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.

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).

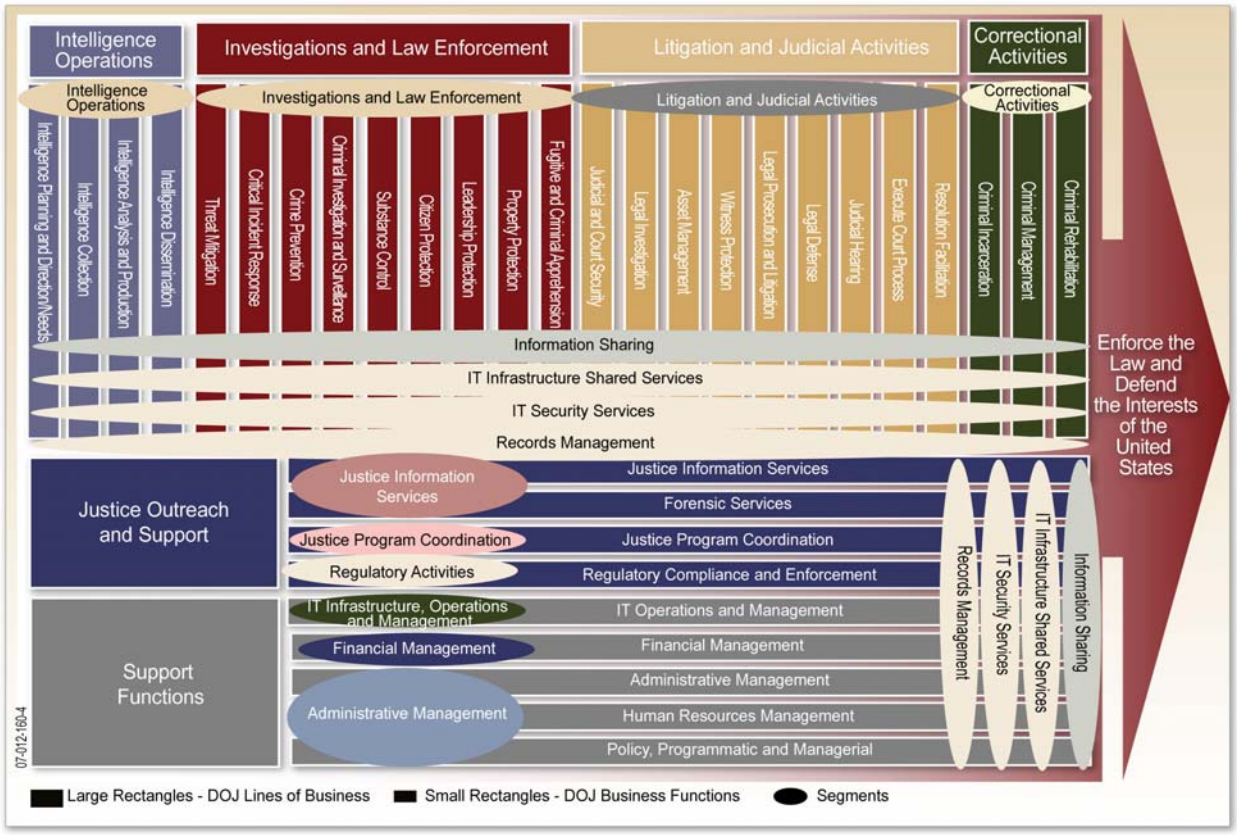

Figure 6: Segments in Context of the DOJ Value Chain

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	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
		DOJ IT Objectives					DOJ Strategic Objectives		
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.

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.

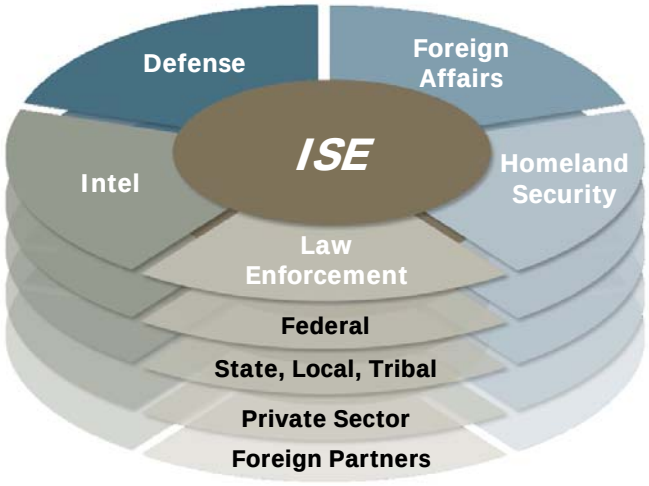

Figure 9: Extended Justice Enterprise

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

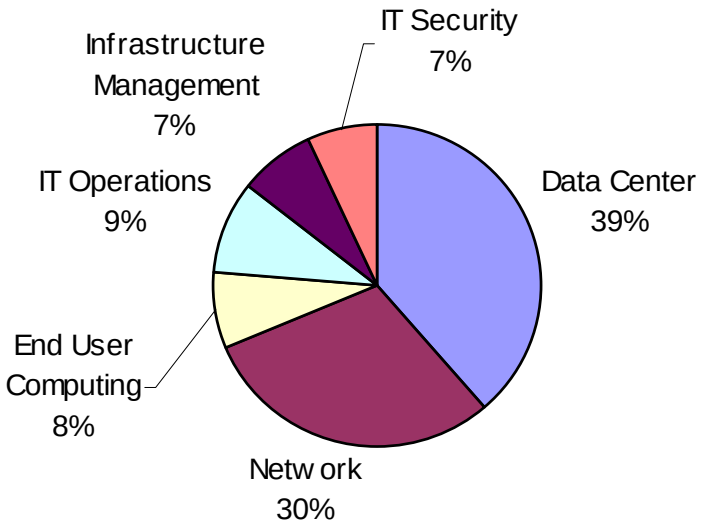

Figure 10: DOJ IT Infrastructure Operations & Management (FY2007)

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.

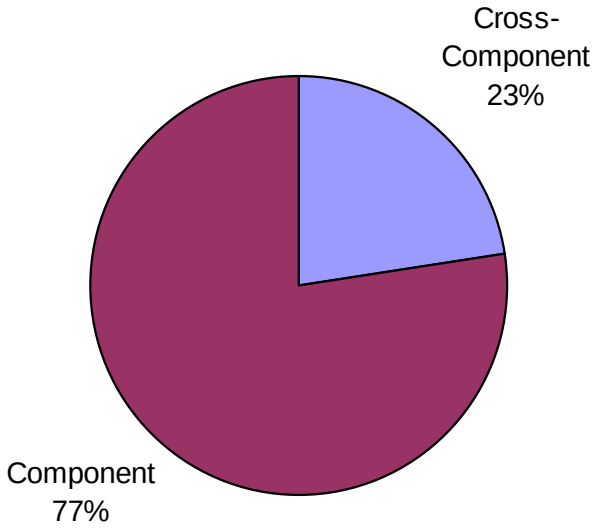

Figure 11: IT Operations and Management Investment—FY2007 Cross-Component Spend

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.