DOJ INFORMATION TECHNOLOGY STRATEGIC PLAN 2008–2013

United States Department of Justice

February 28, 2008

U.S. Department of Justice

Washington, D.C. 20530
February 28, 2008

The Department of Justice plays a leading role in the activities of the nation's law enforcement, judicial, and intelligence communities. The Department's investments provide funding and guidance to national and international efforts, but are also part of a broad, integrated set of activities that involve local, state, and tribal governments. Not only does the Department build systems that protect our citizens, but grant funding provided by the Department is used so that local jurisdictions can build systems and programs to keep their communities safe.

In 2002, I released an initial version of the Department of Justice Information Technology Strategic Plan (ITSP), and since then we have periodically updated the plan. This document represents the latest major update, as we continually seek to more closely align our technology investments with the priorities of the Department and to build upon the programs, tools, and standards that we have delivered to date.

The Department currently spends over $2.4 billion annually on information technology investments. This includes hardware, software, and personnel to manage a complex and secure infrastructure. It is imperative that these investments be undertaken in a cost-effective manner — they must be managed to bring the greatest return on investment and they must be secure. Everything we do within the Office of the CIO looks at the value of the investment, and ensures that what we build can be protected and utilized by our partners at all levels of government. As we move forward, our job is to make sure that every dollar invested in information technology provides the greatest return and makes the best possible use of our resources.

This update to our ITSP starts with a review of my role, and by extension the role of the Office of the Chief Information Officer, within the Department. It then goes on to discuss the key drivers which shape our working environment. Next, I outline our strategy — our response to the key drivers within the parameters of our role.

We have made great progress in helping to support the critical mission activities of the Department. OCIO personnel have built new enterprise systems, helped obtain funding for the components, and validated the security of new systems. OCIO has also put the technical infrastructure in place to allow the Department to meet the increasing expectations of our customers and the public. These accomplishments help the men and women of DOJ execute on our diverse mission across the Department. In support of that mission, I believe that this ITSP provides valuable information to the IT professionals across the Department who continue to support their customers and ultimately the goals of the Department's leadership team.

Sincerely,

Vance Hitch
Chief Information Officer

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. ROLES AND RESPONSIBILITIES

The Office of the Chief Information Officer (OCIO) at major cabinet-level departments is a critical transformation entity in the Federal government. The CIO position was established by the Clinger-Cohen Act of 1996 as the key factor in helping to align agency investments in information technology (IT) closely with agency mission goals and objectives. In particular, Congress envisioned an executive level leader who would be a member of the agency's top-level management team and who would be able to help translate business needs into IT investments.

This mandate has been further codified by the Office of Management and Budget (OMB) in OMB Circular A-130, which outlines in detail the processes that an agency must implement to fulfill the requirements of the Clinger-Cohen Act. This includes the establishment of an agency-wide Enterprise Architecture to describe the future state of the agency's IT environment that closely aligns technology with the agency's mission. In addition, CIOs are required to implement an agency-wide, mission-focused Capital Planning and Investment Control (CPIC) process, implement adequate IT security for systems and applications; and implement a Records Management process to ensure the effective capture, preservation, management, and disposal of agency records and official information. Figure 1 depicts the expanse of the competency areas that the CIO position covers.

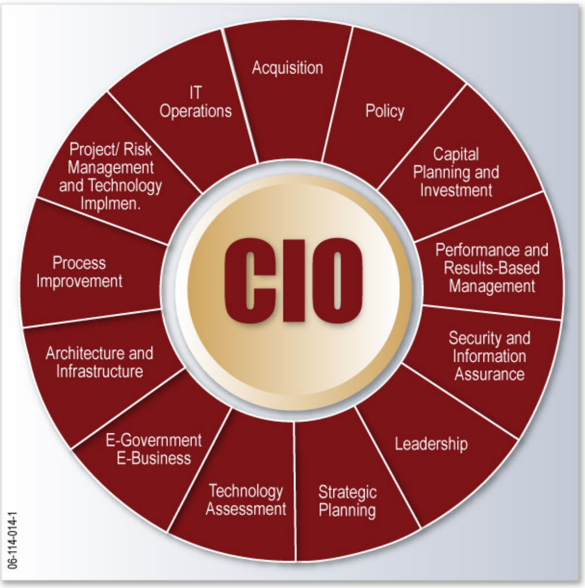

Acquisition
Policy
Capital Planning and Investment
Performance and Results-Based Management
Security and Information Assurance
Leadership
Strategic Planning
Technology Assessment
E-Government E-Business
Architecture and Infrastructure
Process Improvement
Project/ Risk Management and Technology Implmen.
IT Operations
CIO
06-114-014-1

Figure 1: CIO Competency Areas

Within the Department of Justice (DOJ), the importance of the mission and the current focus on effective information sharing and management makes the OCIO even more critical. This has escalated since September 11, 2001 with the mandate from the Congress and various Executive Orders from the President requiring improved and enhanced information sharing between key Federal agencies, between Federal agencies and State and Local law enforcement and judicial agencies, and between the United States and foreign governments. The application of IT is essential to meet these goals and to ensure the security of U.S. citizens worldwide.

As depicted in Figure 2, the DOJ CIO also serves as both a leader and a critical coordination entity between the Justice Department and other key Federal agencies. This includes the Department of

Homeland Security (DHS) and the Director of National Intelligence (DNI), but also State, Local, and Tribal (SLT) governments who have critical on-the-ground responsibilities for law enforcement, judicial processes, incarceration and first response in the event of a terrorist event. Because of the importance of the central role in facilitating information sharing among these key entities, implementing interoperable and integrated technology to support these mission processes is the most critical role of the DOJ CIO. To accomplish this, the DOJ CIO needs to lead the effort to both standardize and consolidate key infrastructure to allow intra-agency and cross-agency sharing of data, information and applications and to leverage the use of existing, and the creation of new, enterprise solutions that will dramatically improve mission results.

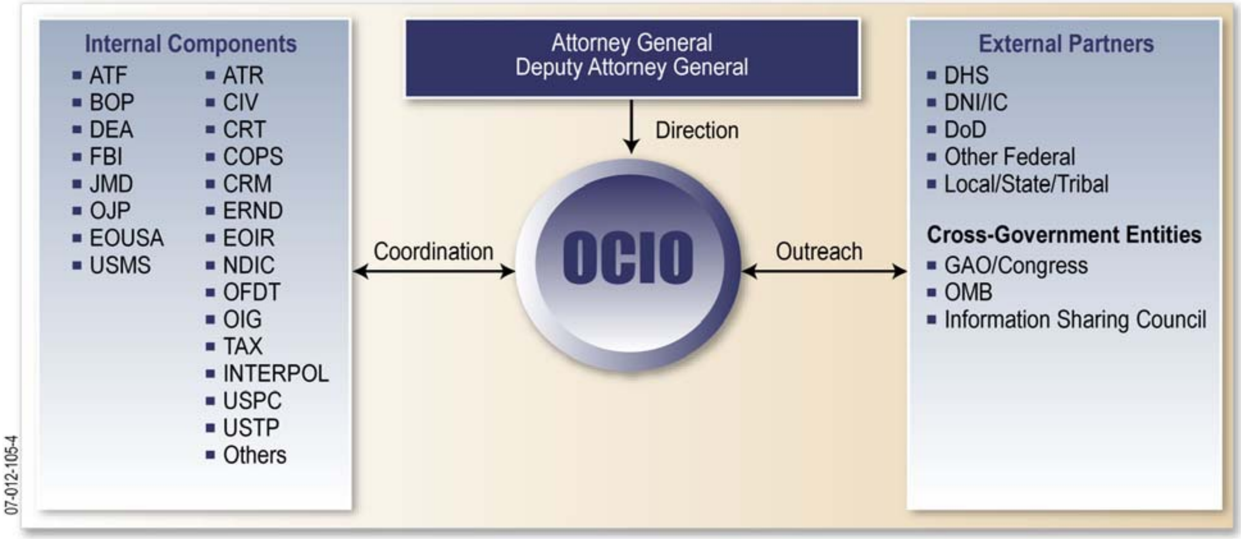


Figure 2: DOJ OCIO Key Relationships

To be successful at these broad and complex responsibilities, the DOJ CIO must also provide leadership and coordinate among the various Components within the Department, each of which has its own critical missions and responsibilities. In many cases the missions are unique to the Component and require specific solutions. The Component CIOs focus on meeting their respective mission IT requirements and providing high quality service to their business customers. However, in many other cases such as IT infrastructure, office automation, case management, administrative support systems, data and information sharing, and records management, there is a need for standardization, consolidation, and sharing of both infrastructure and solutions across the Department. The DOJ CIO plays a critical role in providing leadership and in facilitating the success of these initiatives by driving synergies and providing cross-cutting capabilities. The success of the Department's IT will be through embracing these respective roles in this federated yet collaborative structure. The Department versus Component CIO roles across various dimensions is shown in Table 1 below:

Table 1: Department and Component CIO Roles

	Component CIO	Department CIO
Business Perspective	Vertical-Component Missions	Horizontal-Leverage Across Department
Reporting Relationship	Component Head	Deputy Attorney General / OMB / Congress
Key Customers	Component Mission Owners	Component CIOs / S&L Law Enforcement
Relationship to Business	Service Provider	Service Enabler
Success Driver	Direct-Delivery of Solutions	Indirect-Coordination of Activity to Maximize Corporate Synergy

2. KEY DRIVERS

The DOJ Information Technology Strategic Plan (ITSP) was derived through an analysis of the external and internal environments and identification of the key drivers impacting the strategy for the Department. The key drivers include the Department's evolving mission and how that is impacting IT requirements, the complexity of DOJ business and the IT environment, OMB initiatives, technology trends, and the current financial challenges.

2.1 Mission-Driven Information Technology

The United States continues to face increasing and diffusing threats from domestic and foreign terrorist groups and criminal organizations that are willing and able to invoke either conventional or unconventional (nuclear, cyber, chemical, biological) attacks to exploit our vulnerabilities and endanger our sense of personal safety. In recent years, the destructive capacity of these groups has been fueled by access to more lethal and sophisticated weapons, the use of advanced communications and technology to plan and orchestrate attacks, and the ability to employ even "low tech" means to spread fear or disrupt interconnected systems. In this radically changing threat environment, the potential for harm has increased exponentially, new vulnerabilities are exposed, and traditional law enforcement responses have proved inadequate.

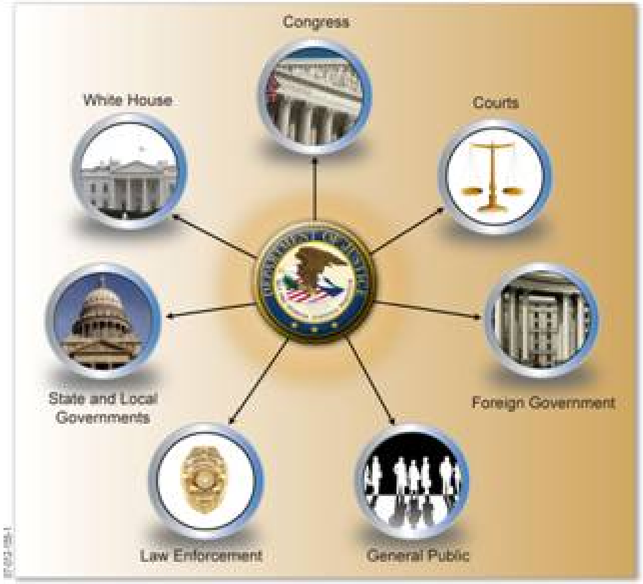


Figure 3: DOJ Customers

To combat these threats effectively, the DOJ must focus its limited resources on its new mission priorities; improve its intelligence and investigative capabilities; and work more closely than ever before with its Federal and SLT partners and cooperating foreign governments as shown in Figure 3. DOJ Customers. Organizationally, the Department must be streamlined, agile, and technologically proficient. To meet these challenges, the DOJ Strategic Plan identifies three overarching strategic goals that the Department will pursue in support of its mission:

- Prevent Terrorism and Promote the Nation's Security
- Prevent Crime, Enforce Federal Laws, and Represent the Rights and Interests of the People
- Ensure the Fair and Efficient Administration of Justice

The Department will fight crimes that are most injurious to the nation and its citizens: terrorism and espionage; violent crime, including firearms offenses; the trafficking of illegal drugs and associated violence; crimes against children; bias-motivated crimes and racial discrimination; corporate crime; cyber-crime; and fraud of all kinds, including tax and identity fraud.

IT is essential to the Department's success in meeting these strategic goals. It is a vital organizational asset that must be strategically developed, deployed, and utilized as an integral part of mission accomplishment. IT provides new and improved capabilities to gather, analyze, and share intelligence information; identify, monitor, apprehend, and prosecute terrorist or criminal suspects; securely share information with our Federal, SLT, and foreign government partners; efficiently manage our criminal and civil cases; provide accessible, speedy, and reliable services to our customers; and efficiently and effectively carry out our internal business practices. In addition, IT provides the communications and computing infrastructure that ensures continuity of operations and rapid response in times of crisis.

2.2 Federated Organizational Structure

The DOJ IT environment consists of a highly diverse and federated organization driven by its mission priorities and complex structure (see Appendix D). The eight major Components and several of the DOJ divisions own and operate their own infrastructure and applications, leveraging a handful of enterprise or common solutions. The current IT portfolio consists of diverse sets of investments that cover the spectrum of core mission and support functions. Within each of these areas, there are numerous IT investments that support a single Component or span across multiple Components. Based on an analysis of FY07 IT spending, there were 207 Support Function IT investments and 94 Mission-level IT investments[1] across the Department. Of those 94 mission-level programs, 5 programs were at the Department[2] level, while 89 were Component-specific investments. In the Support functions area, among the 130 Infrastructure Operations and Management investments, 9 were at the Department level and 121 were Component-specific.

