U.S. Department of Justice
Justice Management Division
Office of the Chief Information Officer

DOJ INFORMATION RESOURCES MANAGEMENT STRATEGIC PLAN 2014 – 2016

United States Department of Justice

Published Date: April 2014

This page has been intentionally left blank

Table of Contents

DOJ Information Resources Management Strategic Plan – Fiscal Years 2014-2016

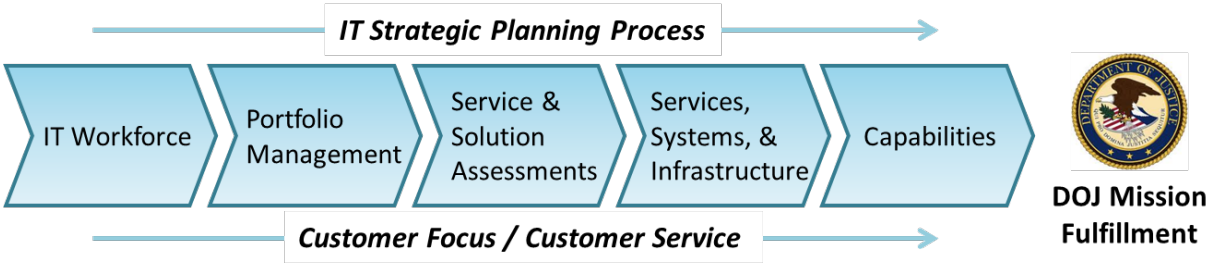
I. CIO introduction and executive summary

On behalf of the employees who are dedicated to serving the Department of Justice's (DOJ's) vital mission through the effective management of our information resources, I am pleased to present this Information Resources Management Strategic Plan for fiscal years 2014 - 2016. The strategic goals and objectives that constitute this plan, summarized in Table 1, were established within the context of the federated model that defines our Department's mission operations. The Office of the Chief Information Officer's (OCIO's) customer groups include DOJ's major law enforcement and litigating component bureaus along with numerous smaller offices across the Department. Each has a vital role to play, and each relies on information technology to accomplish their unique mission.

Unquestionably DOJ's most important customer is the American public. OCIO's efforts, whether indirectly through improving component capabilities or directly through sharing datasets or adding new features to our public Web site, are intended to benefit the public whom we serve. Several goals and objectives are explicitly focused on serving the public, and we will continuously measure and improve our results over time.

This plan, coupled with the DOJ Enterprise Roadmap, establishes the framework that guides how we work with our component bureaus to make the best use of limited funding to operate and maintain our mission systems, applications, and information technology (IT) infrastructure, while investing in promising new technologies and services that advance mission execution. While this plan details the strategic goals and objectives for achieving our vision, the roadmap details specific investments and initiatives where these objectives are applied and measured for progress.

Figure 1 – DOJ Information Resource Management Value Chain



As depicted in Figure 1, the transformation of our IT workforce is foundational to transforming our IT solutions and services delivery model to meet departmental and component mission requirements. First, the portfolio management process will identify departmental and

component priority areas for consolidation as well as new investment. After identifying these priorities, OCIO will work with components to determine the most effective and cost-efficient way to deploy solutions that address them.

This determination will be driven by the new service and solution assessment model OCIO is implementing. This collaborative model will enable the Department and components to determine if requirements can best be met by using a departmental shared service, such as the Justice Security Operations Center (JSOC) for network security; a federal line of business service, such as E-Payroll, provided by the National Finance Center; a component center of excellence, such as the FBI for land mobile radio operations; or a commercial service or solution provider, including cloud computing solutions. For those services and solutions determined to be enterprise commodities, OCIO will serve as a broker to negotiate favorable terms by leveraging the Department's purchasing power.

Once a service or solution determination is made and implemented, the investment becomes part of the Department's IT portfolio management process, and our focus turns to delivering superior performance of the services, systems, and infrastructure that have been deployed. Success depends upon establishing effective governance, management, and analysis for ongoing leadership and process improvement, support and delivery of services, and evaluation and provisioning.

The ultimate goal of these efforts is to use our investments in IT wisely to deliver capabilities to the end user in support of the Department's mission. The pressure to deliver greater, more cost-effective capabilities to end users underscores the importance of being responsible stewards of the taxpayer dollars that fund our investments. In partnership with the component bureaus, DOJ will execute the goals and objectives in this strategic plan in a way that not only optimizes our IT spending, but also delivers capabilities and services to the Department's employees and the public at large.

Kevin Deeley
Acting Chief Information Officer
U.S. Department of Justice
Justice Management Division
Office of the Chief Information Officer

Table 1 – Summary of DOJ IT Strategic Goals and Objectives for FY 2014 - 2016

Strategic Goals	Objectives
1. Institutionalize IT portfolio management	1. Achieve enterprise-wide portfolio optimization 2. Institutionalize strategic sourcing processes 3. Transform and realign the IT workforce
2. Streamline IT operations to better serve customers	1. Deploy enterprise solutions that reduce costs and improve efficiency 2. Identify and rationalize commodity IT services. 3. Invest savings harvested from IT commodity rationalization into new capabilities and innovations that address customer needs 4. Transition the IT service delivery model to a service broker model
3. Enhance IT security	1. Institutionalize appropriate policies and risk-based compliance to assure the security, privacy, and accessibility of data and systems 2. Expand continuous monitoring capabilities to drive risk-based decisions and better inform compliance activities 3. Integrate Identity, Credentials, and Access Management (ICAM) programs 4. Assure a trusted and resilient information and communications infrastructure
4. Deliver innovative solutions to meet customer needs	1. Support component deployment of mission systems to meet specific customer needs 2. Provide mobility services to enhance employees' mission effectiveness and improve service delivery and information access to the public 3. Spur innovation and improve services by engaging the public and making DOJ datasets available
5. Expand information sharing	1. Drive collaboration internally and with the broader law enforcement community 2. Work with the community to develop and use information sharing standards 3. Negotiate sharing agreements and enable shared services with public safety and law enforcement partners 4. Strengthen information safeguarding to protect privacy and civil rights

II. Key drivers

The Department's vision and mission drives OCIO's vision and mission for the management of information resources. In addition to these vision and mission statements, there are several strategic and governance factors that directly impact the formulation of our strategic goals and objectives.

A. DOJ vision and DOJ IT vision

The ***DOJ vision*** is articulated in the Department's strategic plan through three general strategic goals and four priority goals. The three general strategic goals are as follows:

- Prevent terrorism and promote the nation's security consistent with the rule of law;
- Prevent crime, protect the rights of the American people, and enforce federal law; and
- Ensure and support the fair, impartial, efficient, and transparent administration of justice at the federal, state, local, tribal, and international levels.

The four priority goals in the DOJ Strategic Plan are as follows:

- ***National security*** – Increase the number of counterterrorism intelligence products shared by FBI with the broader U.S. intelligence community.
- ***Violent crime*** – Reduce gang violence, by reducing the number of violent crimes committed by gangs.
- ***Financial and healthcare fraud*** – Increase the number of investigations completed per attorney, and track compliance by corporate defendants.
- ***Vulnerable people*** – Increase open investigations on non-compliant sex offenders; increase resolutions of sexual exploitation and human trafficking investigations; increase number of children identified by the FBI in child pornography.

The ***DOJ IT vision***: The DOJ OCIO will assist the components in executing their missions and improve the efficiency and effectiveness of the DOJ through world-class use of information technology.

B. DOJ mission, DOJ IT mission, and DOJ OCIO mission statements

DOJ mission: To enforce the law and defend the interests of the United States according to the law; to ensure public safety against threats foreign and domestic; to provide federal leadership in preventing and controlling crime; to seek just punishment for those guilty of unlawful behavior; and to ensure fair and impartial administration of justice for all Americans.

DOJ IT mission: The mission of the DOJ Chief Information Officer (CIO) and the Office of the Chief Information Officer (OCIO) is to provide IT leadership across DOJ by:

- Identifying and facilitating the delivery of multi-component (enterprise) IT services that drive higher value than independent silo solutions;
- Enhancing the value of the IT portfolio through ongoing assessments and continuous improvement of existing IT assets and vendor relationships;

- Minimizing reporting overhead through standard gathering of information and reporting of same—driving to ensure that overhead activities recognize realities and deliver sufficient value;
- Deploying and driving a multi-level risk management process to ensure that problems are detected and addressed as early as possible;
- Creating, through the CIO Council, standards, policies, and architectures that support the IT vision; and
- Performing all necessary IT tasks to support the Justice Management Division (JMD) and the DOJ executive levels.

DOJ OCIO mission: To support the successful execution of the DOJ component missions and improve efficiency and effectiveness of DOJ processes through world-class use of information technology (IT).

C. Strategic drivers

Table 2 describes key strategic drivers, both from internal and external sources, and their effects on our strategy.

Table 2 – Impact of Drivers on DOJ's Management of IT Resources and Goal Setting

Driver	Impact	Internal/ External
Constrained federal budget	Identifies the need to show value, better articulate cost drivers, and to lower operating costs without threatening mission-critical functions.	External
Shift to centralized delivery of IT capabilities and use of enterprise platforms	Places greater emphasis on identifying standardized technologies to deliver at the enterprise level and achieving efficiencies through economies of scale and reduced duplication of efforts.	Internal
Evolving business requirements of DOJ services and component agencies	Defines the need to engage mission and business customers in governing IT investment management.	Internal
Customer demand for emerging or maturing technology	Demands that IT leadership continually assesses the risks of adopting new technologies too soon or staying with legacy technologies too long.	External
Workforce challenges due to changes in technology and business needs, recruitment challenges, and the need to maintain institutional knowledge	Compels DOJ to ensure the right people with the right skill sets are recruited and retained to support our IT mission needs.	Internal

D. Governance drivers (federal directives)

The development of this strategic plan was informed and guided by a number of important federal and departmental initiatives. First and foremost, this plan supports and aligns with the Department of Justice Strategic Plan for Fiscal Years 2012-2016. The overarching goal of the Office of the Chief Information Officer in its management of the Department's information technology (IT) resources is to support the mission of the Department through the fulfillment of the goals outlined by the Attorney General. The five goals in this plan deliver on the IT goals listed in the Department's strategic plan.

The departmental IT goals in the DOJ strategic plan were developed in consultation with OCIO and serve as the foundation for the goals and objectives in this plan. Also informing this plan are the DOJ components' IT strategic plans as well as domain-specific plans such as the DOJ Digital Strategy and DOJ IT Security Program Management Plan.

