3. STRATEGIES

The challenges outlined in the previous section will require the DOJ OCIO and Component CIOs to work together to share solutions that work, collaboratively build IT that meets common requirements, and make the best use of limited money and talent.

To achieve these goals, the Department has established five key IT strategies, each with primary objectives for implementation. Table 3-1 outlines these strategies:

Strategies	Objectives
Share Business Solutions *"Make Our Customers More Effective"*	• Deliver enterprise solutions
	• Align IT governance to mission needs
Share Information *"Make Us More Knowledgeable"*	• Share information across the Extended Justice Enterprise
	• Develop and implement required information sharing, data security, and privacy policies
	• Develop information sharing architectural standards
Share Infrastructure *"Make Our IT Investments Work Harder"*	• Improve the DOJ infrastructure customer experience
	• Increase the resiliency and quality of our infrastructure
	• Consolidate, standardize, and optimize infrastructure
Strengthen IT Security *"Keep Our Information Secure"*	• Institutionalize information assurance, security, privacy and accessibility
	• Integrate identity, credential and access management programs
	• Assure a trusted and resilient information and communications infrastructure
	• Acquire IT products, solutions and services with a known level of assurance and accessibility
Strengthen IT Management *"Make the IT Organization More Effective"*	• Share acquisition power
	• Increase collaboration among IT staff
	• Attract and retain a skilled workforce
	• Improve process discipline

Table 3-1: DOJ Key IT Strategies and Objectives

3.1. SHARE BUSINESS SOLUTIONS

The highest level lines of business (LoBs) that DOJ performs as an organization are shown in Figure 3-1. Each of the LoBs comprises multiple business functions, which represent the major business activities of the Department. The DOJ Value Chain generally shows how the Department's Mission-related LoBs (in color in Figure 3-1) are being executed and supported by the Management and Support LoBs (in grey in Figure 3-1).

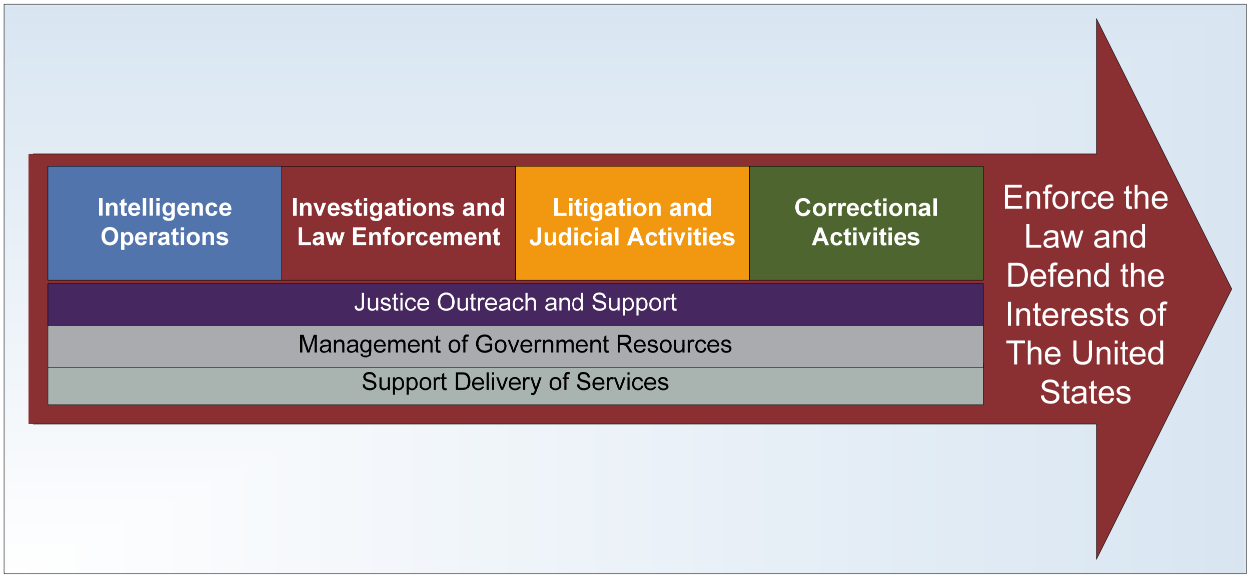
Intelligence Operations
Investigations and Law Enforcement
Litigation and Judicial Activities
Correctional Activities
Justice Outreach and Support
Management of Government Resources
Support Delivery of Services
Enforce the Law and Defend the Interests of The United States