Table 2: DOJ FY07 Programs Spending Categorization

FY07 Program Spend	Number of Investments		
Segment Type	**Cross Component**	**Component Specific**	**Total**
Mission-Segment	5	89	94
IT Infrastructure Operations and Management	9	121	130

Table 2 gives an overview of the number of programs dispersed by Component. The large number of programs within each line of business (LoB) and Components which are often inter-related add to the complexity of managing and operating the Department's IT resources. While DOJ has made significant strides in coordinating efforts among the components, there is still a substantial amount of overlap and unnecessary redundancy across the Department. Addressing this redundancy and further leveraging enterprise solutions and shared IT services is essential to streamlining IT operations and lowering cost while meeting the Department's mission requirements. In addition, IT programs aligned within each segment, but owned by various organizational units, also provide opportunities for improved information sharing across the Department.

[1] Investment is defined as programs found in the FY08 DOJ Exhibit 53 (including all CEI programs).
[2] Programs with JMD designation.

2.3 OMB Direction and Government-wide Initiatives

DOJ is committed to supporting and leveraging Federal Government-wide initiatives such as the OMB E-Government (e-Gov) Initiatives. In the fall of 2001, the OMB and Federal agencies identified 24 e-Gov Initiatives. Operated and supported by agencies, these Initiatives provide high-quality and well-managed solutions for tax filing, Federal rulemaking, and e-training among others. The purpose of e-Gov is to enhance the management and promotion of electronic government services and processes. These e-Gov services and processes establish a broad framework of measures that require using Internet-based IT to enhance citizen access to government information and services. E-Government uses improved Internet-based technology to make it easy for citizens and businesses to interact with the government, save taxpayer dollars, and streamline citizen-to-government communications.

The President's E-Government Strategy has identified several high-payoff, government-wide initiatives to integrate agency operations and information technology investments. The goal of these initiatives is to eliminate redundant systems and significantly improve the government's quality of customer service for citizens and businesses. DOJ supports this initiative as the lead agency for the Case Management Line of Business, including both Litigation Case Management and Investigative Case Management.

E-Gov and other cross-government initiatives are included in the Federal Transition Framework (FTF). The FTF is a single information source for cross-agency IT initiatives using a simple, familiar, and organized structure. It contains government-wide IT policy objectives and cross-agency initiatives including OMB-sponsored initiatives like e-Gov and Segment initiatives and government-wide initiatives, such as Internet Protocol Version 6 (IPV6) and Homeland Security Presidential Directive 12 (HSPD-12). DOJ has incorporated the FTF, IPV6, and HSPD-12 initiatives into its enterprise architecture.

In 2006, OMB initiated the development of the IT Infrastructure (ITI) Line of Business Initiative. Targeting the approximately $24 billion in IT infrastructure, operations, and management spent across the government, the idea is to drive consolidation, standardization, and optimization through establishing benchmarks for cost and service levels and by holding agencies accountable for performance improvement against these benchmarks. The initial focus of the ITI is data centers, end-user (desktop) computing, and help desks. ITI, like all of the e-Gov Initiatives, does not come with dedicated funding. While successful implementation promises cost savings and improved mission support in the long run, there are substantial barriers in the short run, such as cost of migration and cost of scaling up existing IT services. This OMB mandate is one of the drivers for the DOJ OCIO to continue to provide shared infrastructure services across the department, thereby reducing expenditures on commodity IT and applying those savings to direct mission support.

2.4 Technology Trends

Technology advances are increasing performance and capability, and lowering costs, at an amazing and compounding rate. A well known fact from Moore's law describes the rapidly continuing advance in computing power per unit cost, approximately doubling every eighteen months. Retail price/performance for consumer telecommunications, computing, and electronics has been following a similar path. Something that is less well understood but as transformative is the availability today of reliable and secure computing, data storage, data communications, and specific computing (web) services at very low and compelling pay-per-use rates. Further, the use of Internet-based standards for these services means that the cost to integrate is low and increasingly supported in vendor products and services.

Popular culture demands near instant access to complex data sets that are fully integrated and presented to Law Enforcement and Public Safety personnel in a readily accessible and understandable format and translated into immediate action. Maybe not as glamorous, but more real, is the fact that today at the corporate and retail levels, Internet banking and finance, commerce, collaboration, knowledge discovery, and self-service models with high levels of performance and customer satisfaction are accepted parts of day-to-day experience. The DOJ OCIO understands the importance of sharing mission-critical information across DOJ and its partners, as represented by key initiatives such as the Law Enforcement Information Sharing Program (LEISP).

On the other hand, there is an increasing scarcity of the most highly skilled technologists who possess the business transformation, architecture, security and privacy, management skills, and experience to leverage the technology trends cited above and who have the ability to understand and work with our customer base to meet their expectations for technology support in the mission context. These individuals are the crucial link between the possibilities opened up on the supply side and the ability to deliver appropriate solutions on the demand side.

DOJ is committed to working strategically to ensure that our IT spending fully leverages these technology trends and does so in a way that allows us to focus on our mission support role as opposed to duplicating technology services and products that have become commoditized.

2.5 Upholding the Public Trust

Gaining and maintaining public trust is critical for DOJ to operate effectively and carry out its mission. This includes guiding principles such as responsible financial stewardship, appropriate use of authority, and securing the privacy of sensitive information. This is particularly important given DOJ's central role in Federal law enforcement and litigation. In response to direction from the Assistant Attorney General for Administration, DOJ ensured that by June 1, 2007, at least 90 percent of major systems that had been newly built or significantly upgraded since 2002 were covered by completed Privacy Impact Assessments (PIA) including 29 approved (18 conditionally) and 14 others being reviewed or prepared. The PIA template is posted on the DOJ intranet for component use. There is also an effort to assess and recommend needed extensions to PIAs with the DOJ Chief Privacy Officer in accordance with existing statutory and policy guidance

As with any government agency, DOJ has an inherent responsibility to be a good steward of public funds, invest its budget wisely, and be above reproach in its disposition of resources. A key aspect of good financial management is ensuring that the Department is able to provide the public with clean financial audits. Another aspect of fiscal responsibility for the OCIO is to deliver quality products and services in a timely and efficient manner. Investments in IT programs need to be based on a sound business case demonstrating the value of the investments to the mission with appropriate analytical rigor. IT programs must also be executed with discipline and in accordance with established IT governance policies and procedures. IT programs must also fit effectively within the overall DOJ framework as outlined in the Enterprise Architecture to promote consolidation, standardization, and alignment with strategy.

DOJ also has a responsibility to uphold the public trust and the information we collect, and the OCIO recognizes the dual concerns of security and privacy. Security consists of reliability, availability, and integrity. Realizing these attributes requires both technology support and operational services and controls. The goals of our security strategy are to serve as a central focal point, promote awareness, implement policies and procedures, assess risk and determine needs, and monitor and evaluate the security and privacy of DOJ IT systems. In addition, the design and development of DOJ systems needs to always balance the priorities of providing quality timely information while maintaining security and privacy of sensitive data. Citizens have a reasonable expectation of privacy and protection of their personal information and civil rights. DOJ must meet that responsibility and ensure that no person on whom DOJ gathers and stores information is ever, in the words of DOJ's former Chief Privacy and Civil Liberties Officer, "harmed by incorrect information or information used incorrectly."

DOJ must ensure that appropriate processes and policies exist to protect personally identifiable information (PII). DOJ must adhere to all laws, policies, and procedures designed to ensure compliance with privacy and security issues. These include the risk management concepts found in OMB Circular A-130, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-14, "Generally Accepted Principles of Practices for Securing Information Technology Systems" and General Accounting Office (GAO) Report GAO/AIMD-98-68, "Information Security Management — Learning from Leading Organizations."

2.6 Financial Challenges

The Department is facing significant challenges in funding the technology needs for its mission-specific requirements while at the same time providing IT infrastructure and overall support services. The complexity of the mission, challenging business environment, and increasing need for collaboration are all factors driving the need for increased IT investment. In addition, recent investments in new systems development are driving increased Operations and Maintenance (O&M) costs as systems become operational. To meet these financial challenges, DOJ needs to look beyond its current model and explore new alternatives to maximize limited IT resources.

IT infrastructure is an area of significant spending in DOJ's budget and includes technology such as networks, data center, end-user computing, and IT operations. As shown in Figure 4: FY07 DOJ IT Budget Allocation ($2.486 Billion), the percentage of the FY2007 DOJ IT budget used for technical infrastructure was 44 percent. This is a large percentage devoted to IT infrastructure relative to organizational benchmarks. For enterprises with relatively low technology maturity, the percentage of their IT budget in technical infrastructure is typically 35 percent.[3] While government-specific requirements such as duplication of infrastructure across security enclaves do raise costs, there appears to be a meaningful opportunity to reduce the percentage of investment from IT infrastructure operations and management and shift toward direct mission support spend. This would allow for a shift of resources toward direct mission support.

[3] Source – MIT Sloan Center for Information Systems Research (2005), surveyed 103 companies calibrated via detailed case studies including Wal-Mart, Dell, Merrill Lynch, Delta Airlines, Pfizer, IBM, Microsoft.

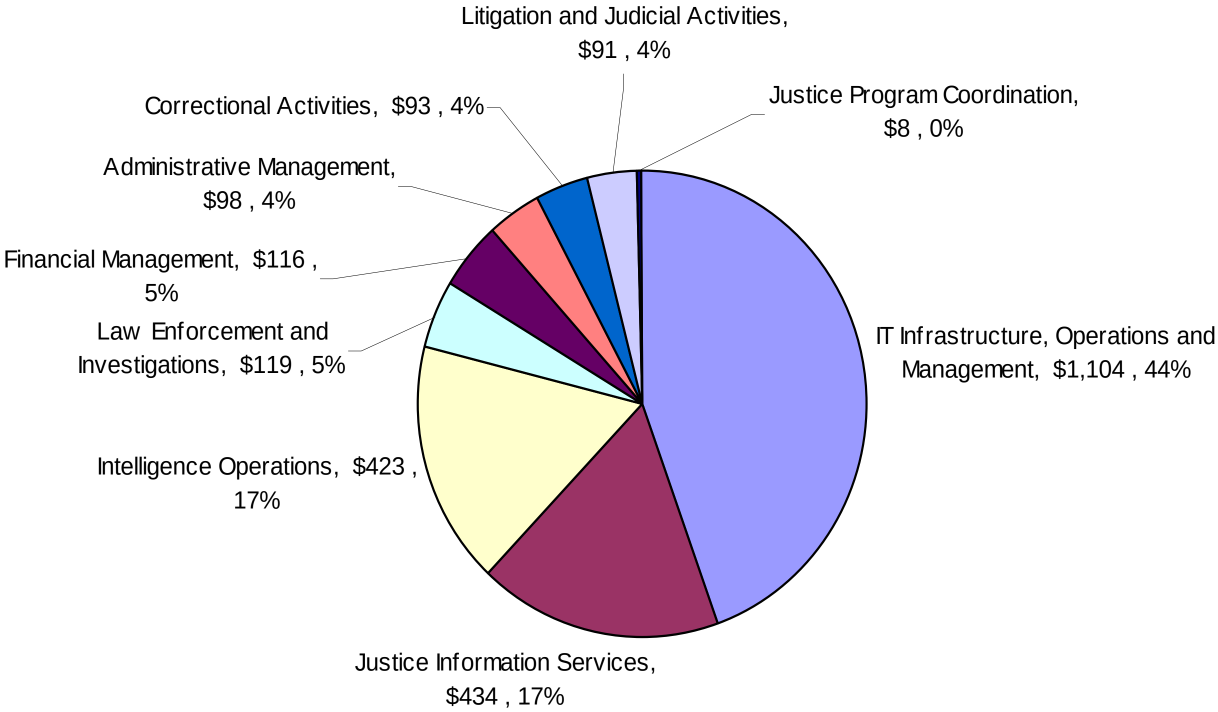


Figure 4: FY07 DOJ IT Budget Allocation by Segment ($2.486 Billion)

3. STRATEGIES

The mission, organizational, technical, and financial challenges outlined above will require the DOJ OCIO and Component CIOs to move to a different operating model. The mission drivers will require increased information sharing, interoperability, and broad-based solutions. The organizational challenges require a more efficient IT management approach, increased coordination among key stakeholders, and more disciplined governance. The financial challenges require greater use of shared services and consolidation, standardization, and optimization of infrastructure. The future operating model is driven by these principles and the primary outcomes of business process interoperability and business process integration.

To achieve these goals, the Department has established five key IT strategies, each having primary objectives for implementation. Table 3 outlines those strategies:

Table 3: DOJ Key IT Strategies and Objectives

Strategies	Objectives
1.0 Share Business Solutions *"Make our Customers more Effective"*	1.1 Deliver enterprise solutions
	1.2 Align IT governance
2.0 Share Information *"Make us more Knowledgeable"*	2.1 Share information across Extended Justice Enterprise
	2.2 Develop and implement required information sharing, data security, and privacy policies
	2.3 Develop information sharing architectural standards
3.0 Share Infrastructure *"Make our IT investments Work Harder"*	3.1 Improve the DOJ infrastructure customer experience
	3.2 Increase the resiliency and quality of our infrastructure
	3.3 Consolidate, standardize, and optimize infrastructure
4.0 Share Acquisition Power *"Make our Purchasing Dollars go Farther"*	4.1 Leverage collective purchasing power
5.0 Share Technology Practices *"Make the IT Organization more Effective"*	5.1 Increase IT collaboration among IT staff
	5.2 Streamline and improve security, audit processes, and reporting
	5.3 Attract and retain a skilled workforce

3.1 Share Business Solutions

In defining the highest level of the business, DOJ depicts the outcome-based business functions of the organization, as shown in Figure 5: DOJ Value Chain below. Five mission-related LoBs represent the major functions of the Department. Each of the LoBs comprises multiple business functions, which represent the major business activities within each LoB. The DOJ Value Chain describes how the Department's mission and strategic planning goals are being executed through the core functions and supporting enterprise processes.

