement robust enterprise architecture to ensure the agency’s technology meets the agency’s complex, integrated business and data requirements. The agency will adopt agile IT principles throughout OPM’s IT portfolio for speed in adapting to evolving policies and business needs. OPM will expand opportunities to enable citizens to better understand Federal career opportunities and Federal agencies to better understand where the best, most diverse talent is located and what motivates them to Federal service. The agency will also strengthen its information security practices to protect the data, and therefore identities and privacy, of Federal employees and their beneficiaries, as well as applicants to Federal positions. OPM will complete the implementation of the first four Continuous Diagnostic and Mitigation controls and dashboard capabilities, and also enforce two factor authentication for 100 percent of non-Personal Identity Verification enabled users. Further, OPM will develop a strategic plan for data.

In FY 2017, OPM will continue with the implementation of Continuous Diagnostic and Mitigation controls. By the end of FY 2017, all appropriate controls will be in place and monitoring the OPM network. Also in FY 2017, OPM will complete the training and/or hiring actions so that 100 percent of the agency’s major investments are managed by a Federal Acquisitions Certification for Program and Project Managers Level 3 certified project manager. Further, OPM will begin the implementation of actions defined in the strategic plan for data that it will develop.

**Contributing Organizations:**

Chief Information Officer (CIO)

Performance Measure	FY 2013 Result	FY 2014 Result	FY 2015 Result	FY 2015 Target	FY 2016 Target	FY 2017 Target
Percent of major investments with IT program managers certified in Federal Acquisition Institute Training Application System	N/A*	N/A*	63.6%~	-	≥80%	100%
<p><b>Progress Update:</b> As of the end of FY 2015, seven of 11 major investments had IT program managers certified in the Federal Acquisition Institute Training Application System. FY 2015 was the first year OPM has used this measure. OPM started the year at 63 percent. Due to resource changes in January, the percentage dropped to 45 percent. Between January and May, two project managers received their certifications, allowing the agency to end the year at 63.6 percent.</p>						

U.S. Office of Personnel Management

\*N/A - Not Available - no historical data available for this period.

## **Strategy: 4.03 Implement enterprise initiatives that leverage capabilities and tools throughout OPM**

### **Strategy Overview:**

Throughout the past year, OPM has placed an increased emphasis on improving its cyber defenses. Simply stated, the goal of cyber security programs is to prevent network intrusions and data breaches. So while we focus on prevention, we also have to focus on improving our ability to detect intrusions, limiting the damage our adversaries might cause, and remediating the issues quickly so that we can adapt to the changing cyber environment and resume normal business operations.

OPM will implement enterprise initiatives that leverage capabilities and tools throughout OPM by:

- consolidating platforms to enhance interoperability and reduce duplication;
- implementing collaboration tools that will provide easy access to all data, information, and systems that individuals are authorized to access, while using the strong controls required for enhanced information security;
- implementing a shared case management solution that provides case tracking and reporting, and workflows;
- implementing a single, virtual data warehouse and sharing capability that better meets business needs while reducing redundancies;
- operating an efficient intranet and providing web services for OPM employees;
- operating an effective secure network, data center, and desktop environment; and
- strengthening financial controls and reporting to enable spending transparency across funding types and programs.

During 2016, OPM IT business and enterprise systems are being measured against the benchmarks for satisfaction, cost, and compliance using a balanced scorecard. These business systems support more than 14,500 users, handle more than 587 million emails, process more than 2.6 million Federal annuitant retirement payment transactions valued at more than \$5.2 billion per month, monitor and prevent more than 30 million network attacks, support more than 5,600 teleworkers, and process more than 2.3 million personnel background investigations. Systems development will leverage shared data among its business systems.

### **Next Steps:**

OPM stores more personally identifiable information (PII) than almost any other Federal agency, including banking information and information collected for background investigations. Being well-positioned to protect this personal information is critical.

OPM intends to create a stronger, more reliable, and better protected network architecture through implemented and sustained agency network upgrades and security software maintenance. To strengthen its defense against cyber security incidents, the agency maintain critical updates that were deployed in FY 2014 and FY 2015. Throughout FY 2014 and FY 2015, OPM has invested and will continue to invest resources to design and build a more modern, flexible, and secure network to meet its mission needs and improve the security and resiliency of its network against cyber-attacks. This updated network must be maintained over time in order to employ the best security tools to protect OPM's IT infrastructure from ever-increasing and exponentially sophisticated network attacks.