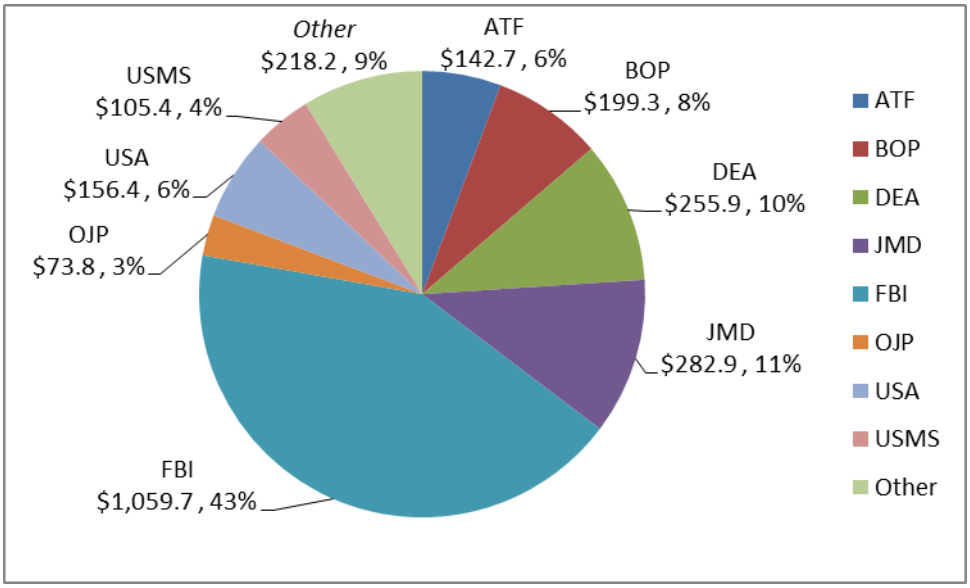
At the federal level, the Department's strategic planning efforts are informed by the Office of Management and Budget's (OMB's) PortfolioStat initiative, launched in March 2012 and directing agencies to assess the effectiveness of their IT management practices and identify areas for improvement. Complementing PortfolioStat are several federal initiatives that further guide the goals and objectives in this strategic plan, including the Federal Shared Services Strategy; OMB Digital Strategy; 25 Point Implementation Plan to Reform Federal Information Technology Management; Committee on National Security Systems (CNSS) directives; and the National Strategy for Information Sharing and Safeguarding.

Key legislative drivers include the Government Performance and Results Act (GPRA) of 1993, which calls for five year strategic plans, project management process improvements, and annual performance goals; as well as the Clinger-Cohen Act of 1996, which calls for improved acquisition and management of agencies' IT resources and strengthens the authorities of the agency Chief Information Officer.

III. DOJ IT enterprise summary

The Department's IT budget is allocated according to our federated model, whereby each component bureau requests funding for the operations and maintenance (O&M) of existing services, systems, and infrastructure, as well as funding for new investments. As part of the annual budget process, the Department's CIO works with component bureau IT leadership to set spending priorities and identify areas for cost savings, increased spending, and new investments. Figure 3 illustrates how the Department's IT spending is spread across numerous components.

Figure 3 – Major Component IT Spending (FY13)

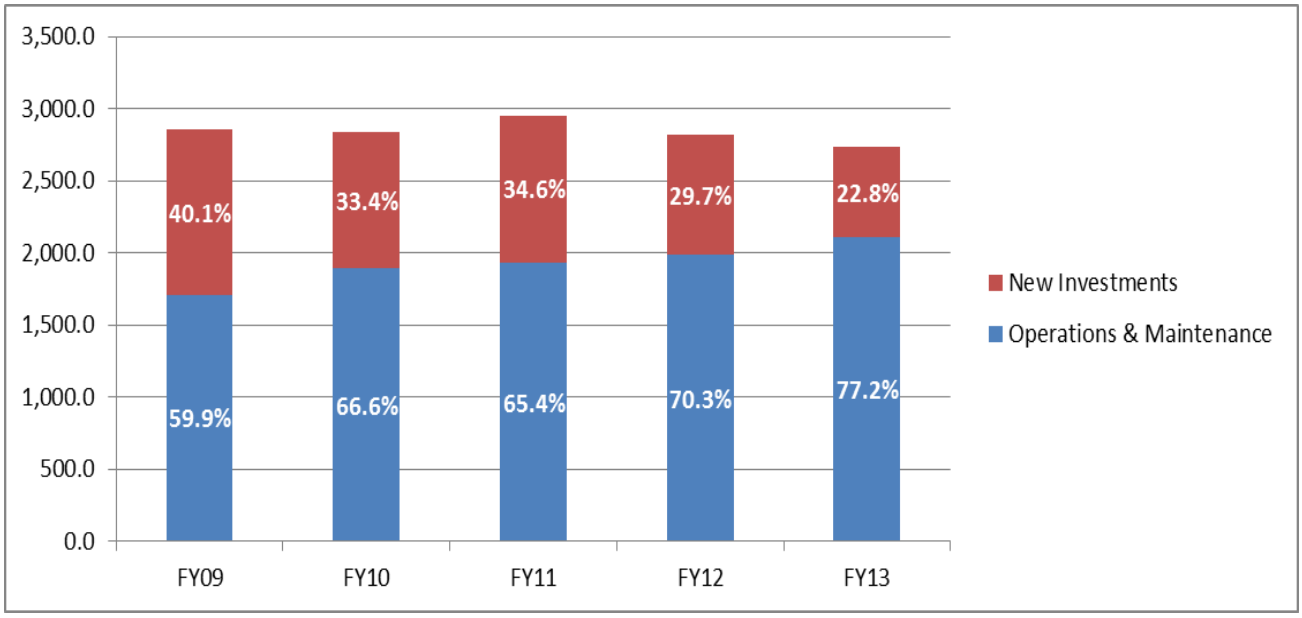


$ in millions

The Department's overall IT budget was reduced by more than $200 million over the last three fiscal years, from $2.95 billion in fiscal year (FY) 2011 to $2.73 billion in FY 2013. As depicted in Figure 4, O&M expenses continue to rise annually and consume a greater percent of the IT budget, significantly constraining funding for new investments. Simultaneously, the demand for IT services and capabilities perpetually increase as technology evolves.

This dynamic is the primary driver of our strategy to institutionalize an IT portfolio management program that results in streamlined operations and cost savings that, in turn, frees additional funding for investments in new services and capabilities. Simply put, we must do more with less.

Figure 4 – DOJ IT Spending FY09-FY13



$ in thousands

IV. Guiding principles

In defining and executing these goals and objectives to further the Department's mission, the OCIO and its counterparts in the component bureaus are guided by four principles:

1. **Seek first to understand the customer** – Because the most effective technology solutions are those that meet users' requirements where their business is conducted, OCIO will ensure customer voices are heard, not just during the identification, design, and development of solutions, but also after deployment to ensure effective use and continual improvement.

2. **Provide exemplary customer service** – OCIO's customers expect IT services to be delivered the same way electricity is: always on, always available, always performing. Both internal DOJ customers and the American public maintain high expectations of DOJ services, from network connectivity and mobile device support, to easy and efficient search capabilities. OCIO will meet these expectations and measure our performance as we do so.

3. **Share first** – To maximize the use of limited IT budgets and prioritize funding for new investments across the Department, OCIO and component IT leadership will work together to identify solutions and services that can be shared across the enterprise while continuing to support solutions and services that address unique requirements.

4. **Improve continuously** – As OCIO strives to listen to and serve our customers better, continuous improvement strategies will be a fundamental part of our strategic planning, portfolio management, and performance management processes.

V. Strategic goals and objectives

Strategic Goal 1: Institutionalize IT portfolio management

An effective IT investment management program is a foundational goal that strengthens the Department's ability to achieve its IT goals and objectives in support of the Department's mission. The Department is evolving its approach from a program- and project-focused model, which targets specific high-dollar and/or high-priority IT investments, to a cascading model that includes portfolio management in addition to program/project oversight. This new model enables a departmental view of investments across the enterprise, including component investments. Investments will be categorized and managed within four major portfolios:

- IT infrastructure and enterprise systems;
- Enterprise business systems;
- Mission systems (primarily operated by components); and
- Security systems (summarized below).

Table 3 – Departmental IT Portfolios

IT Portfolio	Focus Areas
Infrastructure and enterprise systems	Reduce costs of "commodity" IT (data centers, email, mobile devices, and telecom networks)
Enterprise business systems	Improve service delivery and effectiveness by implementing common systems across the department: finance, grants management, human resources, and property management
Mission systems (primarily operated by components)	Strengthen components' systems used to achieve their mission and seek opportunities for cross-component sharing; advance implementation of data standards
Security systems	Perpetually strengthen cyber security programs and system applications; advance implementation of Identity, Credential, and Access Management (ICAM)

By implementing an enterprise-level portfolio model, the Department expects to realize significant cost savings and cost avoidance by rationalizing redundant and commodity investments and from more efficient vendor management. These efficiencies will optimize the use of limited resources to fund IT investments and provide new capabilities that will improve the Department's mission effectiveness.

Executing a portfolio model requires an IT workforce that is responsive to dynamic technology trends even as it manages existing investments, and the Department will continue to prioritize the retention and development of our dedicated IT workforce.

Objective 1.1 – Achieve enterprise-wide portfolio optimization

Portfolio approach to governance leverages enterprise scale. A portfolio approach utilizes value and risk measurements to enable prioritization, planning, and investment decisions to be made for a segmented group of functionally-similar investments called "portfolios." Portfolios are a method of organizing the enterprise IT portfolio into smaller, more manageable groups of investments that can be aligned with a target architecture and roadmap, thus rationalizing the portfolio and identifying areas both for greater investment and for consolidation. This process maximizes investment discipline and optimizes use of available IT funding.

IT governance enables DOJ to maintain continuous alignment among its IT investments, programs, and projects as well as the Department's mission priorities. Building upon the enterprise and program/project governance model already in place, the Department is maturing its portfolio management approach to provide oversight across the enterprise for categories of investments within a portfolio. This refined governance model provides a cascading approach that optimizes technological capabilities as well as services and resources across programs, projects, portfolios, and the enterprise.

To date, the Department has established ten commodity area working groups focused on IT functions, such as data centers, email, and mobility. These working groups are responsible for assessing and making recommendations to the DOJ CIO Council, comprised of component CIOs and chaired by the DOJ CIO, to address the current state of the Department's investments within commodity areas, identify opportunities for consolidation and cost savings, and manage against milestones, budgets, and performance metrics.

Value measurement key to decision making. To assist the commodity working groups in targeting capability gaps and investment duplication, DOJ is implementing a value measurement process. The primary objective of the value measurement process is to increase the value of IT investments while measuring and minimizing risk. To achieve this objective, process, commodity, and component working groups identify underperforming and low-value investments for re-scoping or termination, while innovative, high-value investments (e.g., shared services and/or cost-effective cloud-based solutions) are scored for risk and prioritized for funding. Mapping an investment's value to agency goals and priorities, along with capturing its expected return on investment, alignment with the architecture roadmap, and compliance with security controls, is key to defining an investment's value.

In concert with the value measurement approach, the Department is implementing a "cut, keep, and invest" strategy. The purpose of the "cut, keep, and invest" strategy is to harvest funding on an annual basis from existing investments for investment in innovative and/or high-value solutions. Recommendations on both existing and proposed programs are made by components' IT leadership for component-level investments, departmental commodity working groups for enterprise-level investments. These recommendations are brought first to the components' investment review board, then to the DOJ CIO Council for approval of enterprise-level commodity investments.

Metrics advance agency performance goals. Consistent with Government Performance and Results Act of 2010 (GPRA) directives and in order to provide transparency into value measurement and "cut, keep, and invest" outcomes, the Department aligns IT investments to departmental strategic goals and publishes investment performance metrics to the Federal IT Dashboard and DOJ Dashboard, both of which are publically accessible. To further advance performance goals, the Department plans to establish more quantitative and transparent investment selection, reporting, and monitoring metrics and processes. This process improvement will provide component IT program management, business and mission sponsors, and departmental leadership with objective measures of expected business value, project progress, and program results to enable better decision making for investment funding and continuance.