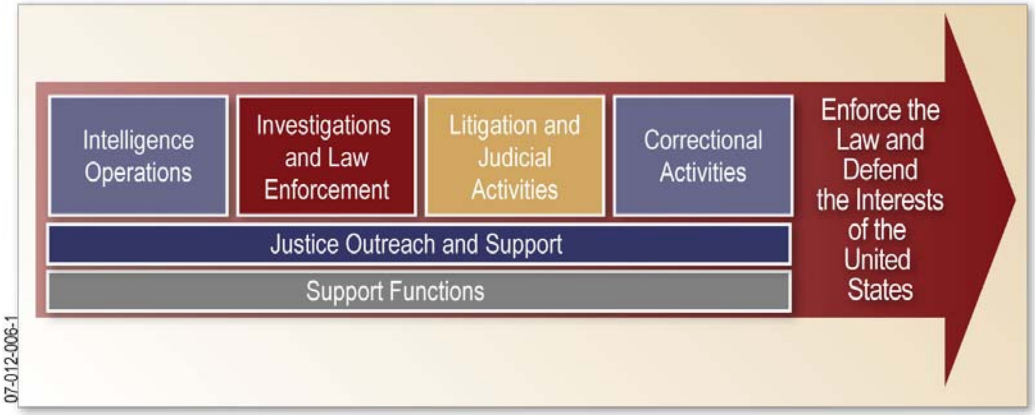

Intelligence Operations
Investigations and Law Enforcement
Litigation and Judicial Activities
Correctional Activities
Justice Outreach and Support
Support Functions
Enforce the Law and Defend the Interests of the United States
07-012-006-1

Figure 5: DOJ Value Chain

The performance of each of the LoBs and output of the supporting business functions need to be the key drivers for all technology investments. It is critical that all IT investments have a clear line of sight to demonstrate how they support the mission and create a return on investment through improved operational effectiveness. Sharing business solutions across these LoBs helps focus IT resources effectively, make our customers more effective, and enable the Department to achieve DOJ's mission priorities.

3.1.1 Deliver Enterprise Solutions

Enterprise Solutions are the primary DOJ programs that represent common solutions addressing the needs of multiple Components or are considered the primary solution for a core mission area. By leveraging these programs to provide services across multiple Components, DOJ is able to reduce overall IT complexity in the Department, eliminate redundant investments, increase information sharing, and make use of shared infrastructure services. Promoting Enterprise Solutions also assists in focusing IT resources by applying them through a more strategic approach to deployment.

The DOJ Enterprise Architecture Program Management Office (EAPMO) identifies enterprise solutions by reviewing all of the major IT programs within the Department and based on a number of criteria including:

- DOJ Segment to which they align
- Cost and size of investment in the program
- Services provided by the program
- Organizational and technical feasibility of leveraging the program's capabilities across multiple components

Moving toward leveraging enterprise solutions drives standardization of business processes, data, and technologies and reuse of IT assets, thereby reducing the cost and complexity of managing the DOJ IT environment. DOJ is implementing key mission initiatives and continues to promote Enterprise Solutions such as Litigation Case Management System (LCMS), Justice Consolidated Office Network (JCON), Consolidated Debt Collection System (CDCS), Justice Secure Remote Access (JSRA), and Joint Automated Booking System (JABS).

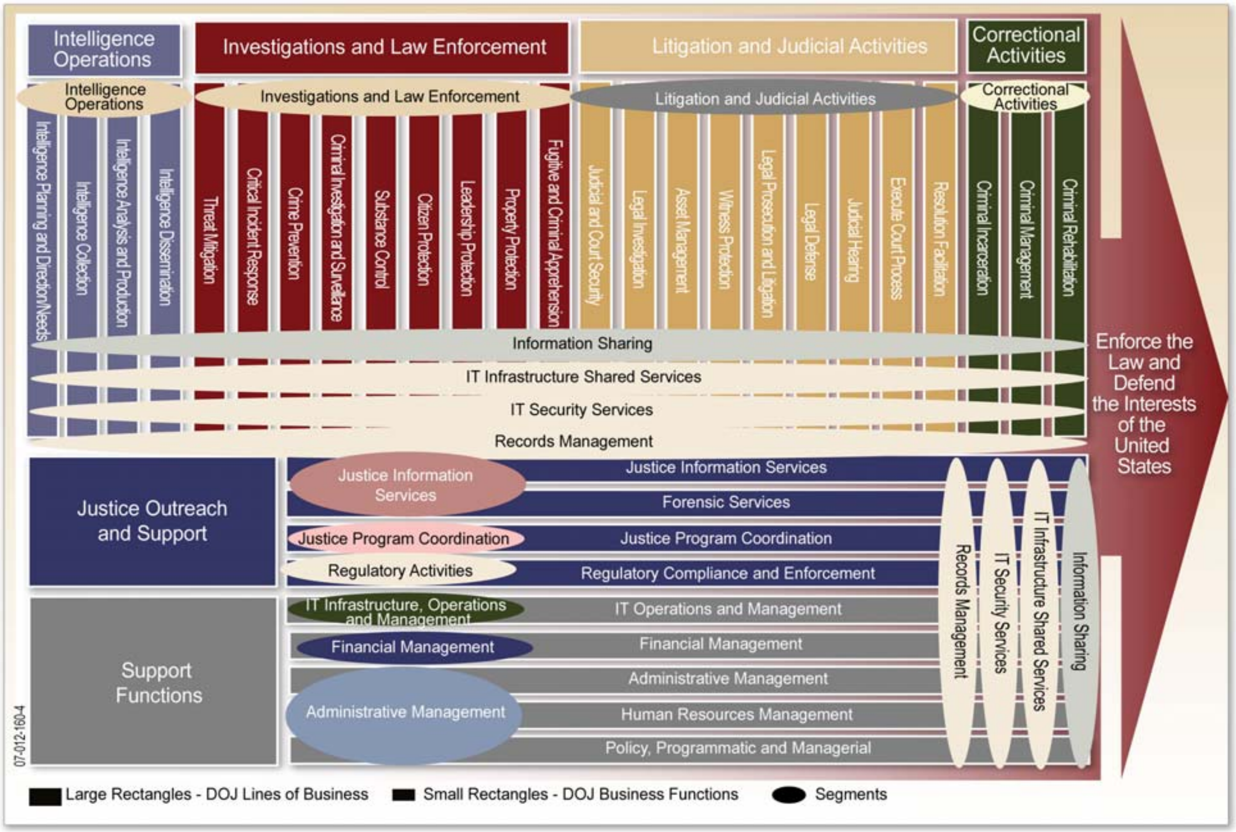

Intelligence Operations
Investigations and Law Enforcement
Litigation and Judicial Activities
Correctional Activities
Intelligence Operations
Investigations and Law Enforcement
Litigation and Judicial Activities
Correctional Activities
Intelligence Planning and Direction/Needs
Intelligence Collection
Intelligence Analysis and Production
Intelligence Dissemination
Threat Mitigation
Critical Incident Response
Crime Prevention
Criminal Investigation and Surveillance
Substance Control
Citizen Protection
Leadership Protection
Property Protection
Fugitive and Criminal Apprehension
Judicial and Court Security
Legal Investigation
Asset Management
Witness Protection
Legal Prosecution and Litigation
Legal Defense
Judicial Hearing
Execute Court Process
Resolution Facilitation
Criminal Incarceration
Criminal Management
Criminal Rehabilitation
Information Sharing
IT Infrastructure Shared Services
IT Security Services
Records Management
Enforce the Law and Defend the Interests of the United States
Justice Outreach and Support
Justice Information Services
Justice Information Services
Forensic Services
Justice Program Coordination
Justice Program Coordination
Regulatory Activities
Regulatory Compliance and Enforcement
Support Functions
IT Infrastructure, Operations and Management
IT Operations and Management
Financial Management
Financial Management
Administrative Management
Administrative Management
Human Resources Management
Policy, Programmatic and Managerial
Records Management
IT Security Services
IT Infrastructure Shared Services
Information Sharing
07-012-160-4
Large Rectangles - DOJ Lines of Business
Small Rectangles - DOJ Business Functions
Segments

Figure 6: Segments in Context of the DOJ Value Chain

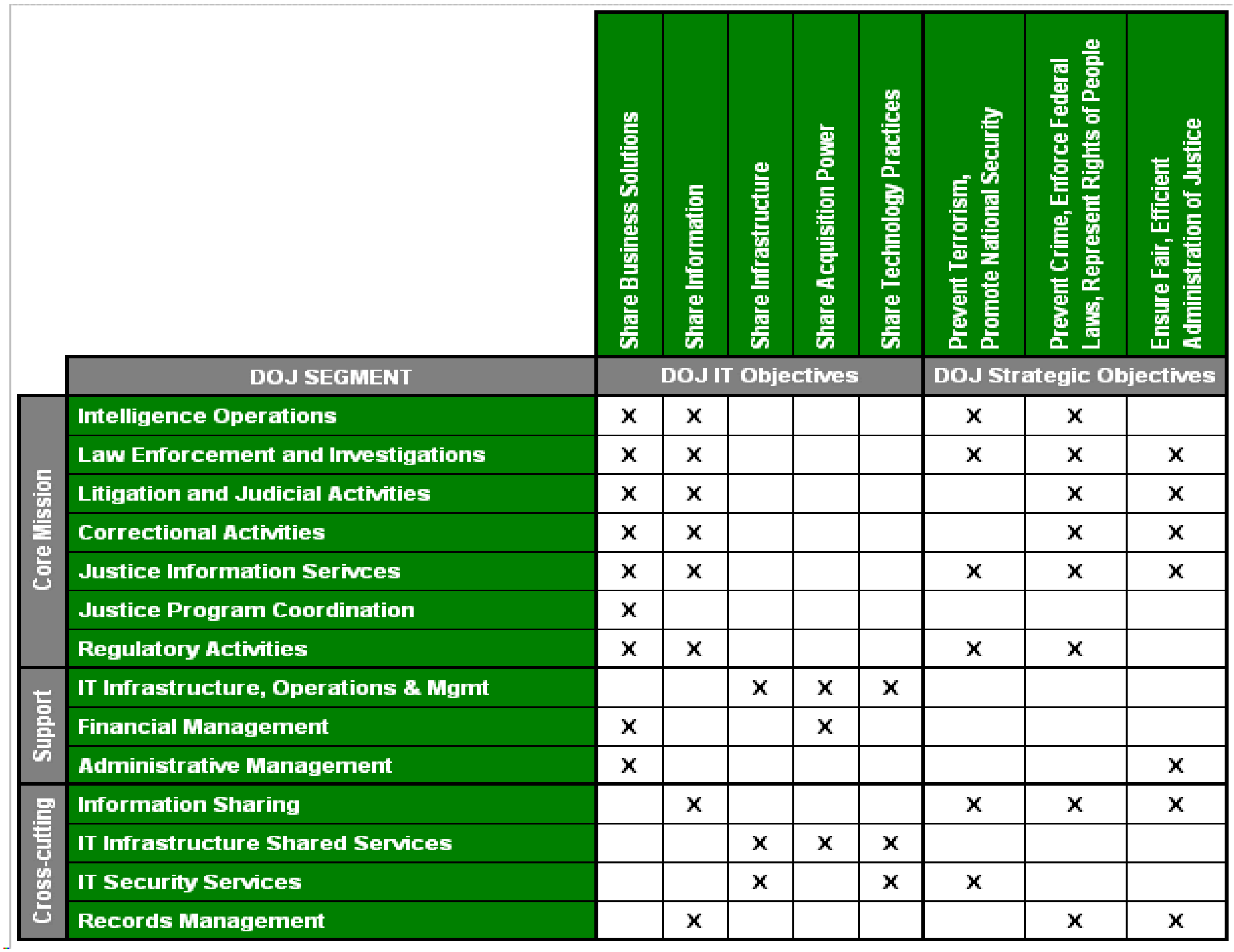
DOJ uses a Segment Architecture[4] approach (Figure 6: Segments in Context of the DOJ Value Chain) to manage its IT resources and to better focus those resources on the continued development and deployment of Enterprise Solutions. Segments serve as a method of organizing the IT portfolio in manageable pieces, while also providing a mechanism for implementing interoperability and sharing across Components.

Segment architecture defines a simple roadmap for a core mission area, business service, or enterprise (cross-cutting) service. From an investment perspective, segment architecture drives decisions for a business case or group of business cases supporting a core mission area or common or shared service. Segment architecture is related to enterprise architecture through three principles: structure, reuse, and alignment. Segment architecture inherits the framework used by the enterprise architecture; reuses important assets at the enterprise level such as data, common business processes and investments, and applications and technologies; and aligns with elements defined at the enterprise level, such as business strategies, mandates, standards, and performance measures.

By identifying and defining segments across the Department, the IT portfolio is organized into logical groups defined by the mission and support functions of the Department. Each group of investments delivers on a common mission purpose or a common cross-cutting service provided by the segment.

[4] Segment Architectures are defined in OMB guidance, "FEA Practice Guidance", Section 2.

Figure 7 below illustrates how the DOJ Strategic Plan and five main IT strategies described in Table 3 apply to these core mission, support and cross-cutting segments.