OPM continues to partner closely with Department of Homeland Security's (DHS) U.S. Computer Emergency Readiness Team in addressing identified vulnerabilities and is proactively taking steps to enforce and enhance its network security architecture to minimize or eliminate impacts to OPM's IT networks. OPM is working with DHS to implement Continuous Diagnostics and Mitigation using Government-wide Information Security Continuous Monitoring (ISCM) tools to enhance its ability to identify and respond, in real time or near real time, to the risk of emerging cyber threats. Through this implementation, we will automate the following information security capabilities: software and hardware inventories, configuration management, and vulnerability assessments. Continuous Monitoring will also reduce the risk and associated costs of data breaches.

OPM will maintain a sustained security operations center to provide critical oversight of its security posture and real-time 24/7 monitoring of network servers to detect and respond to malicious activity. Further, OPM will use firewalls and storage devices for capturing security log information used for analysis should a cyber-attack occur.

OPM will deploy tools on its network to help with intrusion detection and vulnerability assessment and to incorporate other safeguards that will provide real time information to both strengthen the agency's security and provide OPM the ability to respond more quickly to threats.

With a fully accredited data center platform, the Infrastructure Improvement effort will evolve to support the Federal IT Business Systems team as the applications are prepared for and deployed to the Shell platform. The Shell phase of our IT modernization plan phase includes the design and delivery of a new enterprise architecture and target infrastructure that is simplified, modern and flexible. We have designed the target architecture with security in mind.

Internal OPM applications will be updated to align with the Shell platform, tested for functionality, and placed on the schedule for migration to the new platform, adhering to Information Technology Infrastructure Library based processes. In addition, after an analysis of major systems, the Shell program management office will develop a plan that identifies the migration activities of the major systems. Also as part of the Shell migration efforts, OPM expects to decommission a significant amount of end of life servers and software.

## U.S. Office of Personnel Management

In FY 2016, OPM expects to migrate shared collaboration services, for example, email, personal drives, MS Office applications, advanced collaboration mechanisms, etc., to Microsoft Office 365 and integrate them with the Shell platform to maximize the security protections. This effort will provide OPM's employees the ability to provide efficient web-based systems and software to its employees in a secure manner.

In June 2015, OMB issued a new policy requiring all publicly accessible Federal websites and web services to provide content only over secured connections, with a deadline of the close of 2016 calendar year. OPM intends to comply with this new policy and have all websites and web services connections secured with Hypertext Transfer Protocol Secure, which is the strongest privacy and integrity protection currently available for public web connections. The OPM web services manager will strive to achieve compliance for all of the current websites and services well in advance of the 2016 deadline, and will also check any new sites and services for compliance with this new guidance. OPM will track and monitor all existing and new websites and services on a monthly basis for compliance, and provide the information directly to the Associate CIO for Infrastructure.

In FY 2017, OPM will focus on coordinating the migration of components of the major systems that support external stakeholders to Shell. The migration efforts include the testing and staging of components in accordance with CIO enterprise policy. The phased approach will mitigate the risks associated with transitioning High Availability systems.

OPM will continue to assess and improve the management practices for Shell installed in FY 2016 to maintain the continued benefits. OPM will also continue efforts to strengthen the agency's asset management practices and monitor adherence to them, with special attention on decommissioning legacy hardware and software no longer required by the agency. The agency will also complete configuration for Federal Investigative Services and Retirement Services case management solutions. Further, OPM Web Services will define the strategic path forward for an enterprise content management solution.

### **Contributing Organizations:**

Chief Information Officer (CIO)