Monitoring and improving customer service. In addition to performance metrics, the Department's OCIO is developing a customer service evaluation program to ensure the Department's enterprise, business, and security systems are meeting departmental and component requirements. OCIO will use an initial, broad-based survey in 2014 to baseline customer satisfaction, then conduct regular follow-up surveys that will identify perceived or real gaps for OCIO to address. When tracked together over time, performance and customer satisfaction metrics will enable the Department to identify opportunities for improvement in the delivery of customer-facing services and thereby help achieve the strategic goals detailed in this plan.

The DOJ CIO and component involvement. The DOJ CIO has adopted a partnership approach to working with the components in order to carry out assigned CIO responsibilities, most of which are detailed in the Clinger Cohen Act of 1996, OMB Circular A-130, Federal Information Security Management Act of 2002, OMB Memorandum M-11-29, and DOJ 2880.1c, Information Resources Management Program Order. For example, the CIO established an IT security program that relies on component compliance, involvement in working and governance bodies, and shared resource commitments such as the Justice Security Operations Center.

Reductions in IT budgets at the Department and component level, along with OMB's PortfolioStat program, have reinforced the CIO's responsibility for driving IT efficiencies and cost savings. This impetus prompted the CIO to elevate components' involvement in Departmental IT resource management, including a greater decision-making role for the DOJ CIO Council (see description below) and greater involvement on IT commodity teams. The DOJ CIO is supported in this regard by the Deputy Attorney General and the Assistant Attorney General for Administration, who heads the Justice Management Division (JMD).

Program governance. The Department's program governance process is a flexible, adaptable, and repeatable approach that provides program oversight throughout key milestones in the program/project lifecycle. DOJ provides investment and program oversight through sound capital planning, utilization of structured system development life cycle processes, and project management and control processes that focus on cost, schedule, and quality of project delivery.

Risk and performance are assessed throughout the system development and maintenance life cycle and through Department Investment Review Board (DIRB) and TechStat Accountability Session reviews, which focus on the performance and return on investment of selected IT investments.

The scope of these governance processes are detailed in DOJ's Information Resources Management Program Order 2880.1c, the DOJ policy governing the planning, acquisition, security, operation, management, and use of IT resources.

Governing bodies. The DIRB is the highest level of governance over the IT investment portfolio and is co-chaired by the Deputy Attorney General and the CIO and includes senior executives from OCIO and the Justice Management Division budget office. The DIRB meets on a regular basis to review selected investments and programs that have the largest budgets and/or are critical to the mission of the Department or individual components. To increase stakeholders' transparency into the Department's investments, the Department will expand DIRB membership to include component executives and other mission and business leaders.

The DOJ CIO Council also plays a key role in the governance process. Investments in enterprise commodities, along with approvals for IT standards, fall under the purview of the DOJ CIO Council, which meets monthly and is comprised of component CIOs from across the Department. Enterprise Architecture's (EA's) role with the commodity working groups will continue to evolve, and as the Department moves to a service broker model, EA will play a larger role in standards alignment and competitive benchmarking. The Department's Procurement office also plays a key role by supporting the requirements for strategically sourced hardware, software, equipment, and services.

Maturation of the approach. Proper oversight and governance of IT investments and projects maximizes the effective and efficient use of DOJ resources and enables improved decision making that promotes investments that achieve mission outcomes. Investment management policies and procedures, such as DOJ's Information Resources Management Program Order 2880.1c and the IT Governance Guide, along with the Department's system development life cycle are being updated to reflect the portfolio management approach. Future maturation of the approach will include developing a standard procedure for value measurement and "cut, keep, and invest" activities, further strengthening the role of the DOJ CIO Council, establishing cross-cutting teams to address mission-focused categories of investments, evolving the role of the Department Investment Review Board, and chartering additional governance bodies at agency executive level to provide strategic input into the planning and requirements processes.

Future program- and project-level governance enhancements will include an analysis of the criteria for designating "major" investments as well as a reworking of the internal project status reporting and management dashboard tools based on best practices in government and industry.

Service delivery model. Another important initiative to help achieve enterprise-wide portfolio optimization is a service delivery model whose purpose is to broker common IT services across the enterprise. As DOJ increasingly leverages shared services as well as cloud and "cloud-like" services both within and outside of the Department, the need for service brokerage becomes apparent, enabling the Department to speak with one voice when negotiating enterprise services. In order to ensure the Department is receiving the best value for its dollars, an IT broker will act as an intermediary for the Department's components, serving to negotiate for the best pricing, service levels, and customer-focused solutions.

Objective 1.2 – Institutionalize strategic sourcing processes

Propelled by the imperative to achieve more with fewer resources, the Department's vision for strategic sourcing has led to the establishment of a Vendor Management Office (VMO) concentrated on the "smart buying" of IT infrastructure. The VMO provides centralized guidance and prioritization for the Department's decentralized strategic sourcing and commodity purchasing initiatives, utilizing the collective buying power of the entire Department and its components. The VMO features broad representation, including procurement, legal services, and various business units, in addition to IT entities, to help reduce costs and optimize value.

An important part of this effort is to leverage the service broker model and negotiate favorable terms for enterprise licenses with software vendors, which will result in measurable cost savings. DOJ will continue to be a leader in government-wide efforts to consolidate enterprise licenses and leverage greater buying power for software as well as commodity IT, such as email systems. The VMO will lead and assist in the analysis of procurement data and strategies; become the central repository of enterprise procurement vehicles; identify and communicate internal and industry best practices; provide expertise to assist in pricing analysis, procurement strategies, and negotiations; and communicate with strategic external vendors, partners, and other government agencies.

An example of the benefits of implementing a strategic sourcing strategy is the consolidation of the Department's wireless services contracts in 2013, in support of the federal Digital Government Strategy. After analyzing existing contracts across the Department, OCIO identified those with the most favorable terms and worked with components to negotiate their transition to one of three component contracts that are the most cost effective, resulting in cost savings thus far of more than $4 million. The Department will continue to pursue similar consolidation and cost savings.

Objective 1.3 – Transform and realign the IT workforce

DOJ's IT workforce delivers for our customers every day. In the past, IT organizations were focused on building new systems and providing ongoing support for those systems. Whether the systems were custom built or provided as a commercial-off-the-shelf (COTS) package, the IT workforce supported every aspect of building and maintaining a variety of technical platforms

and custom systems. As technology and delivery models have evolved, the skillsets needed by our IT workforce have become more varied.

To meet these evolving skill requirements, the OCIO will continue to implement IT workforce initiatives that transform our workforce to operate effectively in a traditional IT provider model as well as new service and solution delivery models, all while continuing to meet our customers' needs. The ongoing IT model still includes internal system development, while the new models increase emphasis on acquisition management, sharing solutions across DOJ's components, and making use of cross-government centers of excellence for specific services.

To assist with this transformation, we will provide training on new skills to the current workforce and recruit new talent to meet priority skill requirements. Special focus will be given to comprehensive skillsets that include change management and program management at the Department level. These skillsets are crucial for supporting a more resilient and agile IT environment enabled by component-level shared solutions and deployment of new technologies.

OCIO will continue to attract, retain, and develop high-caliber IT professionals through new and ongoing efforts, including identifying new and under-represented skillsets; succession planning; defining IT and program management career tracks; implementing staff development programs; and establishing a mentorship program.

DOJ IT accessibility / Section 508 compliance program

To be successful at recruiting, retaining, and transforming our IT workforce, we must foster an inclusive environment that enables individuals at all levels and capabilities to thrive. A key element of fostering this inclusive environment is implementing measures to ensure compliance with Section 508 of the Rehabilitation Act of 1973, the purpose of which is to make IT accessible and effective for people with disabilities.

The Department's Section 508 compliance is administered as a decentralized program with primary responsibility delegated to the components. As the Department coordinator for Section 508 compliance, OCIO assists components with addressing Section 508 compliance by reviewing IT solicitations for inclusion of appropriate Section 508 requirements, assisting with IT solution compliance testing, and coordinating accessibility training for IT and program staff. These efforts also are described in more detail in the DOJ Enterprise Roadmap.

To build workforce skills that support an environment where Section 508 requirements and responsibilities are understood and enforced across the enterprise, the Department has undertaken a number of specific actions that align with the Strategic Plan for Improving Management of Section 508, released in January 2013 by the Executive Office of the President. Among these actions include the following:

- Developing a department-level Section 508 policy order and guidance to clarify expectations and provide direction on implementing the policy, as well as defining new Section 508 program roles for key Department stakeholders;

- Developing a Section 508 strategic plan and program management plan to define the direction and goals of the Department's Section 508 compliance, as well as the structure, roles and responsibilities, and near-term program objectives;
- Preparing a plan for completing the Section 508 baseline compliance assessment; and
- Conducting Section 508 awareness training, as well as Section 508 compliance training for administrative and Web content development staffs.

Strategic Goal 2: Streamline IT operations to serve customers better

DOJ's IT capabilities exist to serve the Department's customers, and as technology evolves and new solutions and innovations become available, the Department must constantly look to streamline existing systems and applications to ensure they remain effective and efficient while also providing new capabilities to customers. When conducted within the context of an IT portfolio management program, this approach enables the Department and its components to deploy solutions that reduce costs and improve efficiencies, identify and rationalize commodity IT services, and invest savings from these efforts in new solutions and capabilities.

Objective 2.1 – Deploy enterprise solutions that reduce costs and improve efficiency

The Department recognizes that enterprise IT solutions are a key method for delivering effective IT capabilities when common requirements exist across organizational boundaries. Consistency across the organization improves interoperability, and pooling the buying power of a large organization delivers reliable, scalable, and cost-effective solutions. DOJ was an early adopter of enterprise solutions in the areas of IT infrastructure (e.g., Justice Unified Telecommunications Network (JUTNet) Wide-Area Network and Trusted Internet Connection (TIC)); enterprise IT (e.g., Justice Security Operations Center (JSOC)); and business systems (Unified Financial Management System (UFMS)). DOJ will continue to identify and evaluate opportunities to utilize enterprise solutions to support the mission. Leveraging, expanding, and replicating the success of existing enterprise shared service solutions is at the core of the Department's enterprise solutions efforts.

To enable transparency and ensure the effectiveness of this process, new system initiatives will be subject to a cost-benefit analysis of the value of the new service as compared to the existing service (if one exists). The analysis will include financial, operational, and business incentive considerations.

To ensure critical enterprise systems and applications are supported in the event of a disaster or severe disruption, the Department maintains a list of mission essential systems and has defined protocols and processes for their continuity of operations and disaster recovery. The Department uses a risk-based approach to determine which systems and applications are the most critical to the operations and fulfillment of the Department's mission. A list of these systems is contained in the Department's Enterprise Roadmap.

Objective 2.2 – Identify and rationalize commodity IT services

DOJ will utilize an inclusive, cross-component approach for continuous evaluation of our various IT portfolios. DOJ established commodity area working groups in 2012 to evaluate priority commodity IT portfolio areas and develop multi-year plans for rationalizing them. Working groups are already assigned to portfolios within the commodity areas of infrastructure (data centers, end-user computing, mobility, and telecommunications), enterprise IT (email, collaboration, identity and access management, IT security, and Web hosting), and business systems (financial management, grants management, and human resources management). These groups are charged with evaluating their portfolios and identifying opportunities to rationalize them through enterprise solutions, shared acquisition channels, shared infrastructure, shared applications, and use of "as a service" offerings.

Infrastructure portfolio – The Department has already demonstrated success in consolidating Wide Area Network (WAN) services through the JUTNet program and the Trusted Internet Connection (TIC) initiatives. DOJ also will continue to consolidate and transform data centers and identify a set of core enterprise data center facilities that offer a suite of scalable enterprise services to all components at a significant cost savings. For end user computing, which includes desktops, printers, and mobile devices, the Department will fund pilot programs for managed seat services, thin client computing, bring your own device (BYOD), and strategic sourcing to determine where the greatest cost savings can be achieved while maintaining high service levels.