	DOJ SEGMENT	DOJ IT Objectives					DOJ Strategic Objectives		
		Share Business Solutions	Share Information	Share Infrastructure	Share Acquisition Power	Share Technology Practices	Prevent Terrorism, Promote National Security	Prevent Crime, Enforce Federal Laws, Represent Rights of People	Ensure Fair, Efficient Administration of Justice
Core Mission	Intelligence Operations	X	X				X	X	
	Law Enforcement and Investigations	X	X				X	X	X
	Litigation and Judicial Activities	X	X					X	X
	Correctional Activities	X	X					X	X
	Justice Information Serivces	X	X				X	X	X
	Justice Program Coordination	X							
	Regulatory Activities	X	X				X	X	
Support	IT Infrastructure, Operations & Mgmt			X	X	X			
	Financial Management	X			X				
	Administrative Management	X							X
Cross-cutting	Information Sharing		X				X	X	X
	IT Infrastructure Shared Services			X	X	X			
	IT Security Services			X		X	X		
	Records Management		X					X	X

Figure 7: Segments in Context of the DOJ and IT Strategic Objectives

The DOJ Segments, the participating Components, and the representative Enterprise Solution are outlined in Table 4: Core Mission and Business Segments, Components and Representative Enterprise Solutions. Enterprise Solutions discussed in this section are focused on core mission and business activities within the Core Mission Segments. In the future, we continue to look for additional opportunities to add value to DOJ's mission by developing additional cross-cutting segment architectures.

Table 4: Core Mission and Support Segments, Components, and Representative Solutions

Segment	Components	Representative Solutions
Intelligence Operations	FBI, DEA, ATF, USMS	• FBI SENTINEL • FBI Foreign Terrorist Tracking Task Force (FTTTF) • OCDETF Fusion Center System • FBI Terrorist Screening System (TSS) • FBI Digital Collection • FBI Special Technologies and Applications (STAS)
Law Enforcement and Investigations	FBI, DEA, JMD	• FBI ELSUR Data Management System • JMD Joint Automated Booking System (JABS) • FBI Investigative Data Warehouse (IDW) • FBI HQ Investigative Systems Support • DEA E-Commerce-Controlled Substance Ordering System (CSOS)
Litigation and Judicial Activities	US Attorneys, Litigating Divisions	• JMD Litigation Case Management System (LCMS) • EOIR eWorld
Correctional Activities	Bureau of Prisons, USMS	• BOP Inmate Telephone System-II • Joint Automated Booking System (JABS) • BOP SENTRY • USMS Justice Detainee Information System (JDIS)
Justice Information Services	FBI, ATF, DEA	• FBI Integrated Automated Fingerprint Identification System (IAFIS) • FBI Next Generation Identification (NGI) • FBI National Instant Criminal Background Check System (NICS) • Law Enforcement National Data Exchange (N-DEx) • FBI National Crime Information Center (NCIC) • FBI Law Enforcement Online (LEO) • ATF NIBIN • OneDOJ (formerly Regional Data Exchange (R-DEx) • National Gang Intelligence Center (NGIC) • FBI Combined DNA Index System (CODIS) • Terrorist Explosives Device Analytical Center (TEDAC)
Justice Program Coordination	Office of Justice Programs	• Justice Grants Management System (JGMS)
Administrative Management	JMD	• E-Payroll, eTravel
Financial Management	JMD/CFO	• Unified Financial Management System (UFMS) • JMD Financial Management Information System (FMIS) • DEA Financial Management Program (FMP)

Managing by segments enables DOJ to achieve economies-of-scale through integrated and shared solutions, cross-cutting services, and expanding on one Component's body of knowledge of business processes and technologies to other Components. The emphasis is placed on identifying and implementing Enterprise Solutions and on identifying redundant legacy programs to either retire or migrate to an Enterprise Solution, thereby further reducing the complexity and the cost of the IT environment. The key to this process is the Enterprise Architecture analysis that is conducted within each Segment as the segment architecture is developed and matured. This analysis will identify the status and strategic alignment of each solution contained within a segment. As depicted in Figure 7: Program Evaluation Matrix, the results of Enterprise Architecture analysis supports decisions on whether an individual solution should be retired, migrated to an Enterprise Solution, be designated as an Enterprise Solution, or is a niche program within the Segment. Based on these decisions, the structure and direction of each segment portfolio as well as the overall enterprise portfolio is determined.

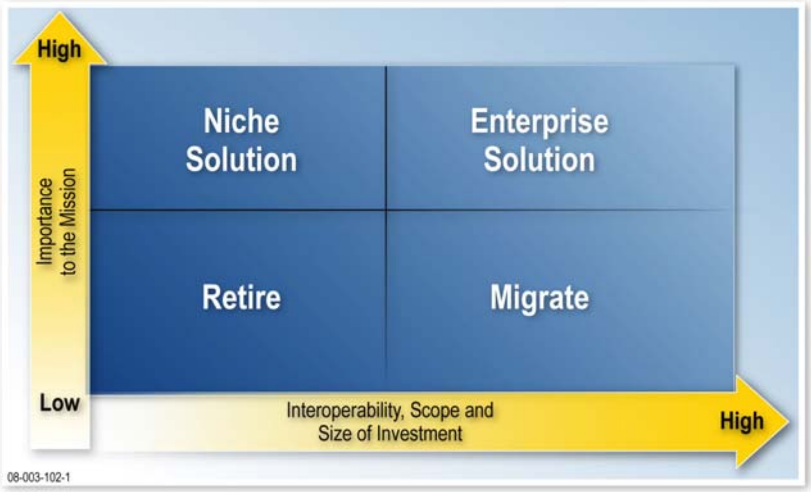

High
Importance to the Mission
Low
Niche Solution
Enterprise Solution
Retire
Migrate
Interoperability, Scope and Size of Investment
High
08-003-102-1

Figure 8: Program Evaluation Matrix

3.1.2 More closely align IT governance to mission needs

To ensure that IT investments are aligned to realize the strategic vision outlined in this plan, the Department continues to refine its IT governance processes as outlined in the IT Governance Guide. The emphasis is on better integration of the IT governance processes both at the Department level and across the federation of Components. Effective IT governance provides the structure and processes to establish and leverage the trust relationship between DOJ Components and the OCIO as well as arrive at agreement on shared value in IT investments. This shared value helps inform the decisions of the governance structures and processes to create a portfolio of investments that provides the greatest return on investment and aligns most closely to the Department's ITSP and ultimately to the DOJ Strategic Plan.

Some of the key elements of the DOJ IT governance structure include:

- **IT Strategic Planning—**Linkage of business strategy, IT organizational structure, roles, and responsibilities, and to external drivers and IT strategies
- **Enterprise Architecture Transition Planning—**IT vision and roadmap for implementation of the ITSP in alignment with DOJ strategic mission objectives and performance measures
- **IT Investment Planning—**Evaluation and allocation of IT resources in line with the strategies outlined in the ITSP (IT portfolio management)
- **IT Budget Planning—**Process by which components use the DOJ IT Investment Plan to prepare IT budget requests. The IT Budget planning process runs for approximately 18 months, spanning the third and fourth quarters of the Planning Year and the entire period of the Budget Year leading up to enactment and appropriation of funding by the Congress.
- **Investment Oversight—**Lifecycle reviews through program/project self assessment, Component assessment and Department assessments via Department Investment Review Board (DIRB) and CIO Dashboard
- **Performance Management—**Results of strategy implementation and return on investment linked to business results
- **Security and Privacy Oversight—**Evaluation of the implementation and execution of security and privacy within programs and organizations within a context of risk management

The governance structure addresses the build-out of the Department's IT governance lifecycle with the integration of the Enterprise Architecture Transition Planning Process to connect IT Strategic Planning and Investment Planning. Additionally, the Department's IT Governance Guide provides detailed descriptions of the IT Oversight Phase compliance review processes identifying initial efforts to integrate compliance reporting and analysis, the implementation of additional compliance reviews, and the introduction of new compliance products and their uses.

3.2 Share Information

A variety of emergency situations in recent years have demonstrated the tragic consequences that often result from the inability of jurisdictions and agencies to effectively share information. Terrorist attacks, natural disasters, and large-scale and organized criminal incidents too often serve as case studies that reveal weaknesses in our nation's information sharing capabilities. Current information collection and dissemination practices have not been planned as part of a unified national strategy. A tremendous quantity of information that should be shared is still not effectively shared and utilized among communities of interest (COIs). The challenges of solving this problem include increasing sophistication and complexity of terrorist and criminal organizations, the highly fragmented and autonomous nature of law enforcement, inadequacy of existing information systems, lack of consistent polices and practices, interagency mistrust, categorization of otherwise shareable information into non-shareable categories, and the need to coordinate information sharing efforts. The key strategies for addressing this issue are discussed in Sections 3.2.1 through 3.2.4.

3.2.1 Share information across the Extended Justice Enterprise

Successful information sharing across the extended Justice community requires DOJ to have accurately defined its information sharing drivers and requirements; established the appropriate governance structures to oversee information sharing initiatives; established the appropriate policies, procedures, and processes; and developed an agile and scalable architecture to facilitate information sharing.

The two primary drivers for DOJ information sharing are DOJ's Law Enforcement Information Sharing Program (LEISP) and the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004. LEISP provides a unified policy framework and coordinated program to address current barriers and creates the needed conditions to facilitate multi-jurisdictional sharing of law enforcement information. The IRTPA established the Information Sharing Environment (ISE) to facilitate the sharing of terrorism information across the Extended Justice Enterprise as shown in Figure 8: Extended Justice Enterprise.

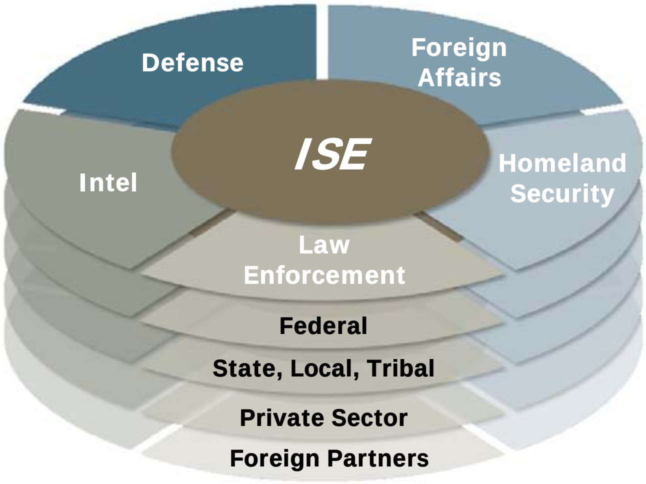


Figure 9: Extended Justice Enterprise

LEISP is a strategy that enables the collaboration and sharing of information across the law enforcement community. OneDOJ (formerly R-DEx) and N-DEx are the Department's first two programs implementing the LEISP strategy. Oversight of LEISP is via the LEISP Coordinating Committee (LEISCC). The Department is committed to finalizing the current implementation of OneDOJ and N-DEx both internally within DOJ and with external partners as a rapidly as possible so that the significant value to information sharing that these two initiatives bring can be fully realized. The planning for the next phases of these two initiatives outlines the vision of continuing to implement needed functionality as rapidly as possible.

As part of LEISP, the Intra-DOJ Information Exchange Architecture (IDEA) Infrastructure is the Department's enterprise solution to provide a secure, automated, electronic distribution facility to integrate the Department's data sources for providing data to OneDOJ and N-DEx. The infrastructure uses the Law Enforcement Exchange Standard (LEXS) to exchange information using a common XML-based approach and includes specifications that define how partnering law enforcement applications can implement federated search capabilities to access distributed information for their corresponding users. DOJ continues to scale the use of IDEA and LEXS across the Department.

In support of information sharing, DOJ plays an executive role in National Information Exchange Model (NIEM) and the Global Justice Information Sharing Initiative (Global). This role enables DOJ to foster sharing with other Federal and SLT agencies including fusion centers to ensure the appropriate exchange standards are in place to support the broad scale exchange of pertinent justice and public safety information. In addition, this participation provides the justice community with timely, accurate, complete, and accessible information in a secure and trusted environment. DOJ continues to participate in governance bodies such as the NIEM Business Architecture Committee (NBAC), NIEM Technical Architecture Committee (NTAC), NIEM Priority Exchange Panel (NPEP), Global Executive Steering Committee (GESC), Global Advisory Council (GAC) and the CJIS Advisory Policy Board (APB) to achieve these goals.

Driven by IRTPA, the DOJ is working in conjunction with the ISE and participates in advisory groups including the Counter Terrorism Information Sharing Standards (CTISS) Working Group (WG), the Chief Architect's Forum (CAF), and the Business Process Working Group (BPWG). DOJ continues to provide executive and strategic support regarding the adoption of the frameworks and standards being developed by the ISE. DOJ's primary focus is using NIEM as the standard for developing the ISE exchange standards through the CTISS WG. Specifically, DOJ led the development of the ISE Suspicious Activity Reporting (SAR) Functional Standard the current operational study to implement it.

By integrating the internal activities and implementing the DOJ LEISP program with those of the PM-ISE, DOJ approaches information sharing from both an internal and external partner perspective.

As these frameworks, programs, and standards are rolled out across the extended Justice community, it is essential the appropriate users can access information using simplified access mechanisms. Under the LEISP umbrella, DOJ conducted a Federated Identity Management (FIDM) pilot by bringing together multiple environments designed to serve five agency communities: intelligence, law enforcement, defense, homeland security, and foreign affairs using a "trusted broker" approach. The Department successfully made the JABS application available to members of the local law enforcement community through the existing authentication channel, the Law Enforcement On-Line (LEO). DOJ continues its work on FIDM, working with its partners at the PM-ISE, DHS, and SLT agencies.