U.S. Office of Personnel Management

Performance Measure	FY 2013 Result	FY 2014 Result	FY 2015 Result	FY 2015 Target	FY 2016 Target	FY 2017 Target
Customer satisfaction with OPM infrastructure services	N/A*	N/A*	3 Satisfied	≥3 Satisfied	≥4 Highly Satisfied	≥4 Highly Satisfied
<b>Progress Update:</b> This survey was administered monthly. The response rate was 3.5 percent, with 2,445 respondents. In FY 2015, OPM reached a high rating of four (92 percent), a low rating of two (76 percent), and an average of three (87 percent). The low rating was attributed to the implementation of security measures that impacted the performance of various systems. The agency quickly mitigated this and the rating increased to three (88 percent) the following month.						
Deviation from SLA cost of OPM infrastructure services	N/A*	N/A*	N/A*	Establish Baseline	Establish Baseline	Establish Baseline
<b>Progress Update:</b> Not available. This is a new measure.						
IT security compliance rating for OPM infrastructure services	N/A*	N/A*	1 Unsecure	≥3 Secure	≥4 Highly Secure	≥4 Highly Secure
<b>Progress Update:</b> While the average rating of the security compliance of the six OPM General Support Systems was one (unsecure), OPM took steps towards strengthening the security posture of the agency's systems. During the tactical phase completed in FY 2015, OPM implemented new security tools and increased the agency's ability to scan its systems for vulnerabilities. These tools identified vulnerabilities previously unknown. As a result, OPM accelerated the implementation of the Continuous Diagnostic and Mitigation tools. The initial set of tools will be implemented by end of the second quarter of FY 2016. In FY 2015, OPM began work on the Infrastructure as a Service project. Infrastructure as a Service is designed as a highly secure platform. By the end of the FY 2015, Infrastructure as a Service was available for development and testing, and is scheduled to receive an Authority to Operate in FY 2016.  OPM made strides in improving the security of its infrastructure in FY 2015, but due to the manner in which this measure is assessed, the true security posture is not represented here. This measure only tracks systems listed in the trusted agent system. Some of the categories only measure completeness of a requirement and do not account for quality. The agency is reassessing the methodology.						
Percent of public-facing OPM systems using single sign on capability	N/A*	N/A*	73.3%	Establish Baseline	Establish Baseline	≥80
<b>Progress Update:</b> In FY 2015, 44 (73 percent) of the 60 identified systems made public through <i>opm.gov</i> had single sign on capabilities through Windows Management Instrumentation Command.						
Percent of internal OPM systems using single sign on capability	N/A*	N/A*	N/A*	Establish Baseline	Establish Baseline	Establish Baseline
<b>Progress Update:</b> Not available. This is a new measure.						

\*N/A - Not Available - no historical data available for this period.

## **Associated Priority Goal: Cybersecurity Monitoring**

### **Priority Goal Statement:**

Continue enhancing the security of OPM's information systems by strengthening authentication and expanding the implementation of continuous monitoring.

OPM will increase the use of multi-factor strong authentication in multiple ways. While OPM enforces Personal Identity Verification (PIV) authentication for its internal users, OPM targets PIV usage for OPM services at 50 percent of Federal users by the end of FY 2016. By the end of FY 2017, OPM will enforce multi-factor authentication for 100 percent of all PIV-enabled users and 80 percent of non-PIV-enabled users.

OPM will increase its security posture by expanding the Information Security Continuous Monitoring (ISCM) capabilities throughout FY 2016. Leveraging the Continuous Diagnostic and Mitigation (CDM) program, OPM will expand continuous diagnostic capabilities by increasing the network sensor capacity, automating sensor collections, and prioritizing risk alerts. By the end of the second quarter of FY 2016, OPM will have acquired, implemented, and refined the four (4) CDM controls including vulnerability management, secure configuration management, hardware asset management, and software asset management. These tools will increase OPM's ability to identify and respond to security issues. By the end of FY 2016, 95 percent of OPM's assets will be visible in the CDM dashboard. In FY 2017, OPM will use the benchmarking results to identify and prioritize the implementation of other ISCM controls.

OPM will continue to pursue a number of additional actions as outlined in its Cybersecurity Monitoring goal.



## **Strategy: 4.04 Implement business initiatives that provide capabilities spanning the HR life cycle, allowing OPM and other Federal agencies to achieve their missions**

### **Strategy Overview:**

Implement business initiatives that provide capabilities spanning the HR life cycle, allowing OPM and other Federal agencies to achieve their missions by:

- supporting integrity of background investigations through innovative technology;
- supporting modern IT systems for retirement processing;
- supporting IT service delivery for customer agencies;
- supporting Health & Insurance initiatives; and
- supporting current and planned business initiatives for which IT is an enabler.

During 2015, OPM created a baseline for IT business services to track improvements in effectiveness and efficiency, and will continue to sharpen these improvements during 2016. OPM will expand on the Enterprise Case Management System being developed from resources provided by Congress in 2014 by initiating the migration of legacy retirement processing systems to a common platform shared with other OPM applications. In doing so, the agency hopes to avoid anticipated future cost increases associated with maintaining mainframe hardware and software systems, and mitigate the difficulty in obtaining and retaining personnel with the knowledge of code written in archaic languages. This will also facilitate future incremental retirement processing improvements that take advantage of data gathered by OPM throughout the employee's lifecycle.