Enterprise systems portfolio - The Department will focus on email, collaboration, and cyber security. The Department currently uses multiple email systems to support 150,000 users, and by consolidating the number of systems, the per-user cost reductions will result in potential yearly savings of several million dollars. The first phase of this effort will implement a cloud-based offering for one component as a proof of concept, while concurrently consolidating the email systems of multiple small offices and litigating divisions onto a single system and adding enhanced user collaboration tools. While the Department's security program is already centralized, the Department is exploring consolidating night and weekend monitoring at the two security operations centers to gain efficiencies, as well as working with the Vendor Management Office to reduce anti-virus and data protection software licensing costs.

Business systems portfolio – The Department will primarily focus on the United Financial Management System (UFMS), which is the new enterprise financial management system, a consolidated human resource system offering, and a shared grants management platform. The UFMS initiative has been underway since 2008 and is already producing cost and user efficiency benefits through consolidation of components' financial systems. Before 2008, the Department operated six separate core financial management systems. As a result of this consolidation effort, the Department has already reduced the number of systems to four in 2013 and will consolidate further to three systems in 2014.

For human resources systems, the Department already uses a shared service center that provides payroll processing and benefits processing for the entire Department. To augment savings gained from this shared service, the Department will continue to evaluate opportunities

for consolidating additional human resources functionality to enterprise-wide platforms and managed services.

For grants management, the Office of Justice Programs (OJP) and Office on Violence Against Women (OVW) use a shared system, while a third grant making organization—Community Oriented Policing Services (COPS)—uses a separate system. Collectively, these three components support approximately $3 billion in grants annually, and the Department will explore the feasibility of consolidating these systems onto a shared platform.

Objective 2.3 – Invest savings harvested from IT commodity rationalization into new capabilities and innovations that address customer needs

Beginning in FY 2014, DOJ will redirect five percent of the Department's IT base resources annually into a reinvestment pool for investment in IT projects that will produce a favorable return on investment or demonstrably improve citizen services or administrative efficiencies, serving to institutionalize a process of funding innovative and transformative IT projects through savings.

Under this reinvestment approach, each component will be required to set aside five percent of IT spending, as reported on the OMB Exhibit 53, to establish an annual pool for reinvestment in enterprise IT projects and efficient IT projects within each component. Components will participate in the investment decision-making process for allocating these pooled funds.

This reinvestment approach has several key benefits. First, it strikes an appropriate balance between empowering component CIOs with giving the DOJ CIO authority over enterprise IT investment. Second, it pools the Department's purchasing power without taking funds from components' base budgets. Third, it challenges components to find efficiencies and consider potentially less-expensive, enterprise-wide solutions. Fourth, it provides a means to redirect funds from lower-value operations and maintenance (O&M) spending to higher-value IT investments, including those proposed by the commodity area working groups, without reducing base resources. Finally, the approach adds transparency to Department-wide projects, allowing components to review and collaborate on planning and implementation.

Objective 2.4 – Transition IT service delivery to a service broker model

Central to streamlining the Department's IT operations is the transition to a service broker model for delivering IT services. Every departmental component depends on IT infrastructure services, such as data center operations, email, and network management to support its mission operations. Historically, the Department's OCIO has had primary responsibility for providing these infrastructure services. Under the new model, OCIO will transition from a service provider model where services are designed, built, and run in-house, to a service broker model whereby OCIO works with components to identify requirements and then selects the most effective and cost-efficient provider to meet those needs.

The Department's current service delivery model itself represents significant progress from the previous in-house development model that accommodated customized IT solutions to meet discrete requirements instead of pursuing shared or third-party solutions. Today's solutions

are often delivered as a service, and the rapid rise of mobile platforms and cloud computing has enabled large, complex enterprises like DOJ to adopt new delivery models that are less expensive yet provide greater, more reliable capabilities.

The new broker model will streamline current operations further by centralizing service acquisition and management within OCIO and enabling component IT leadership to focus on supporting their component's core mission. The Department has already demonstrated early success in implementing this model with JUTNet, a managed network service, as well as the migration of components' legacy email systems to the cloud.

To implement a successful service broker model, the Department must have skilled personnel to serve as service managers (see Objective 1.3–Transform and realign the IT workforce), and the service managers themselves must be highly customer-focused in order to effectively balance departmental cost-savings equities with component interests and requirements.

Strategic Goal 3: Enhance IT security

DOJ's IT security program is highly effective and exemplifies numerous industry and government best practices. Given the evolving nature of the cyber threat and adversaries' constant targeting of DOJ and component networks, it is imperative for the Department to continuously improve and strengthen its security posture. To do so, we will institutionalize risk-based security polices and ensure enterprise compliance, expand continuous monitoring capabilities, integrate Identity, Credential, and Access Management programs (ICAM) into our security program, and assure a trusted and resilient information and communications infrastructure.

Objective 3.1 – Institutionalize appropriate policies and risk-based compliance to assure the security, privacy and accessibility of data and systems

The foundation of the DOJ IT security program is built on the appropriate mix of policy and compliance activities to govern the use and protection of our data and systems. However, the impacts associated with reduced resources, the fluidity of cyber security legislation, the proliferation of mobile devices, and the drive towards shared services necessitates that we carefully examine their effect on our delivery of reliable and secure IT services and on IT security policy and compliance efforts.

To keep pace with consumer demand, new commercial products are often developed without the requisite security incorporated, resulting in inherent vulnerabilities. Although these technologies offer greater flexibility and cost savings they are not absent risks. Such risks coupled with reduced resources create opportunities for our adversaries to compromise our data and systems. As stewards of taxpayer dollars and data we will maintain an ongoing awareness and understanding of these risks and others to further inform our efforts and ensure the appropriate mitigations.

We will develop and enforce a blend of policies and activities that are practical, enhance our secure posture, and comply with regulatory mandates. Our continued work across government

and with private industry has equipped us with a broad perspective that will enable us to responsibly leverage new technologies and services.

Objective 3.2 – Expand continuous monitoring capabilities to drive risk-based decisions and better inform compliance activities

Continuous monitoring of government networks remains a top priority for the federal IT community. Using tools such as automated asset, configuration, and vulnerability management, we are able to maintain an ongoing awareness of DOJ's IT security posture, which is essential to our ability to perform this important mission. Such awareness is also critical in making informed decisions in the context of increasing threats and reduced resources.

The DOJ Continuous Monitoring program provides near real-time insight into the vulnerability, patch, and configuration compliance of our classified and unclassified endpoints (servers, desktops, and laptops). This critical information is made available to DOJ and component management via a Security Posture Dashboard. We also are deploying additional capabilities to enable components to track and manage their endpoint power management and software license usage, as well as provide software whitelisting. Additional enterprise-class solutions are being deployed to allow for security monitoring of databases and network devices.

The insight the Trusted Internet Connections (TIC) program provides into network traffic to and from the Internet, coupled with the network situational awareness provided by the Justice Security Operation Center (JSOC), provides our program with a holistic, in-depth, near-real time view of the DOJ security posture. Leveraging our existing program, we will continue to work closely with the Office of Management and Budget (OMB), National Security Staff (NSS), Information Security and Identity Management Committee (ISIMC), and the components to develop a continuous monitoring framework to be used across government.

Objective 3.3 – Integrate Identity, Credentials, and Access Management (ICAM) programs

Identity, Credentialing, and Access Management (ICAM) is another top Administration and DOJ cyber security priority. Providing secure and efficient access to DOJ data and systems to whoever requires it, using federally-approved standards and technologies, is essential for mission support and agency transparency. OCIO will implement enterprise ICAM processes and technologies, aligned with the Federal ICAM roadmap segment architecture that will ensure the right information is available to the appropriate stakeholders where and when they need it.

To support this objective, DOJ is deploying an enterprise identity federation capability that will facilitate secure and efficient access to DOJ resources from within and outside the Department. Additionally, DOJ is implementing an enterprise virtual directory service capable of providing attribute-based access control, thereby increasing security and improving accessibility to information resources.

DOJ also will evaluate and deploy other required enterprise ICAM capabilities as necessary, such as provisioning identities to those without Personal Identity Verification (PIV) cards and

leveraging multi-factor authentication capabilities, while ensuring an appropriate blend of security, usability, and cost efficiencies is maintained.

Objective 3.4 – Assure a trusted and resilient information and communications infrastructure

The DOJ cyber security program requires a committed investment in people, processes, and technology to provide Information Assurance (IA) and Computer Network Defense (CND) for our mission critical systems and data. Our ability to achieve strategic goals is contingent on our ability to capture, process, manage, analyze, and share information. To meet mission investigative and information sharing requirements, our agents, attorneys, and analysts depend on connectivity to the Internet, other DOJ components, and multiple levels of government. This connectivity level increases the exposure of our systems to disruption from cyber threats and attacks.

Executive Order 13587 (October 7, 2011) directs structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks. As a result of the order and presidential classified safeguarding activities, DOJ is subject to mandates and objectives to enhance classified information sharing and safeguarding across the executive branch. Our focus on removable media control, reducing anonymity, enhanced access controls on systems and applications, and enterprise auditing across classified and unclassified enclaves will result in a more robust and secure information environment that will better enable mission success.

Another significant risk to government information systems is the insider threat, which was demonstrated by the highly-damaging WikiLeaks incident and Edward Snowden's disclosure of National Security Agency (NSA) global surveillance program documentation. In addition to personnel security system enhancements, DOJ will guard against these threats by investing in technical monitoring and detection tools on all classified networks and systems. These investments will also help guard against advanced persistent threats (APTs), which are a family of sophisticated and organized cyber-attack tactics and techniques to access and steal information from compromised computers. With our law enforcement and national security missions, DOJ and its components are increasingly targeted for APT attacks. The use of new technologies will allow us to identify malicious software through advanced network monitoring, advanced host-based monitoring, and behavioral-based detection capabilities.

Strategic Goal 4: Deliver innovative solutions to meet customer needs

DOJ will continue to deliver innovative solutions to meet the needs of various customer groups. DOJ's wide variety of IT customers include criminal investigators, prison guards, U.S. marshals, U.S. attorneys, counter-terrorism analysts, forensics experts, controlled substance regulators, program managers, and administrative staff, to name a few. As compact mobile computing devices and wireless broadband revolutionize the ways we access and use information, much of DOJ's innovation agenda in the coming years will be driven by the adoption of mobility solutions and cloud services.

Objective 4.1 – Support component deployment of mission systems to meet specific customer needs

While many customer needs can be fulfilled with enterprise solutions and commodity IT services, there will always be a need for custom solutions built to meet a specific need for a specific set of users. The reasons a specific solution is needed can vary – restricted access to the information, a focused user base with constantly changing needs, or a specific mission system with complex requirements and data.

The need for these types of solutions is often driven by individual DOJ components. When a commodity service or shared solution is not a feasible option, DOJ will support components in building specific mission systems to meet their own customers' needs. A recent example of this is the FBI's SENTINEL case management system. Because of FBI's unique technical and business requirements for case management, the solution is customized for the FBI and is not a candidate for serving as a shared service platform.

As the Department moves forward with a shared service and service broker approach, we expect certain mission systems to remain component-specific (i.e., not provided as a shared solution). Over the long term, as IT environments continue to evolve into computing ecosystems that put data and application tools in the hands of users, some mission systems will be created directly by customers, using the suite of tools and data made available by IT at either the component or the Department level.