Going forward, DOJ strengthens its commitment to NIEM, the ISE, and LEISP through enhanced resources and capability to support its continued implementation and extension within DOJ and to its external partners. The end result of this is an environment in which DOJ and other Federal-agency critical data sources as well as non-standardized functionality and specialized analytic processing (e.g., fusion centers) can be shared across the enterprise. The Department continues its efforts in integrating privacy and information sharing by developing a more robust privacy training program, implementing the ISE Privacy Guidelines, adding a civil liberties assessment as an addendum to the PIA, and finalizing the DOJ Data Protection Program policy.

3.2.2 Develop and implement required data security and privacy policies

DOJ also has a responsibility to uphold the public trust and the information we collect, and the OCIO recognizes the dual concerns of security and privacy. Security consists of reliability, availability, and integrity of data and privacy deals with protection of individual privacy and sensitive data. Critical data security and privacy issues must be addressed in a proactive way to ensure that each party involved in data sharing is assured that the data they provide and consume is reliable, has integrity and is protected from unauthorized release. This entails a set of activities to reaffirm and extend the LEISCC, the governance and policy adjudication body for DOJ-wide information sharing. This Council plays a key role in developing and establishing policies for sharing, including the determination of data security and privacy policies that incorporate the specific uses of the data by the various entities involved in the sharing process

It is equally critical to continue to enhance the data security policy framework as well as the structure, processes, and technology. This is especially critical in the environment where this information is shared between many disparate entities, including Federal, State, and Local governments across different security domains.

It is important to address the issue of network intrusion and processes to respond to security events are fully in place and effective. The key to this is the Department Incident Response Teams and their ability to react quickly and effectively to security events as they happen. To ensure that DOJ is fully capable of this level of response to security events, the current team structure and processes are being reviewed and needed changes will be made as recommended.

To further address the issue of protecting individual privacy, the department, in conjunction with the Office of the Director of National Intelligence (ODNI), developed privacy guidelines for the ISE (a collection of procedures, policies, and standards for sharing terrorism-related information among all levels of government). The President signed off on the guidelines in December 2006.

The Department continues to improve the development and use of Privacy Impact Assessments (PIAs) within both architecture and system development efforts. PIAs evaluate what effect a new system or a significant upgrade has on the privacy of the system’s data. In a PIA, components must describe the basic use and purpose of the system, what information is being collected, what technical access and security protections are being put in place, to what degree the data is being shared, and what privacy risks were identified and how they were corrected. The PIA template is posted on the DOJ intranet for component use. There is also an effort to assess and recommend needed extensions to PIAs with DOJ CPO in accordance with existing statutory and policy guidance.

To address data security and intrusion protection, it is important that both applications and infrastructure are fully up to date with the latest security patches and most effective system configurations. This is a difficult and ongoing process that requires effective strategies as well as tools that assist system administrators and program managers to maintain concurrency with software vendor changes. To assist with this, DOJ continues to review existing tools, policies, and procedures for managing configurations and versions to ensure they provide the most effective, highest level of security capabilities.

Finally, it is essential to approach security from an enterprise perspective by developing and implementing common IT security architecture along with common security services that will be used across all Segments. This ensures consistency as well as a much greater level of data protection across all Departmental systems.

Going forward, the Department will focus on key issues in this area:

- Develop a new policy for privacy in remote access
- Add a civil liberties assessment addendum for national security PIAs
- Develop more robust privacy training

- Implement the ISE privacy guidelines across participating agencies

3.2.3 Protect personally identifiable information (PII) and sensitive data

DOJ is conducting a vulnerability assessment project, which continues to use technology to improve the vulnerability status of all DOJ systems. In addition, configuration management is a priority while moving toward Center for Internet Security (CIS) benchmark system hardening compliance. Research and testing is being conducted on removable media, Personal Data Assistants (PDAs) and Smart Phone encryption. Blackberry Enterprise Servers, Blackberry devices, and the remote connections between them are being secured to the IT Security Technical Guide. Data flow analysis, to know where data moved and by whom, where, and how the data is saved allow DOJ to choose the correct data protections for the different missions and sharing requirements of all DOJ data. Enterprise rights management will be addressed for its value in role-based data access matched with controlled encryption. With the added need for remote access, Wireless policies and protections are being developed to support the mission of those employees and support staff working remotely.

The discussion of privacy versus security in the handling of information takes on renewed urgency amidst conspicuous instances of compromised data, such as the stolen Department of Veterans Affairs (VA) laptop containing the personal information of over 26 million American veterans in May 2006 or the Boeing laptop stolen in December 2006 containing extremely sensitive personal information such as Social Security Numbers, names, and addresses for over 382,000 of its current and former employees. DOJ itself collects personal information, from investigative, witness, and litigation information to prisoner and personnel records, and we process and store PII in many of our IT systems. A breach of IT security could expose personal data to theft and cripple DOJ's ability to complete its mission. The DOJ has a responsibility to its constituents and its employees to protect the privacy of their personal information in the Department's IT systems.

It is especially important that privacy policy issues be effectively addressed in a formal way to ensure that sensitive data is protected. This requires reaffirming and extending protections around privacy of constituent data in accordance with policy and law. A key Component of this is ensuring that the most appropriate technology solutions such as FIDM are brought to bear on this issue. Critical engineering support for privacy requirements, including the protection of PII, continues to be a requirement. Finally, there will be an effort to assess and recommend needed extensions to existing privacy policies that will serve to improve the capability to protect data that is being shared between government entities and lower the risk associated with that process.

In June 2006, OMB issued Memorandum 06-16 in response to the theft of the VA laptop, laying out mandates for protecting sensitive information on Federal agency remote access mechanisms, such as JSRA, and on remote computing devices, such as laptops, cell phones, Blackberry devices, and PDAs. The memorandum also required each Federal agency to complete a review of the status of its remote access security within 45 days. The DOJ CIO reacted to this requirement by creating the Data Protection Program, which directs all Components to ensure that all remote computing devices employ an encryption mechanism certified in Federal Information Processing Standard (FIPS) 140-2 and submit a plan to the CIO for bringing in remote access solutions into compliance with departmental policies.

3.2.4 Develop required information sharing architectural standards

The DOJ is using its Enterprise Architecture as the means to document and communicate DOJ's role in these information sharing initiatives. DOJ has developed the ***DOJ Information Sharing***

Segment Architecture (ISSA) document, which outlines the DOJ strategy for architectural standards and technologies to enable information sharing. The Segment is defined as an enterprise service[5] in the DOJ Enterprise Architecture. The ISSA uses a set of business scenarios to provide prescriptive guidance to Core Mission Segments in terms of applicability of standards and highlighting the needed information exchanges. The business scenarios include Justice Outreach (i.e. Criminal Justice Information Services (CJIS) and OneDOJ), the Justice Lifecycle (Investigation to Litigation to Sentencing and Corrections), and Terrorism Information Sharing (e.g., SAR). DOJ is leveraging the work being done under LEISP, NIEM, and the ISE to complete these scenarios. To drive adoption of standards and alignment to overall enterprise architecture, the ISSA will be leveraged during Department's investment reviews and program architecture assessment processes.

The DOJ OCIO has adopted NIEM as the standard for documenting information exchanges. DOJ continues to expand on the integration of LEXS and NIEM across the DOJ. The Department will also support the ISE CTISS WG in developing additional information exchange standards following the NIEM Information Exchange Package Documentation (IEPD) Development Lifecycle. DOJ will work with its Federal and SLT partners for opportunities in reusing the NIEM and ISE standards.

In addition, the DOJ has adopted the principles behind Global's Justice Reference Architecture (JRA) which is a technical implementation that addresses the full range of information sharing use cases, and provides a comprehensive blueprint for implementing interoperable data sharing services and capabilities.

For the successful implementation of the DOJ Information Sharing Segment Architecture (ISSA), the data security and privacy issues must be addressed aggressively up front. This requires reaffirming and extending the governance processes and policy activities around information sharing. To fulfill this strategic vision of horizontal and vertical information sharing, an effort is being made to connect and build upon existing systems, to create enhanced data privacy safeguards, and to incorporate auditing mechanisms.

The DOJ *Information Sharing Segment Architecture (ISSA)* provides an enterprise perspective on information sharing activities, drives the adoption of existing exchange standards and technologies, considers security and privacy issues in an information exchange and describes how information sharing principles are integrated throughout DOJs Enterprise Architecture.

3.3 Share Infrastructure

The Department employs an extensive IT infrastructure to support its diverse missions and organizational units. Currently, multiple systems have become overly complex, conform to a range of standards, require highly trained technical and administrative personnel in each Component, and employ a wide array of COTS packages that address the same issues. These systems exist as isolated enclaves within organizations and rarely exchange information except through specialized integration and conversion gateways. IT Infrastructure is an area of

[5] Enterprise services are defined by the Federal Enterprise Architecture (FEA) as common or shared IT services supporting core mission areas and business services.

significant expenditure (See Figure 4) within the overall budget at DOJ and includes technology such as networks, data centers, end-user computing, and IT operations.

The Department's IT infrastructure modernization and growth has highlighted the need for a consistent enterprise infrastructure approach suitable for all DOJ organizations and applications. Investments in the centralized IT Infrastructure solutions can provide the required infrastructure services to DOJ Components and align with the IT Infrastructure O&M Segment. Such investments can lead to standardization, consolidation, and therefore optimization of the IT infrastructure across the entire Department. IT programs can leverage existing infrastructure services that are provided by any DOJ Component or new infrastructure services that are provided either centrally or by a lead Component, thus reducing the need for multiple Components to build and maintain similar infrastructures themselves. By leveraging these infrastructure programs to provide shared infrastructure services across the Department, DOJ can reduce overall IT infrastructure expenditures while providing consistent quality services to the mission Components.

The benefits of using a shared services infrastructure model for Components include:

- **Competitive pricing—**ability to leverage economies of scale savings to pass on to Components
- **Security and Continuity of Operations (COOP) compliance—**government mandates are reflected in the design of the product
- **Product quality and performance—**design built on a common set of Component requirements, industry best practices, and lessons learned
- **Product range and flexibility—**not a "one size fits all" solution, for example, while delivering on a base set of standard out-of-the-box functionality, solution is configured to meet Component-specific requirements
- **Deployment reliability/delivery speed—**develop implementation and migration processes (e.g., scheduling, training, application integration, etc.) in a manner that is least disruptive to current working environment
- **Post-migration support—**operations planning and support considered early in the planning process to engage multiple stakeholders, while offering the power to control the level of service to the Components formalized in SLAs and ability to review delivery performance with Component management team. It is important to note that Components can retain control of the service delivery through service level agreements (SLAs) and memoranda of understanding (MOUs).

Sections 3.3.1 through 3.3.3 describe the primary actions for achieving these objectives.

3.3.1 Improve DOJ infrastructure customer experience

For infrastructure to be effectively shared, the satisfaction of customers must be a critical priority. Customers must have confidence that infrastructure services be consistent, meet their performance objectives, and flexible enough to adapt to their changing business requirements. Customers must have confidence that the infrastructure services they procure meet the desired service levels monitored by SLAs and security compliance mandates. To reach this objective, a

Customer Service Assessment process is being initiated to determine customer expectations for shared infrastructure services. The results of this assessment forms the basis for a reengineering of the Department's approach to providing shared infrastructure services, including service definition, service provisioning, and issue resolution. Improved service management and service delivery processes is being designed and implemented based on customer requirements. This effort will also focus on the development and deployment of enhanced collaboration tools for DOJ employees as well as an integrated, cohesive internal identity management capability for both electronic and physical access.

3.3.2 Increase the resilience and quality of infrastructure

A critical factor of quality infrastructure services delivery is the ability to support expected levels of system restoration and COOP Plan in the event of man-made or natural disasters. It is incumbent on the Department, in moving toward shared infrastructure services, to engineer into the consolidated systems the level of redundancy and response necessary to meet customer requirements. To determine these requirements, a formal COOP needs to be developed jointly with Components that will identify critical systems requirements, performance metrics, restoration levels and availability requirements. An engineered solution includes a capability to support a formal infrastructure to deliver security operations, incident reporting and management, and remote management capabilities.

The most critical objective of delivering a resilient infrastructure is the ability to reduce risk and the ability to deliver services at customer-required service levels cost effectively. The key to this is to develop and implement Enterprise-level security services that are architected to industry standards and can provide the agreed-to levels of risk reduction to all Components. Three critical features of this approach are to finalize development of the Department-wide IT Security Program Management Plan in close coordination with Department Components; develop Department-wide enterprise security architecture and IT Security Technical Guide; and develop and implement both enterprise security services and a world-class enterprise security management and monitoring capability to implement the Plan. To further demonstrate quality infrastructure services, it is critical that infrastructure products are designed, built, and configured to meet the Component service levels requirements. It is important to follow this up with implementation, migration, and post-migration support to demonstrate commitment to improving customer experience.

3.3.3 Consolidate, standardize, and optimize infrastructure

The first step in moving to shared infrastructure is leveraging the DOJ Enterprise Architecture to characterize the Department-wide infrastructure portfolio and identify opportunities to standardize, consolidate, and ultimately optimize the infrastructure. Based on this characterization, analysis can be conducted to identify ways to reduce increasing complexity and duplication through effective investment management. Consolidating the procurement process across the Components can reduce costs and improve performance. Finally, customer experience and continuity of operations data can drive process improvement efforts that enhance the optimization of infrastructure investments.

Figure 9 depicts the current (FY 2007) breakout of IT Infrastructure Operations and Management Segment funding by major areas.