### **Next Steps:**

In FY 2016, OPM will build upon the foundational successes in FY 2014 and FY 2015 by continuing to track improvements in effectiveness and efficiency and monitor the IT service metrics baselined in FY 2014 and FY 2015; expanding the use of toolsets, such as the Enterprise Case Management System, to other lines of business to reduce the number of toolsets providing the same functional capability throughout OPM; supporting the Enterprise Case Management System with incremental improvements and further enhancing and leveraging the common platform for Retirement Solutions; and operating and maintaining systems for Retirement Services, OCFO, Healthcare and Insurance and Actuaries. Major projects that OPM will develop during FY 2016 are the Enterprise Case Management System, Online Retirement Application, the data bridge to FACES, and an online natural transaction menu and the Payroll Office Master File replacements. OPM will also implement four major releases of the next generation of the USAJOBS website. The roadmap for the next generation will be approved through the USAJOBS Executive Steering

U.S. Office of Personnel Management

Committee in FY 2015, and the program office will keep the Committee informed of all activities, including any necessary changes that may arise during the implementation phase. Further, the program office will conduct extensive performance testing and usability testing throughout the design and implementation phases to ensure the product meets user needs. OPM will also implement systems to support Healthcare and Insurance’s Multi-State Plan Program.

In FY 2017, OPM will continue efforts to migrate systems to the Shell environment per the migration created in FY 2016. USAJOBS will implement four releases that will result in redesigned job opportunity announcements, a job matching search tool, upgraded résumé center and improved notification/job status capabilities. In addition to the job seeker changes, the agency portal will include enhancements delivered within the same four releases that improve existing data analytics dashboards and launch three new dashboards.

**Contributing Organizations:**

Chief Information Officer (CIO), Employee Services (ES), Federal Investigation Services (FIS), Office of the Chief Financial Officer (OCFO), Merit System Accountability & Compliance (MSAC), Healthcare & Insurance (HI), and Planning and Policy Analysis (PPA)

Performance Measure	FY 2013 Result	FY 2014 Result	FY 2015 Result	FY 2015 Target	FY 2016 Target	FY 2017 Target
Aggregate customer satisfaction rating with OPM IT business systems	N/A*	N/A*	2.5 Below Standards	≥3 Satisfied	≥4 Highly Satisfied	≥4 Highly Satisfied
<p><b>Progress Update:</b> The eOPF survey was administered October 1, 2014 through June 30, 2015 and July 1, 2015 through September 30, 2015. The response rate was 24 percent, with 3,666 respondents.</p> <p>The USAJOBS survey was administered monthly. The response rate was 46.9 percent, with 10,919 respondents.</p> <p>The results for this measure remained consistent throughout FY 2015. It comprised the average ratings of USAJOBS and eOPF. USAJOBS received an average rating of two (73 percent), and eOPF received an average rating of three (87 percent). OPM has determined that the USAJOBS target is not achievable, and will reassess the target.</p>						
IT security compliance rating for OPM business systems	N/A*	N/A*	1 Below Standards	≥3 Secure	≥4 Highly Secure	≥4 Highly Secure
<p><b>Progress Update:</b> OPM started the year with a rating of two and maintained this level for most of the year (October through July). The score dropped to a level of one in August and September. The average rating for the year was two, which is below the compliance standards. While the score was below standards, OPM did take steps towards strengthening the security posture of the agency’s systems. During the tactical phase completed in FY 2015, OPM implemented new security tools and increased the agency’s ability to scan its systems and better detect vulnerabilities. As a result, OPM accelerated the implementation of the Continuous Diagnostic and Mitigation tools. The initial set of tools will be implemented by end of Q2 FY 2016. In addition to these tools, OPM is working to remediate Plans of Actions and Milestones.</p> <p>OPM made strides in improving the security of its systems in FY 2015, but due to the limited manner in which this measure is assessed, the true security posture is not</p>						

U.S. Office of Personnel Management

Performance Measure	FY 2013 Result	FY 2014 Result	FY 2015 Result	FY 2015 Target	FY 2016 Target	FY 2017 Target
represented here. This measure only tracks systems listed in trusted agent. Some of the categories only measure completeness of a requirement and do not account for quality. OPM is reassessing how this measure is calculated.						

\*N/A--no historical data available for these periods