Objective 4.2 – Provide mobility services to enhance employees' mission effectiveness and improve service delivery and information access to the public

DOJ is committed to providing mobile services to enhance our customers' experience, empower employees, and inform the public. With sales of mobile devices outpacing desktop and laptop computers, the computing marketplace will continue to evolve rapidly towards the use of mobile services. Today, private industry and the public use mobile services on a daily basis, and the federal government is making significant progress bringing these capabilities into the IT environment in an effective and secure way. Public consumption of DOJ data for use on mobile devices is growing, and our employees want to use the same mobile productivity tools at work that they have at home. The OMB Digital Strategy, a federal initiative in which DOJ is heavily involved, addresses this dynamic and sets a strategic path to capitalize on the expanded capabilities mobility services provide.

In line with the OMB Digital Strategy, DOJ has developed a strategy to expand enterprise mobile services in four areas:

- ***Open data services*** – These services will make standardized, high-value data sets available to employees and the public, so users can manipulate the data and develop mobile applications use the data in innovative ways. (See also Objective 4.3.)
- ***Mobile application services*** – These services will provide user-friendly application development tools for employees and various partners across the community. DOJ

approved applications (apps) will be certified for security, privacy, and legal soundness before being published to a store for download by employees and the public.

- ***Mobile device services*** – These services will provide DOJ employees with the mobile devices they need to do their jobs, while managing these devices from acquisition to replacement.
- ***Mobile platform services*** – These services will provide the infrastructure and management services to implement and operate a mobile application environment containing a DOJ apps store that provide DOJ-certified apps for download, ensure application, data, and device security, and promote strategic sourcing for federal or enterprise mobile contracts.

To manage the mobile assets of open data, mobile applications, and mobile devices, DOJ will create a management life cycle that integrates policy, governance, security, contracting, and communication and collaboration.

Objective 4.3 – Spur innovation and improve services by engaging the public and making DOJ datasets available

In support of the Federal Open Data Policy, and to better manage the Department's data set assets, DOJ will build and expand data set management services for internal use of data, and for sharing with the public as appropriate.

Along with other agencies across the federal government, DOJ participates in the Open Government Initiative and has made data sets available online for public use. DOJ will continue to be responsive to public requests for data that serves the public interest and improves awareness of the Department's mission operations.

When we do so, DOJ is committed to providing data that complies with federal standards for openness and easy public use. To promote openness, DOJ will implement a development environment that is consistent with GSA's Project Open Data initiative. The environment will include support for developing open data sets, as well as cataloguing services for hosting, marketing, and making available open data sets to the public. To manage the open data sets, DOJ will develop a life cycle that spans the identification of potential high-value data sets through creation, use, and final disposition. Integrated into the life cycle will be various controls to ensure protections for data security, access security, records management, privacy, legal stature, civil rights protection, and eDiscovery.

DOJ will also engage proactively with the public to identify data sets that are desirable for public access. To do so, DOJ will partner with mission owners to develop and manage public interaction tools that provide the Department with greater awareness of public interest and enable the public's greater involvement in providing input into the Department's public policy making process.

To measure the effectiveness of this public engagement, the Department will capture performance metrics and analytics that measure usage and satisfaction of various customer groups. Currently, the Department analyzes and publishes key performance metrics on

enterprise IT investments, infrastructure, and transformation initiatives through the Federal IT Dashboard, DOJ Dashboard, and Exhibit 53 and 300 submissions. To expand this level of transparency, the Office of the CIO will establish a program performance and reporting team whose purpose is to provide oversight, evaluation, and tracking of OCIO performance and establish quantitative metrics to better measure expected business value, customer satisfaction, and return on investment.

These performance metrics will be shared with component IT program management, business and mission sponsors, and departmental leadership to enable better decision making for investment funding and continuance. The Department CIO also plans to create a communications and coordination team that will establish OCIO communication protocols and improve engagement with DOJ customers, including components, external agencies, and key stakeholders. The communications team will develop communication strategies to optimize information sharing and coordinate with the program performance and reporting team to analyze feedback from customers on OCIO performance and satisfaction levels.

Use of Social Media to Engage Public Participation. In addition to making datasets available to spur innovation, the Department will continue to use social media platforms to enhance our interaction with the public and advance mission priorities. These innovative technology platforms are extensively used by the general public and enable the Department both to push (publish) as well as to pull (receive) information from the public to assist with investigations and other mission activities.

An example of social media's value to our mission is the FBI's response to the Boston Marathon bombing in April 2013. Following the bombing, the FBI published pictures of the prime suspects to both their website and Twitter account and asked the public to submit tips, including digital pictures or videos of the bombing, via social media. The massive response via social media provided numerous leads that assisted the investigation.

Strategic Goal 5: Expand information sharing

Information sharing among the Justice community has been a priority for the Department since before the September 11, 2001, terrorist attacks on the World Trade Center and the Pentagon. Further efforts to improve counter-terrorism and homeland security information sharing in the wake of 9/11 have resulted in the apprehension of terrorist suspects and prevented terrorist attacks from occurring within the United States. Law enforcement information sharing remains the primary focus of DOJ's information sharing program, and our progress has steadily improved as new technologies, capabilities, and standards are made available to DOJ users and the law enforcement community nationwide. While we have made great strides in information sharing, there is more to be done.

Objective 5.1 – Drive collaboration internally and with the broader law enforcement community

In recent years, DOJ's internal collaboration on information sharing has focused on the most important data assets for law enforcement and counter-terrorism. We have addressed many of

the most pressing information sharing needs for the Department, through the National Data Exchange Program (N-DEx) and other initiatives. Building on these achievements, DOJ will continue to identify new information to be shared and to develop innovative methods for sharing.

In addition to our internal efforts, DOJ will continue to improve how we share timely and relevant information with law enforcement and intelligence community partners. The FBI's Criminal Justice Information Services (CJIS) branch is at the forefront of DOJ's sharing with the nationwide law enforcement community, and additional capabilities are provided by the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), U. S. Drug Enforcement Administration (DEA), and other components. Numerous DOJ systems support the analysis, aggregation, and dissemination of criminal history, biometric identification, firearms eligibility and ballistics, forensic and lab analysis, statistical, and reference information to assist DOJ, its federal law enforcement partners, and state, local, and tribal (SLT) law enforcement agencies. We will continue to refine how we provide these information services to ourselves and our partners to ensure the right information is available to the right people at the right time. As we move forward, an increasing focus on preventing crime, in addition to responding to it, will require a more proactive approach to information sharing, while ensuring the privacy and civil rights of U.S. citizens continue to be protected.

Objective 5.2 – Work with the community to develop and use information sharing standards

Successful information sharing across the extended Justice community requires a deep understanding of user requirements; governance structures to oversee information sharing initiatives; clear policies, procedures, and processes; and a flexible technology environment to facilitate information sharing. In collaboration with the broader Justice community (through FBI's CJIS division, the Bureau of Justice Assistance (BJA), and other DOJ organizational units), the Department has contributed many information sharing standards now in use. One example is the National Information Exchange Model (NIEM), which is the descendent of the highly successful Global Justice XML Data Model (GJXDM). DOJ will continue to work with our partners who maintain and use NIEM and other standards, such as DOJ's Law Enforcement Exchange Specification (LEXS), to evolve these standards and amplify the benefits of standards-based information sharing.

In addition, DOJ's Office of Justice Programs (OJP) sponsors DOJ's Information Exchange Package Documentation (IEPD) Clearinghouse, a repository of reusable information exchanges created by the information sharing community. DOJ also works with the Program Manager for the Information Sharing Environment (PM-ISE) to expand information sharing across the justice and intelligence communities.

Objective 5.3 – Negotiate sharing agreements and enable shared services with public safety and law enforcement partners

DOJ is committed to sharing all pertinent law enforcement information with our federal, state, local, and tribal criminal justice partners. To that end, the Department has re-established the

Law Enforcement Information Sharing Coordination Council (LCC) as the governing body for the Department's information sharing efforts. The council is responsible for ensuring that the Department and its components are able to accomplish our information sharing policy objectives, including the establishment and administration of sharing agreements with law enforcement partners.

Component organizations within DOJ, such as FBI's Criminal Justice Information Services division, ATF, and DEA, already provide essential information services and systems that are used to prevent and solve crimes. These systems include the Integrated Automated Fingerprint Identification System (IAFIS), National Crime Information Center (NCIC), Internet-based firearm trace request submission system (eTRACE), Combined DNA Index System (CODIS), and Law Enforcement Online (LEO). These systems are used to collect and disseminate information for criminal investigations, background checks, identification services, criminal statistics, and other related areas for law enforcement. These and other systems serve the community well and are examples of the federal government's commitment to providing information sharing services to the broader state, local, and tribal user base.

To strengthen the flow of information among the larger law enforcement community, an important challenge is expanding the horizontal sharing of information between state, local, and tribal agencies, especially when there is a federal interest in improving collaboration. Opportunities to improve these information sharing services include: 1) further standardizing processes and data across the user base; 2) co-locating services out of regional service centers; and 3) continuing to deploy new services that provide user friendly, access-controlled tools for law enforcement and public safety users.

Objective 5.4 – Strengthen information safeguarding to protect privacy and civil rights

Privacy, civil rights, and civil liberties protections are integral to maintaining the public trust, and this trust is a cornerstone of our information sharing and safeguarding efforts. DOJ's Office of Privacy and Civil Liberties reviews the information handling practices of the Department to ensure these practices consistently and effectively protect personal information. Our IT security programs in DOJ, both at the Department and component level, provide the technical and policy implementation mechanisms to protect DOJ's controlled unclassified information (CUI) and ensure the privacy and protection of citizen's personally identifiable information (PII). These controls are verified routinely through data calls and by conducting private impact assessments of IT systems that process PII. Awareness of the importance of information safeguarding also is strengthened through mandatory workforce training.

DOJ and our component bureaus use a risk-based approach to identify and deploy appropriate security and safeguarding measures. The specific implementations of these measures can vary, based on the sensitivity and criticality of the information handled during counter-terrorism, law enforcement, litigation, incarceration, and other operations.

The federal government is deploying more comprehensive and adaptable security controls, such as common identity and access management solutions. These controls along with other enterprise-wide approaches will lead to a more stable trust model between government

agencies and our partners, which will help further reduce barriers to information sharing and enable more timely and monitored sharing in the future. To accomplish this, information protections will need to be continuously reinforced and assessed, including monitoring of access and use controls, analysis of audit and usage information, and regular and systematic compliance reviews. In the past, protecting information and sharing information were frequently at odds, with sharing often considered counter to maintaining information security. As we move forward, the trust relationships based on established and monitored levels of security between partners will enable more effective information sharing, rather than hinder it.

VI. Alignment of DOJ IT strategic goals to the DOJ Strategic Plan

The Department of Justice Strategic Plan for Fiscal Years 2014–2018 lists three strategic goals. The Department's five IT strategic goals that are detailed in this document align with these goals and are included in the DOJ Strategic Plan's "Managing the Mission" section. Because information technology is an enabling function—and not a mission function—IT goals may be construed as supporting all departmental goals indirectly since the ultimate purpose of IT is to enable agencies and their personnel to carry out their respective missions effectively and securely. That said, the following table maps the Department's IT goals to the departmental strategic goals to which they are most aligned.