Network – Communications services, including terrestrial, wireless, and land mobile and the support activities associated

Data Center – Storage, management, hosting, facilitation and dissemination of electronic data and information to multiple users

IT Operations – Administration operation and maintenance of the data center, network and end user computing capabilities

End User Computing – Computing platforms and appliances to the users.

IT Security – Secured access and monitoring of government IT infrastructure

Infrastructure Management – Ensuring infrastructure operations are efficient and effective

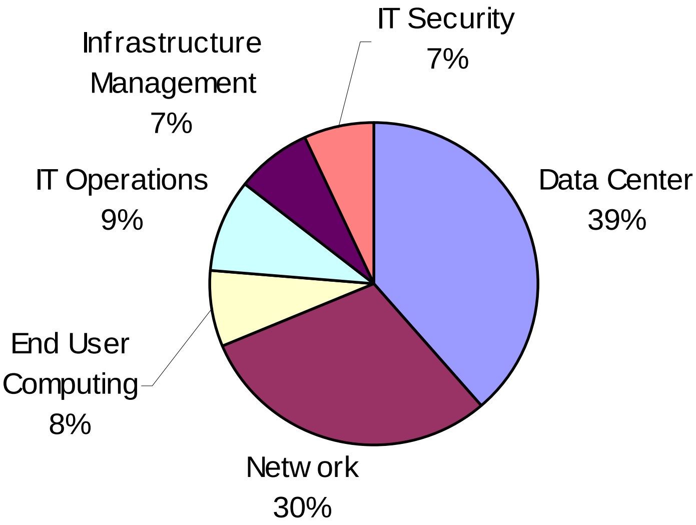


Figure 10: DOJ IT Infrastructure Operations & Management (FY2007)

The analysis of the IT Infrastructure Operations and Management Segment spend helps determine the appropriate program synergies and consolidation candidates.

Another issue that is identified from analyzing this financial data is the very large percentage of IT spending (over 75%) is component-specific (See Figure 10). This analysis illuminates the initial opportunities for investing in existing programs and the opportunities for consolidating duplicative infrastructure services. A major objective of this strategy is to reallocate redundant Component-specific infrastructure investments to cross-Component programs benefiting the entire Department. As shown in Figure 10, a very large percentage (over 75 percent) of the IT Operations and Management investments for FY07 were Component-specific.

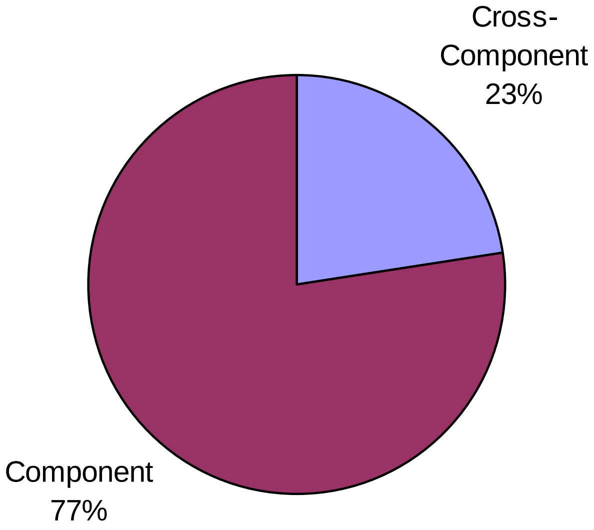


Figure 11: IT Operations and Management Investment—FY2007 Cross-Component Spend

To achieve this strategy, the Department has taken steps to ensure use of common IT Infrastructure Shared Services by components across the Department. As described in Section 2.3, OMB is mandating through the ITI initiative that agencies move towards consolidated and optimized infrastructure environment. Through this continued analysis and program outreach, a standardized, consolidated, and optimized infrastructure can become a reality. Once the infrastructure services are matured and able to meet the requirements of the Department, existing and new programs can start transitioning to using these services and migrate or retire their own redundant infrastructure.

3.4 Share Acquisition Power

DOJ needs to take better advantage of the scale of aggregate external expenditures to achieve lower pricing and improved quality of service. Components and the Justice Management Division (JMD) primarily procure software, hardware, and IT support services separately. By using the Enterprise Architecture and Asset Management best practices, DOJ can begin to understand and categorize IT expenditures by product and service across the Department. This enables the identification of opportunities to consolidate purchases at levels that can drive substantial discounts from suppliers. In addition, DOJ intends to identify and share price information obtained across the Department and proactively promote better price points from vendors. Finally, DOJ intends to promote optimal sourcing of DOJ-wide services to preferred providers, which can be a Component- or JMD-level or can be outsourced to a commercial entity.

Sections 3.4.1 through 3.4.4 describe the primary actions for achieving these objectives.

3.4.1 Collectively identify and track vendors, products used, and services provided

By developing an enterprise architecture that cuts across the entire Department and by building out the architecture in logical business focused segments, DOJ begins to create a database of information about the products and services that are used within Department programs to deliver IT value. This data can begin to show which vendors are used by each program and the services and products that are provided by each vendor. This is powerful information for the Department to be able to use in developing plans and processes to leverage its buying power for both products and services and in working with common vendors to improve both the scope and quality of what each vendor provides.

Using the data developed in the Enterprise Architecture process, the process of identifying key products being used across the Department that are common to two or more Components helps drive towards consolidated enterprise licensing agreements (ELAs) and blanket purchasing agreements (BPAs) with the product vendors. The ELAs should be developed and tracked depending on product or service type. For example, the BPA model for printer purchases initiated and managed by the Executive Office for United States Attorneys (EOUSA) could be used by any DOJ components. This should help lower the cost of these products for Components, thereby obtaining greater levels of consistent support across the Department and from the product vendors.

3.4.2 Develop and implement vendor performance standards

The data developed within the Enterprise Architecture process can also help to support processes for systematically measuring the performance of vendors in meeting the service levels of key programs across the Department. As part of this process, the Department should develop a vendor performance reporting template that can use enterprise architecture data to establish for each vendor performance indicators, metrics, and service levels that are tied to the strategic business and IT goals and strategies outlined in this ITSP. This performance measurement process and the data developed during the Enterprise Architecture process can help to ensure that vendors are strategically aligned with DOJ priorities and rewarded for good performance. It can also help the Department to identify key suppliers who are effectively supporting enterprise goals to assist in growing those relationships.

3.4.3 Characterize IT demand and supply to support DOJ-wide enterprise goals

A key use of our DOJ Enterprise Architecture and associated processes is to help shape the demand for, and manage supply of, business applications, IT services, and shared data. This is accomplished by characterizing demand and supply in a standardized manner and funneling demand for similar applications, data, services, and technology to appropriate suppliers within the Department that can leverage internal Component-based shared services or external smart sourcing. A further dimension for characterization is performance. On the demand side, this is satisfied by a qualitative view of the business case; on the supply side this comes down to service and cost metrics.

The key to achieving this action is to start with standardized models and frameworks for characterizing demand at a high level through the Enterprise Architecture. The next step is to put demand in context through Segment architectures. The details are fleshed out by developing cross-cutting enterprise service architectures for information sharing and infrastructure shared services. This final level of detail then is tied to the overall *DOJ Transition Strategy and Sequencing Plan*, which brings together the higher-level picture of demand and supply. This is crucial to tracking return on investment in terms of improved mission performance, cost savings, and cost avoidance.

A major hurdle to conducting strategic management of demand and supply as described is the poor quality of data that we do have across the Department in this regard. The plan moving forward is to improve data quality through institutionalizing program and Component guidance through the *DOJ Enterprise Architecture Program Managers User Guide*. This document provides guidance for enterprise architecture data collection, clearly linked to the lifecycle status of the program and integrated into the Department CPIC and annual budget processes.

3.4.4 Effectively integrate security requirements into the acquisition process

It is critical to build security into systems development and implementation efforts at the earliest stages. To accomplish this, it is critical to integrate security requirements into the earliest acquisition processes including requests for information (RFI), requests for quotes (RFQ), as well as requests for proposals (RFP). The most effective way to do this is to identify security requirements within the Enterprise Architecture process at each level of the architecture, in particular the target architecture, both at the enterprise level as well as at the segment architecture level. When security requirements are built into the architecture and an overall enterprise acquisition process flows from the identification of the target architecture, security is embedded into both the design and development processes for new systems as well as the acquisition process for securing the products and services for those system initiatives.

3.5 Share Technology Practices

To fulfill the promise of increased program performance through the effective use of information technology and to take advantage of using Enterprise Solutions, shared information, shared infrastructure, and shared acquisition power, it is critical that the IT community perform at a high level. The degree to which this community can bring industry standard practices, processes, and tools to this endeavor will help define its success in fully supporting DOJ's strategic goals and objectives. This is especially critical in assuring the security and privacy of the data that the Department holds in its custody and uses to fulfill its responsibilities, including jointly with law enforcement and intelligence partners at the Federal, SLT, and international levels.

3.5.1 Increased collaboration among IT staff

To effectively guide the implementation of this complex and forward-looking strategy it is critical that the key IT leaders within the Department, both at the Component level and within the OCIO work collaboratively and effectively together. To this end, the restructuring and enhancement of existing vehicles such as the Department CIO Council and other coordinating and advisory entities are a key initiative. In particular, the CIO Council must become a key forum for discussion and agreement on key policy directions, technical strategies, and organizational issues required to effectively implement this ITSP.

Given the federated nature of the DOJ, it is important for Component CIOs, as well as the Department CIO, to have a forum to discuss these key issues and to arrive at collaborative decisions. The restructured and repurposed CIO Council provides that forum. Another forum would be to hold one-on-one meetings between the Component CIO and the Department CIO to discuss key issues.

In support of the restructured and reenergized CIO Council, other supporting groups are being either re-chartered or created. These include a Department Architecture Advisory Board (DAAB) as well as specific technology domain working groups such as the Standard Infrastructure Working Group (SIWG).

3.5.2 Streamline and improve security, audit processes, and reporting

The DOJ has identified several management, operational, and technical initiatives that are focused on improving protection of agency information systems and sensitive data. The integration of security into the overall planning and implementation of IT resources has to be one of the most important efforts at the management level that can bring about a well-funded, consistent approach to the deployment of security monitoring tools. This can be enabled by the development of a DOJ-wide security architecture that is being developed jointly by all Component IT Security Chiefs under the CIO's supervision.

The deployment of jointly owned IT security resources will be supported by the Justice Security Operations Center (JSOC) project. The JSOC will provide a single real-time report of correlated events across all DOJ networks. The JSOC, which is still in the planning stages, will be in operation in 2008. Other initiates include the Security Content Automation Protocol (SCAP). This is a method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation (e.g., Federal Information Security Management Act (FISMA) compliance). The Department's IT security staff are committed to moving toward an automated compliance and audit process that can help Components achieve compliance in less time and at lower cost.

3.5.3 Attract and Retaining a Skilled Workforce

The key to delivering on the promise of IT that enables program success is through the attraction, retention, and growth of skilled government technology staff who can manage and oversee the partnership with top commercial and government providers of technology services to the Department. It is critical for the Department to continue to recruit and then retain top-level staff in key IT positions such as enterprise architects, program and project managers, IT security managers, contracting staff and officers with a deep understanding of IT contracting requirements, and, most importantly, staff who would like to move into key managerial and executive positions in the future. Government staff must continue to provide key leadership and direction to the IT program of the Department, as most technology implementation and operational work is being outsourced to commercial and other government service providers.

This evolution requires government staff with critical skills in the development of long-range technology strategies that help to drive program improvement; understanding how various complex technologies can enable a efficient program operation; development of architectures to drive implementation of those technologies; strategic skills in the management and oversight of large, complex IT projects critical to the Department's objectives; and skills in the purchase of these technologies and the service providers that help to implement and operate them.

While programs currently exist to attract, recruit, and retain staff with these skills, it is critical that these programs and processes be enhanced and expanded. Competition for quality talent at all grade levels is increasing with commercial providers as well with other government agencies. The Department must be able to provide exciting and rewarding IT careers to top-level prospects to secure talent and succeed in this competition. With constraints on salaries within the Federal government, it is critical to offer staff the opportunity to grow rapidly in their skills, in work assignments, and in levels of responsibility. It is also important to create other ways to increase the compensation package for these employees. This can be done through improved performance award packages based on performance plans that are tied directly to program success. As IT performance is more closely linked to improvements in processes and ultimately to program and customer outcomes, the contributions of key staff should be linked to this success. This also requires a progressive management and technology training program that is funded on a long-term basis; mentoring programs that facilitate the growth of talented managers and executives; and certification programs and processes that facilitate staff to grow rapidly into technology leadership positions.

Most importantly, government staff must believe that they are able to accomplish significant and important goals that directly contribute to the success of the Department's key programs. The DOJ is a key player in the war on terrorism, in critical law enforcement efforts throughout the country, and in carrying out fundamental justice in a democratic society. IT is playing a critical role in delivering on the Department's goals for those programs. Attracting, retaining, and growing key IT staff to manage and oversee the programs and projects that deliver on this promise is the most critical objective goal of this ITSP.

The Department has taken some actions to address these objectives through the "IT Workforce Skills Assessment Survey." This survey should be used as a basis to develop a training plan for each of the grade levels of the 2210 IT Series. This helps to proactively identify both strengths and needs in our IT workforce and to implement strategies and activities to address the needs. Further guidance on the human capital management goals and objectives can be referenced in the recently published DOJ Human Capital Strategic Plan: http://www.usdoj.gov/jmd/ps/missionfirst.pdf.

4. KEYS FOR IMPLEMENTATION

The previous chapter introduced several opportunities for increasing value. This section looks at the Department's capability to deliver this value. Clearly, the target will be to focus on highly developed and valuable opportunities while continually improving the Department's capability to deliver as shown in Figure 11.

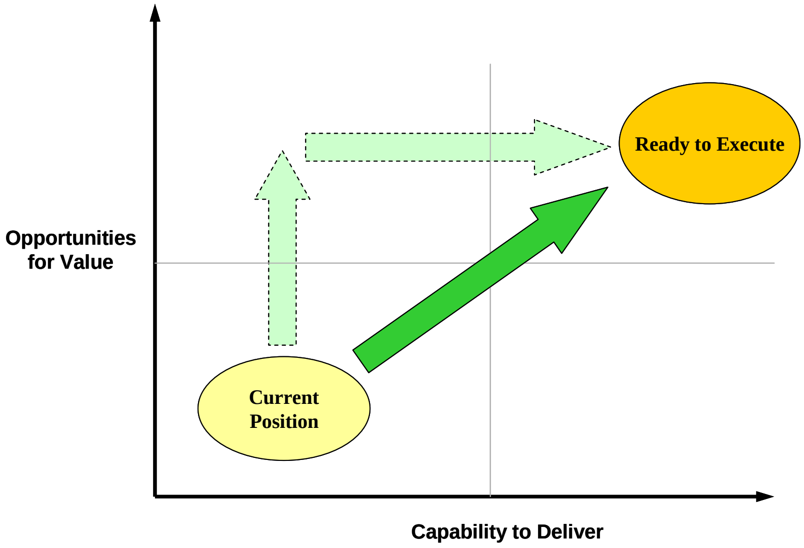


Figure 12: DOJ Maturity of Vision and Capability

In implementing the strategic initiatives, we see the following dimensions as key to improving the Department's delivery capability:

- Operational excellence
- Evolving the business model
- Organizational implications including management requirements
- Stronger cross-organization governance and policy support

For these dimensions, DOJ will continue to rigorously develop our understanding of where we are, where we need to be, and how we get there. Closing the gap involves making decisions about fundamental change in how we operate. Therefore, this analysis must involve key stakeholders: IT leadership across the Department; Budget and Finance leadership; and Department and Component Executive leadership. Then, together with our stakeholders, making the trade-offs between our ability to absorb change, the value enabled by the change compared to the risk, and the level of executive sponsorship across the Department move to close the identified gaps.

4.1 Operational Excellence

A core prerequisite for success in delivering on this plan is the ability to undertake IT projects and operate IT infrastructure with operational excellence. IT projects are complex and fail to deliver on cost, time-to-delivery, quality, and business expectations at a high rate. Many of the risk factors for these failed projects —a federated distributed operating environment, very large-scaled operations, and a rapidly evolving mission environment —are present within the DOJ environment. Furthermore, customer expectations for user experience, service levels, and degree of data integration and performance are constantly rising due to both the pervasiveness of IT in popular culture, the reality of the modern online consumer experience, and the centrality of IT to enabling mission performance.

Therefore, it is incumbent on the Department to focus on the critical operational drivers that can reduce the inherent risk factors present within DOJ, while at the same time implementing world-class IT operations, business practices, and tools that can deliver the service levels and performance expectations of mission Components.

Improving IT management effectiveness is a constant focus, and IT organizations across the Department have successfully instituted and are continually improving practices, policies, and procedures along these lines. The key issue then will be to leverage the solid work being done in some Components in implementing business standard processes and broadening and standardizing those implementations across the Department to support shared solutions and infrastructure.

4.2 Evolving the Business Model

Much of government IT exists in stove-piped silos —meaning that applications are funded, developed, and operated in a manner independent from other IT activity. This is true as well within the DOJ environment. Fundamental to successful implementation of this ITSP is breaking down these silos with a focus on enterprise solutions; interoperability across those solutions; and consolidated, optimized, and, when appropriate, centralized common services. To change this behavior, DOJ needs to fundamentally change its business model.

The business model includes how to establish and track service levels; how to determine the optimal cost structure to support effective delivery of shared solutions and infrastructure, both in cases where funding is provided up front and metered with the delivery of the service; how to establish prospective cost and service expectations that are mutually agreed to by the provider and the consumer of the service; how to manage deviations from expected service levels; how to establish appropriate and manageable terms and conditions that accompany the service; and how to bill, collect, and report on the service.

Currently the Department leverages the Working Capital Fund (WCF) to bill Components for shared services and infrastructure. Progress has been made to bring the cost and billing structure for shared services more in accord with actual direct costs for specific services. However, there are still charges that are not explicitly linked to services and service levels delivered. JMD must do a better job of exposing the specific purpose of charges, how the cost is allocated to individual Components and the basis of that allocation, and the benefits that the Components receive for the cost billed.

With infrastructure shared services in particular, OMB, through the ITI Line of Business, is moving rapidly toward a metrics driven approach to driving consolidation, standardization, and optimization. Specifically, OMB is establishing government-wide benchmark metrics and measures for service levels and cost across infrastructure functions such as networks, IT operations, end-user computing, and data centers. OMB plans to utilize their independently established metrics to evaluate effectiveness and consistency of existing infrastructure costs across the Federal Government. Agencies will be given the opportunity to justify their decisions. If they are unable to do so, OMB will then use its authority to force movement to more cost-effective, improved service alternatives. It is incumbent on DOJ to get out in front of this effort by adopting OMB's approach and implementing it within the Infrastructure Segment Architecture target model.

The target business model will more closely align internal cost and billing models to actual direct costs. Furthermore, it will provide meaningful guidance to allow Components to realize cost savings as they are realized and reinvest in Component mission support as appropriate to the accelerated implementation of the ITSP. Finally, the target business will include processes and measures for evaluating services against agreed-to service levels and for providing greater transparency on billing that directly ties charges to services received.

4.3 Stronger Cross-Organization Coordination, Governance and Policy Support

Currently, IT is organized across the Department as relatively independent Component-based entities. Among the Components, JMD has a significant emphasis on delivery and operation of DOJ-wide Enterprise Solutions and infrastructure, although there are notable pockets of shared activity elsewhere including Terrorist Explosive Device Analytical Center (TEDAC) with Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) and Federal Bureau of Investigation (FBI) and the Organized Crime Drug Enforcement Task Force (OCDETF) with the Drug Enforcement Administration (DEA). However, as the Department moves toward increasing the development and use of shared solutions, information and infrastructure, it is critical to assign clear responsibility for operating and delivering these shared capabilities.

In some cases such as Records Management, and Security and Privacy there are already naturally aligned entities (DOJ Records Management Office and Records Council; DOJ OCIO ITSS) that currently have policy and oversight responsibility Department-wide, and where the overall cross-Component model works well and can be further extended.

Governance concerns for cross-Department solutions include those to manage and oversee product management, as well as joint issue resolution. Product management is forward looking and includes the processes for ensuring stakeholder input and buy-in for solution requirements and implementation approaches. Issue resolution includes both operational issues as well as forward-looking concerns that cannot be addressed via conventional product management activities and need to be escalated through standard and repeatable processes. Currently the model is program specific —for example the governance structure for the LCMS is across the U.S. Attorneys and the DOJ Litigating Divisions. It is likely that governance structures will need to be put in place for the management and evolution of shared assets, with membership including appropriate personnel from each Component with mission equities in that segment. The LCMS governance model example is precisely the sort of structure that could be expanded.

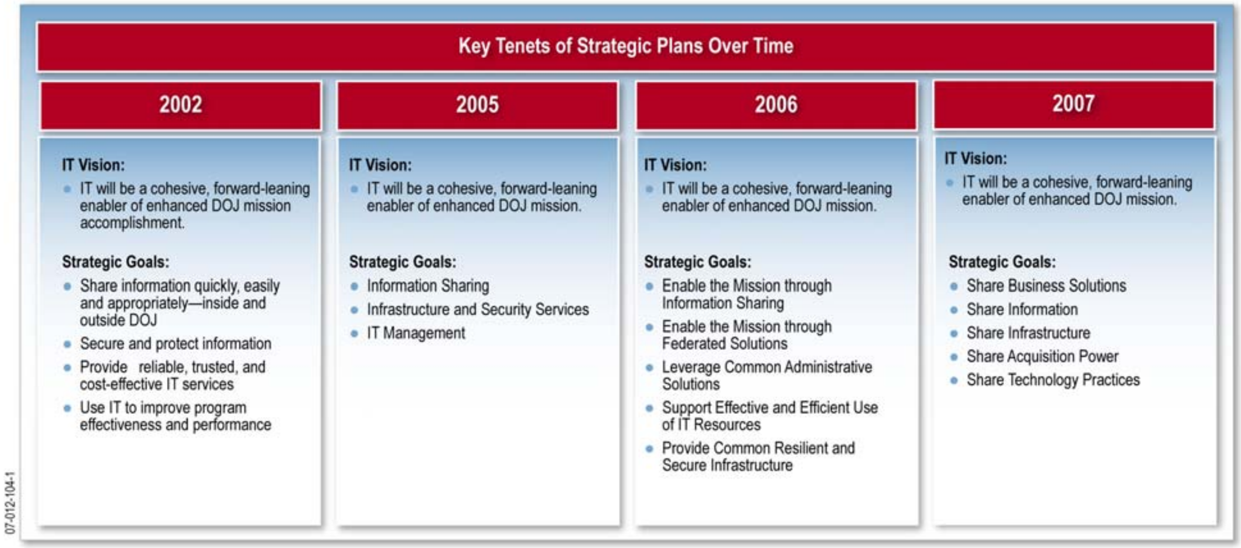
The CIO Council and the Department Architecture Advisory Board (DAAB) can provide the necessary forums for establishing shared standards, overall management, and oversight processes and provide guidance and resolution for exception cases.

Finally, looking across all of the dimensions it is clear that there is a need to formulate DOJ-wide policy and to validate and align these policies with non-IT stakeholders, including budget and finance, general council, senior Department leadership, and with issues across the Components. Indeed, the stakeholders in the vetting process will need to include OMB and the pertinent Congressional Committees and Appropriators. Policy needs to cover the DOJ-wide implementation, participation and business model.

5. CONCLUSION

The mission of DOJ, and much of the direct IT support for it, resides in the Components. Inherent in the federated structure of the Department is a division of responsibilities and scope of actions both across the Department and in each Component. The call for action is for IT to drive higher levels of mission performance within flat or shrinking budgets. In an environment of tightening IT budgets, it is imperative that we take a hard look at how to better use these limited dollars. This requires us to take a more coordinated approach to sharing business solutions, sharing information, making better use of our existing IT infrastructure, leveraging Department-wide purchasing power, and making our IT organization more effective. It has become increasingly important to get better value from the Department's enterprise solutions by leveraging them to solve similar business problems across the department. Only by making better use of our IT dollars through enterprise solutions, will we be able to continue to serve our business users and our citizens effectively.

APPENDIX A — EVOLUTION OF IT STRATEGIC PLANS



Key Tenets of Strategic Plans Over Time

2002	2005	2006	2007
IT Vision: • IT will be a cohesive, forward-leaning enabler of enhanced DOJ mission accomplishment.	**IT Vision:** • IT will be a cohesive, forward-leaning enabler of enhanced DOJ mission.	**IT Vision:** • IT will be a cohesive, forward-leaning enabler of enhanced DOJ mission.	**IT Vision:** • IT will be a cohesive, forward-leaning enabler of enhanced DOJ mission.
Strategic Goals: • Share information quickly, easily and appropriately—inside and outside DOJ • Secure and protect information • Provide reliable, trusted, and cost-effective IT services • Use IT to improve program effectiveness and performance	**Strategic Goals:** • Information Sharing • Infrastructure and Security Services • IT Management	**Strategic Goals:** • Enable the Mission through Information Sharing • Enable the Mission through Federated Solutions • Leverage Common Administrative Solutions • Support Effective and Efficient Use of IT Resources • Provide Common Resilient and Secure Infrastructure	**Strategic Goals:** • Share Business Solutions • Share Information • Share Infrastructure • Share Acquisition Power • Share Technology Practices

07-012-104-1

Figure 13: Evolution of IT Strategic Plans

APPENDIX B—CROSS-WALK OF STRATEGY WITH ENTERPRISE ARCHITECTURE

References to implementation planning for strategies are outlined in the following sections of the DOJ Enterprise Architecture documentation.