Table 4 – IT Strategic Goal Alignment with DOJ Goals

DOJ Strategic Goals	DOJ IT Strategic Goal Mapping
GOAL 1: Prevent terrorism and promote the nation's security consistent with the rule of law	IT Goal 3 - Enhance IT security IT Goal 4 - Deliver innovative solutions IT Goal 5 - Expand information sharing
GOAL 2: Prevent crime, protect the rights of the American people, and enforce federal law	IT Goal 3 - Enhance IT security IT Goal 4 - Deliver innovative solutions IT Goal 5 - Expand information sharing
GOAL 3: Ensure and support the fair, impartial, efficient, and transparent administration of justice at the federal, state, local, tribal, and international levels	IT Goal 1 - Institute IT portfolio management IT Goal 2 - Streamline IT operations IT Goal 3 - Enhance IT security IT Goal 4 - Deliver innovative solutions IT Goal 5 - Expand information sharing

VII. Compendium of component goals and priorities

The Department consists of over fifty component agencies, offices, and programs that execute the Department's law enforcement mission. From smaller offices such as the Office of Tribal Justice and Office of Privacy and Civil Liberties, to large components such as the Federal Bureau of Investigation and the Criminal Division, the Department's components rely on the effective use of information technology to accomplish their unique missions.

This section summarizes the IT goals, priorities, and major investments and initiatives of selected components and offices from across the Department. While Departmental investments in IT infrastructure such as data center consolidation benefit components Department-wide, components' missions often require investments that provide unique capabilities to their workforce. As the Department institutionalizes its IT portfolio management model (strategic goal #1), components will have greater visibility into each other's requirements and investments, resulting in increased shared solutions and a smaller number of stand-alone investments.

Please note: The following summaries are not meant to be all-inclusive but are representative of the Department's use of IT to support its mission.

Major Components *(as defined by personnel size and overall budget)*

A. Bureau of Alcohol, Tobacco, Firearms and Explosives

Component Mission: ATF protects our communities from violent criminals, criminal organizations, the illegal use and trafficking of firearms, the illegal use and storage of explosives, acts of arson and bombings, acts of terrorism, and the illegal diversion of alcohol and tobacco products. ATF partners with communities, industries, law enforcement, and public safety agencies to safeguard the public we serve through information sharing, training, research, and use of technology.

Strategic IT goals and priorities for FY 2014-2016

1. Achieve seamlessness of information throughout ATF and its partners.
2. Expand the capacity of ATF laboratories and the Financial Investigative Services Division (FISD).
3. Deliver authoritative information, forensic services, and technology related to firearms, explosives, and arson.
4. Shape customer demand to better support ATF's enterprise current and future needs.
5. Attract, develop, and retain an expert workforce to execute the OST mission.

Strategic IT investments and initiatives

- Support a comprehensive and coordinated firearms tracing program by maximizing electronic access to firearms transaction and tracing data, within constraints of legal permissibility. Deliver eTrace 5.0 and "Access 2014."
- Improve internal communication and collaboration, provide content management and process automation, and comply with records management requirements through implementation of SharePoint.
- Deploy Laboratory Information Management System (LIMS).
- Maximize cost predictability and economy and achieve critical technology refreshment through the realization of fuller managed services under the Enterprise Standard Architecture (ESA) IV contract.
- Begin acquisition of a Next Generation Case Management System that will improve the quality and completeness of case management information; enable end user mobility; automate streamlined business processes; and support adaptation for inevitable changes in business needs and technology.

B. Bureau of Prisons

Component Mission: The Federal Bureau of Prisons protects society by confining offenders in the controlled environments of prisons and community-based facilities that are safe, humane, cost-efficient, and appropriately secure, and that provide work and other self-improvement opportunities to assist offenders in becoming law-abiding citizens.

Strategic IT goals and priorities for FY 2014-2016

1. Transition legacy mainframe system user interface and workflows to take advantage of modern web technologies to improve system integration/data sharing.
2. Develop and implement enterprise mobile and cloud applications to support operational activities in the institutions.
3. Digitize workflows and reduce paper printing to eliminate waste and enhance staff and inmate productivity.
4. Deploy HSPD-12 PIV cards to BOP staff and contractors enterprise-wide.

Strategic IT investments and initiatives

- Issue PIV cards and deploy logical access control systems (LACS) to comply with HSPD-12 directive.
- Deploy the Inmate Consolidated Network (i-Connect) in support of mandatory electronic GED (general educational development) testing.
- Deploy Electronic Inmate Central File (e-ICF) in support of developing an electronic workflow for inmate document processing and reduce the use of paper files.

- Deploy Web SENTRY Phase 2, including user interface redesign and framework/architecture strategy.
- Migrate enterprise solutions to managed service/Cloud, including BOP.gov and MyFX/IDEA.
- Replace the BOP's Joint Automated Booking System (JABS) submissions server with the Rapid Biometric Identification Detection (RaBID) application. The application allows BOP staff to submit and retrieve biometric information directly from FBI's Integrated Automated Fingerprint Identification System (IAFIS) via DOJ's Joint Automated Booking System (JABS) services framework.

C. Drug Enforcement Administration

Component Mission: The mission of the Drug Enforcement Administration (DEA) is to enforce the controlled substances laws and regulations of the United States and bring to the criminal and civil justice system of the United States, or any other competent jurisdiction, those organizations and principal members of organizations, involved in the growing, manufacture, or distribution of controlled substances appearing in or destined for illicit traffic in the United States; and to recommend and support non-enforcement programs aimed at reducing the availability of illicit controlled substances on the domestic and international markets.

Strategic IT goals and priorities for FY 2014-2016

1. Strive to reduce the overall cost of ownership through implementation of innovative processes and technologies.
2. Create a user experience that is high quality, consistent and robust regardless of the users location or access method.
3. Transform hardware and software platforms to support emerging technologies.
4. Develop and implement processes and technologies to improve cyber security and critical infrastructure protection.

Strategic IT investments and initiatives

- Implement Next Generation Network (NGN) technology to improve security and performance of the Firebird SBU network, also providing a tech refresh of the network and reducing future implementation and management costs.
- Provide easy, secure network access to employees in every DEA office by developing and implementing a service-based model that allows personnel to access DEA resources via multiple mobile-based solutions.
- Transition the legacy M204 corporate system to a lower cost, web-based solution.

- Implement efficiencies and reduce Operations & Maintenance costs by combining individual Oracle database systems into a clustered environment. Move to MS SQL to reduce licensing costs and simplify integration with other MS products.
- Consolidate and streamline printer management to gain efficiencies and reduce costs. Transition to a centralized printing model using existing network printers and reducing use of individual desktop printers.
- Reduce Depot costs by using blanket purchase agreements that enable just-in-time equipment purchases.
- Reduce energy consumption by implementing and monitoring power-saving features on Firebird desktop systems, including all peripheral equipment.
- Reduce the number of service contracts to minimize management overhead and improve project lifecycle efficiencies.
- Ensure DEA IT purchasing efficiencies by centralizing and managing all IT purchases through the PortfolioStat program.

D. Executive Office for the U.S. Attorneys

Component Mission: Charged with ensuring "that the laws be faithfully executed," the 93 United States Attorneys work to enforce federal laws throughout the country. The President appoints a United States Attorney to each of the 94 federal districts (Guam and the Northern Mariana Islands are separate districts but share a United States Attorney). The United States Attorney is the chief federal law enforcement officer in their district and is also involved in civil litigation where the United States is a party.

Strategic IT goals and priorities for FY 2014-2016

1. Fortify and extend the IT infrastructure.
2. Safeguard information technology assets.
3. Enhance information systems' capabilities.
4. Improve the effectiveness and accountability of the IT staff.
5. Maintain core business responsibilities.
6. Implement enterprise-wide cost savings initiatives.

Strategic IT investments and initiatives

- Maintain core services to keep operations running effectively, including USAMail, EVOIP Remote Access, and mission activities such as debt recovery.
- Implement a print management solution (Pharos) to provide reports to baseline and then improve enterprise print management processes.
- Continue to develop and implement a comprehensive case management and time tracking system, Caseview, that provides real-time access to data, reporting, and

analytic tools for use by EOUSA and the USAOs to better manage cases and resources, to improve outcomes, and to obtain greater value from available resources.

- Increase video teleconferencing (VTC) bridging capacity and federate with other DOJ components.

E. Federal Bureau of Investigation

Component Mission: The mission of the FBI is to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners; and to perform these responsibilities in a manner that is responsive to the needs of the public and is faithful to the Constitution of the United States.

Strategic IT goals and priorities for FY 2014-2016

1. Sentinel case management system.
2. Establish enterprise IT cost transparency.
3. Network modernization.
4. Hardware tech refresh.
5. Consolidate data centers.
6. Implement end user environment.

Strategic IT investments and initiatives

- Network modernization: Enhance data transport services throughout the FBI, enabling cost-effective access to critical information systems. This initiative will increase reliability of network and speed of transport to end users.
- Hardware tech refresh: Enable the FBI to maintain current technologies and replace end of life cycle equipment. Replace the current practice of end of year funding for technology refresh as budgets shrink.
- Sentinel case management: Provide world class case management to FBI investigations; increase IT efficiencies and reduce lag time of serialized documents entering case files.

F. Justice Management Division (JMD)

Component Mission: The mission of JMD is to provide advice to senior management officials relating to basic Department policy for budget and financial management, personnel management and training, procurement, equal employment opportunity, information processing, telecommunications, security, and all matters pertaining to organization, management, and administration.

JMD is comprised of four distinct offices: Office of the Controller, Human Resources and Administration, Information Resources Management (Office of the CIO), and Office of Policy, Management, and Planning. Each office has a unique focus area with its own strategic goals,

priorities, investments, and initiatives, all of which contribute to the fulfillment of JMD's mission imperatives. JMD's overarching goals to support this mission are as follows:

Strategic IT goals and priorities for FY 2014-2016

1. Reduce costs and improve service delivery to customers by transitioning to shared services and deploying enterprise solutions Department-wide.
2. Provide improved use of data and reporting to customers and decision makers.
3. Increase workforce productivity by leveraging process automation, enterprise solutions, and accountability metrics.

These goals frame and inform the four JMD offices' IT goals and priorities, listed as follows:

Office of the Controller

Strategic IT goals and priorities for FY 2014-2016

1. Reduce O&M costs for the Unified Financial Management System (UFMS) and leverage economies of scale for UFMS and the Financial Management Information System (FMIS) legacy system that UFMS is replacing.
2. Reduce costs of products and services, including those in the Working Capital Fund, by streamlining and upgrading administrative IT solutions; pass savings to component agencies.
3. Improve financial analysis by upgrading data analysis tools, processes, and capabilities.

Strategic IT investments and initiatives

- Implement UFMS enterprise solution at additional components.
- Upgrade the Consolidated Debt Collection System (CDCS) for case load optimization, Java-driven forms, reporting, executive dashboards, and data mart expansion to improve performance and scalability.
- Expand the eShare web portal and use eDocs to improve information sharing and customer service for asset forfeiture.

Human Resources and Administration

Strategic IT goals and priorities for FY 2014-2016

1. Improve HRA accountability to component customers by using:
    a. USA Staffing system to track cases and create audit trails;
    b. eOPF (Electronic Official Personnel File Automated System) to improve record quality and information sharing; and
    c. SSC (Shared Service Center) to automate personnel action processing, streamline workflow, and track performance metrics.

Strategic IT investments and initiatives

- Expand use of USA Staffing system.
- Deploy eOPF to JMD offices, boards, and divisions.