Table 5: Cross-Walk of Strategy with Enterprise Architecture

Strategy	Enterprise Architecture Document	Document Section
Share Information	Information Sharing Segment Architecture	Entire Document: 3 Volumes - Executive View, Program View and Architecture View
	As-Is & To-Be Enterprise Architecture	**Section 4.2—**Data Sharing (As-Is) **Section 4.3—**Data Sharing (To-Be) Section 5.2.2-As Is ISSA Section 5.3.2-To be ISSA Section 7.4.3-ISSA
	DOJ Transition Strategy & Sequencing Plan	**Section 15—**Information Sharing Segment Architecture **Section 19.3—**NIEM Adoption Results
	Enterprise Architecture Framework and Methodology	**Section 2.2.4—**Information Sharing
	Program Managers User Guide	**Section 3.2—**IT Strategic Plan and Strategic Focus Areas Section 4.1 – Information Sharing
Share Business Solutions	Justice Information Service Segment Architecture	Entire Document
	Litigation and Judicial Activities Segment Architecture	Entire Document
	As-Is & To-Be Enterprise Architecture	**Section 2.2.2—Business** Enterprise Solutions **Section 5.2.1—As Is** Enterprise Solutions Architecture **Section 5.3.1—To Be** Enterprise Solutions Architecture
	DOJ Transition Strategy & Sequencing Plan	**Section 5—**Intelligence Operations Section 6 – Investigations and Law Enforcement **Section 7—**Litigation and Judicial Activities **Section 8—**Correctional Activities **Section 9—**Justice Information Services **Section 10—**Justice Program Coordination **Section 13—**Financial Management
	Enterprise Architecture Framework and Methodology	**Section 2.2.3—**Enterprise Solutions
	Program Managers User Guide	**Section 3.2—**IT Strategic Plan and Strategic Focus Areas Section 4.3 – Enterprise Solutions
Share Infrastructure	As-Is & To-Be Enterprise Architecture	**5.2.4.2—**Shared Infrastructure Services **Section 6.3.1.3—**Consolidation, Standardization and Optimization
	DOJ Transition Strategy & Sequencing Plan	**Section 11 – IT Infrastructure Operations & Management** **Section 12 – IT Infrastructure Shared Services** **Section 20.3—**Infrastructure Consolidation, Standardization and Optimization **Section 20.26—**IT Infrastructure Optimization
	Enterprise Architecture Framework and Methodology	**Section 2.2.5—**Infrastructure Shared Services
	Program Managers User Guide	**Section 3.2—**IT Strategic Plan and Strategic Focus Areas
Share Acquisition Power	TBD	TBD

APPENDIX C—LINE OF BUSINESS DEFINITIONS

The highest level of the Value Chain contains the Department of Justice (DOJ) lines of business (LoBs). These LoBs encompass all of the Business activities that occur across the entire Department. The Enterprise Architecture Program Management Office (EAPMO) uses the Value Chain to establish a high-level representation of the DOJ enterprise. When reviewing the business architectures of DOJ's Components certain activities were obvious candidates for LoBs, to include Investigations and Law Enforcement, Intelligence Operations, Litigation & Judicial Activities, and Correctional Activities. These are the core outcome activities of the Department that are most visible to the public. In addition to these core mission organizations, the Department has two LoBs categorized as Justice Outreach/Support and Support Functions. Descriptions of the LoBs are listed below:

Intelligence Operations—Intelligence Operations involves collecting and analyzing information to meet the national security challenges of the United States by processing reliable, accurate foreign intelligence and disseminating intelligence products to policymakers, military commanders, law enforcement entities, and other consumers.

Investigations and Law Enforcement—The activities to protect U.S. national interests, people, places, and things from criminal activity resulting from non-compliance with U.S. laws. This includes deterrence, patrols, undercover operations, response to emergency calls, as well as arrests, raids, and seizures of property.

Litigation and Judicial Activities—Litigation and Judicial Activities refers to those activities relating to the administration of justice.

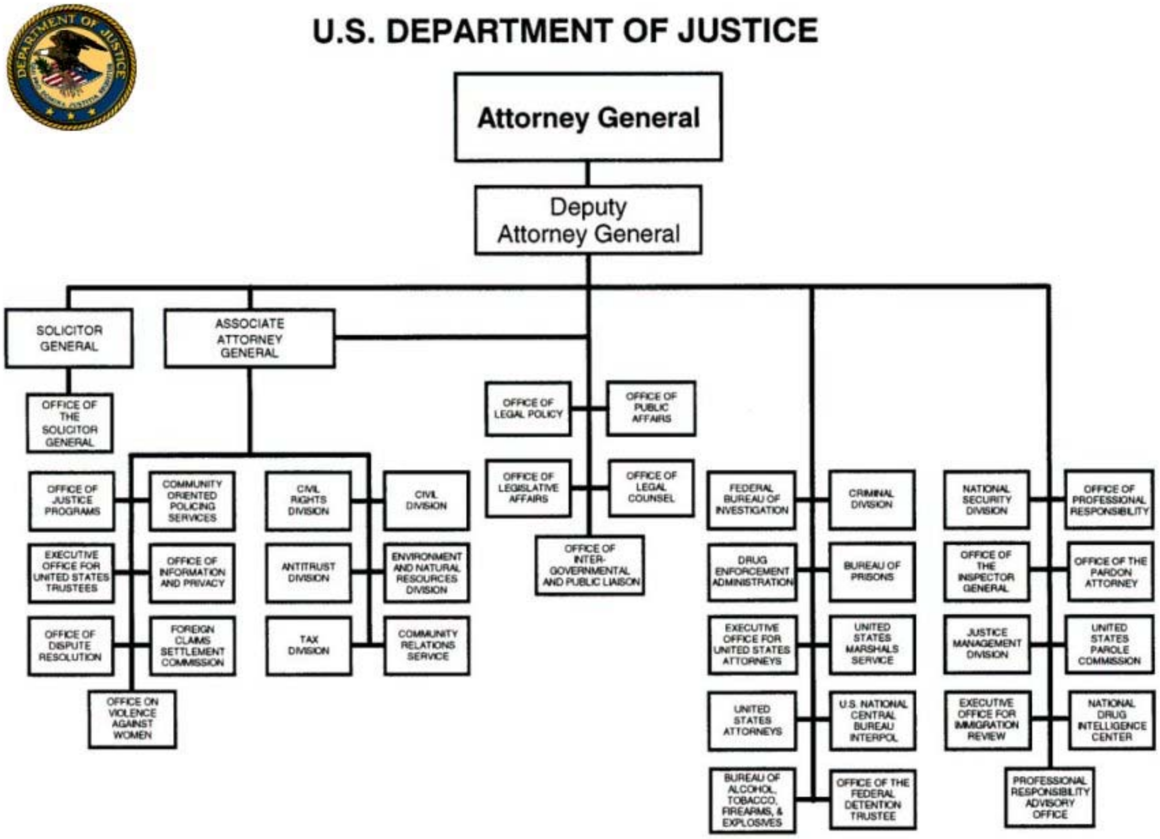
Correctional Activities—Correctional Activities involves all Federal activities that ensure the effective incarceration and rehabilitation of convicted criminals.

Justice Outreach and Support—Justice Outreach and Support involves providing leadership and criminal justice services to Federal, State, municipal, and international agencies and partners to enable national security, law enforcement, litigation, judicial, correctional and intelligence activities.

Support Functions—Those support functions that are cross-cutting across the agency in support of the core mission activities.

Along with all the other layers of the DOJ Enterprise Architecture, the complete business architecture information is maintained in a centralized repository established by the EAPMO. This repository was established through a mass data collection, conversion, and consolidation effort consisting of all documents that pertained to As-Is DOJ Enterprise Architecture. As the enterprise architecture is developed and matures, this information is constantly updated within the repository. This information is accessible through enterprise architecture reports generated by the EAPMO.

APPENDIX D—ORGANIZATIONAL CHART AND COMPONENT LISTING


U.S. DEPARTMENT OF JUSTICE
Attorney General
Deputy Attorney General
SOLICITOR GENERAL
ASSOCIATE ATTORNEY GENERAL
OFFICE OF THE SOLICITOR GENERAL
OFFICE OF LEGAL POLICY
OFFICE OF PUBLIC AFFAIRS
OFFICE OF LEGISLATIVE AFFAIRS
OFFICE OF LEGAL COUNSEL
OFFICE OF INTER-GOVERNMENTAL AND PUBLIC LIAISON
OFFICE OF JUSTICE PROGRAMS
COMMUNITY ORIENTED POLICING SERVICES
CIVIL RIGHTS DIVISION
CIVIL DIVISION
EXECUTIVE OFFICE FOR UNITED STATES TRUSTEES
OFFICE OF INFORMATION AND PRIVACY
ANTITRUST DIVISION
ENVIRONMENT AND NATURAL RESOURCES DIVISION
OFFICE OF DISPUTE RESOLUTION
FOREIGN CLAIMS SETTLEMENT COMMISSION
TAX DIVISION
COMMUNITY RELATIONS SERVICE
OFFICE ON VIOLENCE AGAINST WOMEN
FEDERAL BUREAU OF INVESTIGATION
CRIMINAL DIVISION
DRUG ENFORCEMENT ADMINISTRATION
BUREAU OF PRISONS
EXECUTIVE OFFICE FOR UNITED STATES ATTORNEYS
UNITED STATES MARSHALS SERVICE
UNITED STATES ATTORNEYS
U.S. NATIONAL CENTRAL BUREAU INTERPOL
BUREAU OF ALCOHOL, TOBACCO, FIREARMS, & EXPLOSIVES
OFFICE OF THE FEDERAL DETENTION TRUSTEE
NATIONAL SECURITY DIVISION
OFFICE OF PROFESSIONAL RESPONSIBILITY
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF THE PARDON ATTORNEY
JUSTICE MANAGEMENT DIVISION
UNITED STATES PAROLE COMMISSION
EXECUTIVE OFFICE FOR IMMIGRATION REVIEW
NATIONAL DRUG INTELLIGENCE CENTER
PROFESSIONAL RESPONSIBILITY ADVISORY OFFICE

Approved by: ________________ Date: 3-13-04

ALBERTO R. GONZALES
Attorney General

DOJ Components include the following:

- Office of the Solicitor General (OSG)
- Office of the Inspector General (OIG)
- Office of Legal Counsel (OLC)
- Office of Legal Policy (OLP)
- Office of Intelligence Policy and Review (OIPR)
- Office of Professional Responsibility (OPR)
- Office of Legislative Affairs (OLA)
- Office of Intergovernmental and Public Liaison (OIPL)
- Office of Information and Privacy (OIP)
- Office of Public Affairs (PAO)
- Office of Dispute Resolution (ODR)
- Justice Management Division (JMD)
- Executive Office for United States Attorneys (EOUSA)
- Antitrust Division (ATR)
- Civil Division (CIV)
- Civil Rights Division (CRT)
- Criminal Division (CRM)
- Environment and Natural Resources Division (ENRD)
- National Security Division (NSD)
- Tax Division (TAX)
- Federal Bureau of Prisons (BOP)
- Federal Prison Industries
- National Institute of Corrections
- Drug Enforcement Administration (DEA)
- Federal Bureau of Investigation (FBI)
- Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)
- United States Marshals Service (USMS)
- INTERPOL - United States National Central Bureau (USNCB)
- Executive Office for Immigration Review (EOIR)
- Office of the Pardon Attorney (OPA)
- United States Parole Commission (USPC)

- Executive Office for United States Trustees (EOUST)
- Community Relations Service (CRS)
- Foreign Claims Settlement Commission (FCSC)
- Office of Justice Programs (OJP)
- Office of Community Oriented Policing Services (COPS)
- National Drug Intelligence Center (NDIC)
- Professional Responsibility Advisory Office (PRAO)
- Office of the Federal Detention Trustee (ODT)
- Office on Violence Against Women (OVW)

APPENDIX E—ACRONYM LIST

Acronym	Definition
APB	Advisory Policy Board
ATF	Bureau of Alcohol, Tobacco, Firearms, and Explosives
BPA	Blanket Purchase Agreement
BPWG	Business Process Working Group
CDCS	Consolidated Debt Collection System
CIS	Center for Internet Security
CJIS	Criminal Justice Information Services
COI	Communities of Interest
COOP	Continuity of Operations
CPIC	Capital Planning and Investment Control
CPO	Chief Privacy Officer
CTISS	Counter Terrorism Information Sharing Standards
DARB	Department Architecture Review Board
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DIRB	Department Investment Review Board
DNI	Director of National Intelligence
DOJ (or Justice Department or Department)	Department of Justice
e-Gov	E-Government
EAPMO	Enterprise Architecture Program Management Office
EAWG	Enterprise Architecture Working Group
ELA	Enterprise Licensing Agreement
EOUSA	Executive Office for United States Attorneys
FIDM	Federated Identity Management
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act

Acronym	Definition
FTF	Federal Transition Framework
GAC	Global Advisory Committee
GAO	General Accounting Office
GESC	Global Executive Steering Committee
Global	Global Justice Information Sharing Initiative
HSPD-12	Homeland Security Presidential Directive 12
IDEA	Intra-DOJ Information Exchange
IEPD	Information Exchange Package Documentation
IPV6	Internet Protocol Version 6
IRTPA	Intelligence Reform and Terrorism Prevention Act
ISE	Information Sharing Environment
ISSA	DOJ Information Sharing Segment Architecture
IT	Information Technology
ITI LoB	IT Infrastructure Line of Business
ITSP	Information Technology Strategic Plan
JABS	Joint Automated Booking System
JCON	Justice Consolidated Office Network
JMD	Justice Management Division
JRA	Justice Reference Architecture
JSOC	Justice Security Operations Center
JSRA	Justice Secure Remote Access
JUTNET	Justice Uniform Network
LCMS	Litigation Case Management System
LEISP	Law Enforcement Information Sharing Program
LEO	Law Enforcement On-Line
LEXS	Law Enforcement Exchange Standard
LoBs	Lines of Business
MOU	Memorandum of Understanding

Acronym	Definition
N-DEx	National Data Exchange System
NBAC	NIEM Business Architecture Committee
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
NPEP	NIEM Priority Exchange Panel
NTAC	NIEM Technical Architecture Committee
O&M	Operations and Maintenance
OCDETF	Organized Crime Drug Enforcement Task Force
OCIO	Office of the Chief Information Officer
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
PDA	Personal Data [or Digital] Assistant
PIA	Privacy Impact Assessment
PII	personal identifiable information
OneDOJ	Regional Data Exchange System
SAR	Suspicious Activity Reporting
SCAP	Security Content Automation Protocol
SIWG	Standard Infrastructure Working Group
SLA	Service Level Agreement
SLT	State, Local, and Tribal
SRM	Service Reference Model
TEDAC	Terrorist Explosive Device Analytical Center
TRM	Technology Reference Model
UFMS	Unified Financial Management System
VA	Department of Veterans Affairs
WCF	Working Capital Fund
WG	Working Group