Information Resources Management / Office of the CIO

Strategic IT goals and priorities for FY 2014-2016

1. Customer-Driven View of IT: Partner with component CIOs to adopt a customer-centric view of IT that integrates mission and business partners.
2. Efficient, Effective, Secure, and Sustainable Information Technology: Provide continuous improvement to and secure IT infrastructure and application services to support customer mission requirements.
3. Value-Added IT Governance: Improve overall IT systems management, planning, and oversight through more effective governance.
4. IT Portfolio Optimization and Rationalization: Drive IT efficiencies using a portfolio-based approach.
5. Organizational Culture and Workforce Excellence: Develop a world-class IT workforce focused on an organizational culture of delivering excellence, and one that contributes to and supports employee engagement, innovation, and satisfaction.

Strategic IT investments and initiatives

- Consolidate Departmental and component email systems onto a cloud-based, shared enterprise solution.
- Implement a Mobile Application Environment (MAE) to support components' use of mobile technology for mission requirements and operational efficiency.
- Consolidate Departmental and component data centers into shared, enterprise data centers.
- Transition Departmental IT service delivery to a service broker model.
- Establish a Vendor Management Office to improve strategic sourcing and reduce licensing costs.
- Improve workforce management by recruiting and retaining employees with requisite IT and organizational skills.

Office of Policy, Management, and Planning

Strategic IT goals and priorities for FY 2014-2016

1. Increase productivity and achieve efficiencies by leveraging enterprise systems, including the asset management system and the procurement capabilities of UFMS.
2. Streamline and improve the Department's acquisition process by transitioning to shared systems as part of GSA's Integrated Acquisition Environment (IAE) program; begin planning the transition to IAE's consolidated System for Award Management (SAM).
3. Participate in OMB transparency initiatives.

Strategic IT investments and initiatives

- Upgrade the PRISM grants management system and fully implement dashboard capabilities.
- Phase out ASRS for updating the Federal Procurement Data System (FPDS).
- Implement IQ Archive tool to improve processing of FOIA requests.

G. U.S. Marshals Service

Component Mission: The mission of the USMS is to enforce federal laws and provide support to virtually all elements of the federal justice system by providing for the security of federal court facilities and the safety of judges and other court personnel; apprehending criminals; exercising custody of federal prisoners and providing for their security and transportation to correctional facilities; executing federal court orders; seizing assets gained by illegal means and providing for the custody, management, and disposal of forfeited assets; assuring the safety of endangered government witnesses and their families; and collecting and disbursing funds.

Strategic IT goals and priorities for FY 2014-2016

1. Provide a stable, secure, resilient IT infrastructure.
2. Increase stakeholder engagement and promote customer satisfaction.
3. Enhance innovation and provide clear added value in delivering effective technology capabilities.
4. Organize and transform our workforce to efficiently meet the future needs of the USMS.

Strategic IT investments and initiatives

- Complete the realignment of the IT Division (ITD) and redesign of the customer service model.
- Identify solution(s) to internally fund ITD's budget shortfall without degrading essential services (e.g., JABS, JCON, JCON S/TS, SharePoint, IT infrastructure).
- Transition Office of the Federal Detention Trustee (OFDT) users, IT services and solutions, and contracts into the USMS IT environment.

Litigating Components

H. Antitrust Division

Component Mission: The mission of the Antitrust Division is to promote competition in the U.S. economy through enforcement of, improvements to, and education about antitrust laws and principles.

Strategic IT goals and priorities for FY 2014-2016

1. Increase the efficiency and thoroughness of ATR legal staff's review of evidentiary materials by implementing the Relativity software platform.
2. Redesign the ATR intranet (ATRnet) and implement the Drupal Web Content Management System; upgrade web services infrastructure from Windows to Linux.

3. Increase the capacity and efficiency of the Division's internal processing center to handle productions of native files as well as search warrant materials.
4. Increase the capability to review both audio/video evidence and foreign language documents; pilot software that provides foreign language translation with increased capacity and accuracy of translations.
5. Streamline and automate primary business processes, including transaction review, editing, and approval; implement PIV-based digital signatures, dashboards, electronic forms, and analytical tools accessible on desktop, laptop, and mobile platforms.
6. Strengthen ATR's security program capabilities and management by deploying the LockPath Keylight Governance, Risk, and Compliance (GRC) platform.

Strategic IT investments and initiatives

- Complete migration to the Justice consolidated email system.
- Complete implementation of PIV card use for network login; modify Division applications to accept PIV card for login credentials.
- Upgrade JUTNet connection bandwidth to remote offices to better serve staff in locations outside of Washington, D.C.
- Upgrade desktops and laptops to Windows 7 operating system.
- Upgrade San Francisco and Chicago offices' telephony systems using repurposed components from closed regional offices; upgrade hardware and refresh software.

I. Civil Division

Component Mission: The Civil Division represents the United States in any civil or criminal matter within its scope of responsibility – protecting the United States Treasury, ensuring that the federal government speaks with one voice in its view of the law, preserving the intent of Congress, and advancing the credibility of the government before the courts.

Strategic IT goals and priorities for FY 2014-2016

1. Customer Driven: Work closely with attorneys in developing, testing, and deploying information technology investments that meet their needs.
2. Improve and Streamline: Use cutting edge technology to efficiently meet the litigating mission of the Civil Division.
3. Resource Management: Develop hardware-agnostic and vendor-neutral requirements to drive cost saving procurements that meet green government initiatives.
4. Service Delivery: Provide high quality IT support and assistance to attorneys through multiple channels.
5. Privacy and Security: Ensure the security, confidentiality, availability, and privacy of electronic information.

Strategic IT investments and initiatives

- Implementing IT solutions and custom workflows for the collection, search, and processing of information for FOIA requests; backlog reduced more than 50% in FY 2013.
- Continue implementing server, desktop, and application virtualization, resulting in significant O&M cost reduction, increased customer satisfaction and capabilities, and best in class security compliance for non-classified systems.
- Implementing advanced analytical and data mining tools to assist attorneys in manipulating and managing large, complex, and often unrelated data sets to advance litigation capabilities and outcomes.

J. Civil Rights Division

Component Mission: The Constitution of the United States promises equal justice under the law and freedom for all. The Civil Rights Division enforces the Civil Rights Acts; the Voting Rights Act; the Equal Credit Opportunity Act; the Americans with Disabilities Act; the National Voter Registration Act; the Uniformed and Overseas Citizens Absentee Voting Act; the Voting Accessibility for the Elderly and Handicapped Act; and additional civil rights provisions contained in other laws and regulations. These laws prohibit discrimination in education, employment, credit, housing, public accommodations and facilities, voting, and certain federally funded and conducted programs.

Strategic IT goals and priorities for FY 2014-2016

1. Deliver IT solutions that increase workforce productivity and efficiency.
2. Strengthen IT security to safeguard systems and protect stakeholder and customer data.
3. Streamline IT operations to reduce costs and enhance the customer's experience.

Strategic IT investments and initiatives

- Ensure accessibility of electronic and information technology (EIT) to individuals with disabilities a priority.
- Implementing the Relativity software platform to assist the litigation staff's review of legal materials.
- Implemented the Symantec Enterprise Vault document archiving solution to improve email management and advance the processing of electronic discovery (eDiscovery) capability to assist litigation investigations.
- Consolidate CRT data centers at Patrick Henry Building and Northwest Building in support of the Department's data center consolidation program.
- Leverage Virtual Desktop Infrastructure (VDI) as a platform as a service (PaaS) to secure and protect Department data and to administrator and manage desktop environment as well as hardware costs reduction.
- Upgrading to SharePoint 2013 to enhance the eDiscovery, records management, document management and collaboration functionality; which all support the mission of the Civil Rights Division.

K. Criminal Division

Component Mission: The mission of the Criminal Division is to develop, enforce, and supervise the application of all federal criminal laws, except those specifically assigned to other divisions.

Strategic IT goals and priorities for FY 2014-2016

1. Customer Driven: Work closely with attorneys in developing, testing, and deploying information technology investments that meet their needs.
2. Improve and Streamline: Use cutting edge technology to efficiently meet the mission of the Criminal Division.
3. Resource Management: Sustain efforts to achieve procurements that meet Section 508, green government initiatives compliance, and cost savings initiatives
4. Service Delivery: Provide high quality IT support and assistance to attorneys and support professionals through multiple channels.
5. Privacy and Security: Ensure the security, confidentiality, availability, and privacy of electronic information.

Strategic IT investments and initiatives

- Continue implementing server, desktop, and application virtualization, resulting in significant O&M cost reduction, increased customer satisfaction and capabilities, and best in class security compliance for non-classified systems.
- Implementing advanced analytical and data mining tools to assist attorneys in manipulating and managing large, complex, and often unrelated data sets to advance litigation capabilities and outcomes.

L. Environment and Natural Resources Division

Component Mission: The mission of the Environment and Natural Resources Division is, through litigation in the federal and state courts, to safeguard and enhance the American environment; acquire and manage public lands and natural resources; and protect and manage Indian rights and property.

Strategic IT goals and priorities for FY 2014-2016

1. Deploy a converged computing infrastructure that enables virtualization and reduces stovepipe systems and O&M costs.
2. Improve desktop computing performance and management by migrating user data, profiles, settings, etc. to a central repository from the desktop ("thinning").
3. Expand virtualization.
4. Provide updated technologies to accomplish the mission.
5. Deploy a cost effective printing solution.
6. Reduce environmental impact of IT infrastructure and programs.

Strategic IT investments and initiatives

- Deploy a converged computing infrastructure. To end the proliferation of stovepipe systems required to support the Division's varied computing requirements, ENRD will deploy a scalable unified platform running VMware on Cisco UCS servers over Cisco networks with NetApp storage, combining routing, switching, storage, and servers into a converged infrastructure. This infrastructure, referred to as FlexPod, offers a unified management and support approach to networking, storage, and server virtualization, reducing O&M support costs.
- Expand virtualization by deploying a virtual desktop infrastructure (VDI) pilot to determine its effects on cost and the overall end-user experience.
- "Thinning" the Current Desktop. ENRD will relocate user data, profiles, settings, and customization files from individual desktop computers to centralized storage ("thinning"), thereby co-locating all user-specific data and making it easier to update and manage the inventory of deployed PCs; upgrade desktop hard drives to improve performance, extending the desktop lifespan to 10 years and saving the Division money as well as reducing environmental waste.
- Reduce environmental impact by focusing on energy efficiency and reducing IT infrastructure waste (data centers, desktops, printers) and by deploying collaboration software, online conferencing, and remote access, all of which reduces vehicle emissions by eliminating the need to travel.

M. Tax Division

Component Mission: The Tax Division's mission is to enforce the nation's tax laws fully, fairly, and consistently, through both criminal and civil litigation, in order to promote voluntary compliance with the tax laws, maintain public confidence in the integrity of the tax system, and promote the sound development of the law.

Strategic IT goals and priorities for FY 2014-2016

1. Improve security of federal tax information (FTI) and other personally identifiable information (PII).
2. Improve the "mobility" of Tax Division attorneys by deploying IT solutions the enable and enhance teleworking from a variety of remote locations.
3. Provide a secure desktop with platform-independent access; enable secure access through BYOD, iPads, laptops, thin clients, PCs, smartphones, and public computers.
4. Secure remote access to Automated Litigation Support (ALS) review platforms to enable experts and other agencies to review data without the need to produce DVDs and external hard drives.

Strategic IT investments and initiatives

- Implementing virtual desktop infrastructure (VDI) in order to provide a secure desktop that is platform-independent and eventually enable users to work remotely from any

device and location. This will improve the overall security of FTI and PII, while also improving access for our attorneys when traveling.

Law Enforcement Components

N. Executive Office for Immigration Review

Component Mission: The primary mission of the Executive Office for Immigration Review (EOIR) is to adjudicate immigration cases by fairly, expeditiously, and uniformly interpreting and administering the Nation's immigration laws. Under delegated authority from the Attorney General, EOIR conducts immigration court proceedings, appellate reviews, and administrative hearings.

Strategic IT goals and priorities for FY 2014-2016

1. Maintain reliable, secure, and sustainable EOIR infrastructure services and enterprise application services.
2. Develop and enhance court application services that enable EOIR to achieve its mission.
3. Deliver end user computing services that enable a mobile workforce to maintain its efficiency and effectiveness from anywhere.
4. Leverage evolving technologies to provide innovative unified communications services.

Strategic IT investments and initiatives

- Windows 7 Migration. Support for the current Windows XP desktop operating system ends in April 2014. Upgrading the desktop operating system and hardware where appropriate will ensure the sustainment of a secure and reliable desktop infrastructure.
- Virtual Server/Storage Upgrade. The virtual server environment and storage area network reach the end of support in December 2014. These infrastructure components host numerous production applications and all of EOIR's data; upgrading these critical infrastructure components will improve sustainment and stability.
- Digital Audio Recording (DAR) system upgrade. The DAR system is required by EOIR to digitally record its hearings and is an integral part of adjudicating immigration cases. The DAR system hardware (servers and workstations) as well as the operating system and recording application are all outdated. With other components of the infrastructure being updated, this application must also be updated to be sustainable.

O. Executive Office for U.S. Trustees

Component Mission: The United States Trustees act in the public interest to protect and preserve the integrity of the bankruptcy system of the United States by regulating the conduct of parties; ensuring compliance with applicable laws and procedures; bringing civil actions to address instances of abuse; securing the just, speedy, and economical resolution of bankruptcy cases; and identifying, evaluating, referring, and supporting the prosecution of criminal bankruptcy violations.

Strategic IT goals and priorities for FY 2014-2016

1. To streamline IT operations, deploy solutions that reduce costs and improve efficiencies; migrate to shared IT services where possible.
2. To deliver innovative solutions to meet customer needs, expand the implementation of SharePoint and other collaboration tools that can accommodate changing business needs; support the Consolidation of Function project that is underway within the program; and expand and support a more mobile workforce using mobile technology.
3. To expand information sharing, streamline the use of collaboration tools for information sharing and remove the geographical barriers and improve data exchanges with the U.S. Courts.
4. Continually improve the USTP security posture by expanding continuous monitoring and continuing the integration of identity, credential, and access management (ICAM) into our security program.

Strategic IT investments and initiatives

- Virtualization: The USTP has implemented a redundant Hyper-V cluster to migrate servers off of aging equipment and to avoid procurement of server hardware wherever possible. The virtual servers will be replicated to the USTP COOP site.
- Email migration: The USTP is in the final stages of migrating its email system to the Justice Communication System (JCS), the Department's consolidated email platform.
- Portal development: USTP is consolidating all related USTP data collections under a single web interface (portal), enabling staff to view case data across all data collections at once rather than having to search individual collections.
- SharePoint: The implementation of SharePoint services has enabled increased information sharing and collaboration between field offices.

P. National Security Division

Mission: The mission of the National Security Division (NSD) of the Department of Justice is to carry out the Department's highest priority: to combat terrorism and other threats to national security. The NSD, which consolidates the Department's primary national security elements within a single Division, currently consists of the Office of Intelligence Policy and Review; the Counterterrorism and Counterespionage Sections, formerly part of the Criminal Division; and a new Law and Policy Office. This organizational structure ensures greater coordination and unity of purpose between prosecutors and law enforcement agencies.

Strategic IT goals and priorities for FY 2014-2016

1. Foster relationships with NSD customers.
2. Empower NSD's Information Technology Management (ITM) employees.
3. Provide reliable, secure IT solutions for NSD.
4. Measure and report ITM performance.

Strategic IT investments and initiatives

- Catalog and formalize ITM service level agreements (SLAs). Coordinate efforts with the CS3 strategy (customer interaction lifecycle) to determine current SLAs and "to be" SLAs, conduct a gap analysis and prioritization, draft or revise the needed SLAs.
- Implement a mission awareness development program for ITM. Enhance ITM employees' understanding of NSD's mission and operations to increase customer service effectiveness (e.g., help desk).

Q. INTERPOL Washington (USNCB)

Component Mission: The mission of INTERPOL Washington is to facilitate international law enforcement cooperation as the United States representative to INTERPOL on behalf of the Attorney General.

Strategic IT goals and priorities for FY 2014-2016

1. Extend information sharing services and capabilities through new and enhanced partnerships with domestic and foreign law enforcement agencies.
2. Protect IT infrastructure through enhanced security measures and practices.
3. Enhance IT infrastructure through standardized systems, management processes and automated workflows.
4. Streamline IT operations by adopting standardized policies, procedures and requirements.

Strategic IT investments and initiatives:

- Automation: Increased automation for case management and workflow activities. Overall reduction of manual process and enhancing access to national lookout systems and populating national systems with international law enforcement data for improved border security and reduction in transnational crime.
- Federal and Local Information Sharing: Further expansion of INTERPOL information and capabilities to domestic law enforcement through strategic partnerships (FBI/DHS/Nlets/RISS/State/Local/Tribal Law Enforcement).

R. U.S. Parole Commission

Component Mission: The mission of the USPC is to promote public safety and strive for justice and fairness in the exercise of its authority to release and supervise offenders under its jurisdiction.

Strategic IT goals and priorities for FY 2014-2016

1. Deploy Web-Based Workflow Management System. The USPC is automating its work processes and task assignment utilizing custom SharePoint workflows and lists, allowing for detailed task management, tracking, and data collection. The data collected, along with the management of improved performance metrics, will allow the

USPC to perform detailed trend analysis and reporting while interfacing with partner agencies for more effective offender management.

2. Deploy Web-Based Case Management System. The USPC is developing a SharePoint based case management system to allow for offender profile management and paperless case processing in a low cost, sustainable environment. The system will provide a secure and detailed offender profile, history, and management tools to assist in the improvement of the offender services rendered in a consistent and transparent manner.
3. Remove Thirty-Five Servers from Service. The USPC currently has Forty-Five physical servers in use. Thirty-Five of those servers will be decommissioned, salvaged, or transferred to other components for repurposing.
4. Complete Paperless Transition. The USPC is converting all case and correspondence related work processes to a paperless environment. This will increase efficiency, transparency, training, and trend analysis capabilities within the organization. The overall result will be significantly lower cost operations, and greater document control and security. This process also enhances the ability to share data and information with offender management partners in a secure and auditable manner.
5. Improve Customer Service. The USPC is will improve IT and operational customer service through the use of user friendly interfaces, transparent systems, and the enhanced utilization of thin client devices. This will accommodate force reductions, while enhancing the capability of overall USPC operations.

Strategic IT investments and initiatives

- Deploy a web-based workflow management system.
- Deploy a web-based case management system.
- Decommission thirty-five servers for salvage or transfer to other components for repurposing.
- Transition to a paperless environment.
- Improve customer service through the use of user friendly interfaces, transparent systems, and the enhanced utilization of thin client devices.

Grants Management Components

S. Community Oriented Policing Services

Component Mission: The primary activity of the COPS Office is the awarding of competitive, discretionary grants directly to law enforcement agencies across the United States and its territories.

Strategic IT goals and priorities for FY 2014-2016

1. Complete implementation of all phases of the NexGen COPS Management System.
2. Investigate the feasibility of implementing a shared services solution for grants management systems with OJP, OVW, and COPS.

3. Redesign the COPS internet and intranet websites.
4. Implement the NexGen Enterprise Reporting System.

Strategic IT investments and initiatives

- Complete implementation of the compliance modules for the multiphase NexGen Grants Management System, including Audit Management System, Grants Monitoring Information System, Issue Resolution module, and enhancement to the COPS Agency Portal that will enable enhanced user interaction with grantees.
- Complete implementation of the Enterprise Reporting System. The NexGen Enterprise Reporting System will leverage Microsoft SQL Server Reporting Services and SharePoint 2010 technology to replace the legacy reporting system. The NexGen Enterprise Reporting System will provide standardized reports for end users and enable them to create customized ad hoc queries based on their specific data needs.

T. Community Relations Service

Component Mission: The Community Relations Service (CRS) serves as "America's Peacemaker" for the U.S. Department of Justice. CRS helps local communities address community conflicts and tensions arising from differences of race, color, and national origin.

Strategic IT goals and priorities for FY 2014-2016

1. Complete refresh of IT infrastructure, including laptops, servers, and telecommunications switches.
2. Increase bandwidth in regional and field offices to provide employees with improved computing performance.
3. Deploy SharePoint to headquarters, regional, and field offices to improve information sharing and workforce productivity.
4. Virtualize IT infrastructure elements once bandwidth is upgraded in regional and fields offices to streamline IT operations.
5. Deploy software tools to improve efficiency and effectiveness of field office employees' mediation assignments.

Strategic IT investments and initiatives

- IT infrastructure refresh: CRS is performing a major equipment refresh to include laptops, servers and switches due to obsolescence of legacy infrastructure and the end of vendor support for Windows XP.

U. Office of Justice Programs

Component Mission: OJP's mission is to increase public safety and improve the fair administration of justice across America through innovative leadership and programs.

Strategic IT goals and priorities for FY 2014-2016

1. Improve Human Capital Performance: Attract, retain, and prepare OJP's OCIO workforce for future IT challenges, thus ensuring the continuing effectiveness of OCIO by designing and implementing an effective organizational structure and workforce to carry out our mission; by augmenting OCIO workforce with contractors and detailees; and by continuously developing workforce skills in line with OJP requirements.
2. Partner with OJP Bureaus and Program Offices: Working in partnership with OJP Bureaus and Offices OCIO will improve outreach and service to the grant community. By developing an OCIO organization, Business Technology Consulting Division (BTCD), whose mission is to foster partnering and outreach to OJP bureaus and offices and specifically to the external Grant community; by actively infusing emergent collaborative, mobile and social technology.
3. In-Sourcing: OCIO will become the partner of choice for OJP Bureaus and Offices thus enhancing access to the many external data stores, reducing costs, and increasing security by developing robust infrastructure to accommodate the many external web-sites.
4. Improved Operational Efficiency and Effectiveness: Through partnership with OJP Bureaus and Offices increase OCIO operational effectiveness and efficiency by consolidating IT Investments to a common delivery platform supported by staff with skills in development, operations and maintenance of enterprise as well as emergent collaborative, mobile, and social media technology.

Strategic IT investments and initiatives

- Create a common web content management system (WCMS) platform for publishing content to external sites using a standard set of templates. Bureau and Program Office web sites and web applications will be migrated to the common platform that will drive operational efficiencies and harmonize the end-user experience.
- Establish a Business Technology Consulting Division (BTCD), a new OCIO Division focused on partnering with OJP Bureaus and Program Offices (OJP goal #2). This division will lead OJP in a visionary, collaborative, and stakeholder-focused manner to leverage IT resources to improve business processes and accomplish strategic OJP missions, goals, and program objectives.