Figure 3-1: 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 Information technology investments. IT investments need a clear line of sight to demonstrate how they support the mission and create a return on the IT investment by improving operational effectiveness. Sharing business solutions across these LoBs helps focus IT resources effectively, makes our customers more effective, and enables the Department to achieve DOJ's mission priorities.

3.1.1. Deliver Enterprise Solutions

Enterprise Solutions are DOJ programs that provide common solutions to address 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 IT investments, increase information sharing, and make use of shared infrastructure services.

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

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

Moving toward 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 continue to implement key mission initiatives and continues to promote Enterprise Solutions. Such initiatives include Litigation Case Management System (LCMS), Justice Consolidated Office Network (JCON), Consolidated Debt Collection System (CDCS), Justice Secure Remote Access (JSRA), Joint Automated Booking System (JABS), and FBI's Next Generation Identification (NGI).

DOJ uses a Segment Architecture approach 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 roadmap for a specific core mission area, business service, or enterprise (cross-cutting) service. From an IT 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.

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 IT investments delivers on a common mission, purpose, or cross-cutting service provided by the segment. The DOJ Segments, the participating Components, and the representative Enterprise Solution are outlined in Table 3-2 DOJ Segments, Major Components, and Representative Solutions. Enterprise Solutions discussed in this section are focused on core mission and business activities within the Core Mission Segments (see Appendix C for detailed description of IT strategies, solutions, and 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.

DOJ Segment	DOJ Segment Type	Components	Representative Solutions
Intelligence Operations	Core Mission	FBI, DEA, ATF, USMS	• DEA Speedway • FBI Data Integration and Visualization System • FBI Terrorist Screening System (TSS) • FBI Digital Collection • FBI Investigative Data Warehouse
Investigation and Law Enforcement	Core Mission	FBI, DEA, JMD	• JMD Law Enforcement Wireless Communication (LEWC) • FBI SENTINEL • JMD Joint Automated Booking System (JABS) • DEA EPIC Seizure System (ESS)
Litigation and Judicial Activities	Core Mission	US Attorneys, Litigating Divisions, EOIR	• EOIR eWorld • JMD Consolidated Asset Tracking System (CATS) • JMD Litigation Case Management System (LCMS)
Correctional Activities	Core Mission	Bureau of Prisons	• BOP Inmate Telephone System (TRUFONE) • BOP SENTRY
Justice Information Services	Outreach	FBI, ATF, DEA	• ATF NIBIN • FBI Combined DNA Index System (CODIS) • FBI National Crime Information Center (NCIC) • FBI National Instant Criminal Background Check System (NICS) • OCDETF Fusion Center System
Justice Program Coordination	Outreach	Office of Justice Programs	• COPS Management System (CMS) • OJP Community Partnership Grants Management System (CPGMS)
Administrative Management	Support	JMD	• BOP HRM Automation - E-Clearance • DEA IT Quality Management • FBI Compass • FBI Enterprise Workflow System • JMD AEGIS
Financial Management	Support	JMD/CFO	• Unified Financial Management System (UFMS) • JMD Financial Management Information System (FMIS) • DEA Financial Management Program (FMP)
Information Sharing	Enterprise	FBI, JMD	• FBI Law Enforcement National Data Exchange • JMD LEISP Program Management
IT Infrastructure	Enterprise	All Components and JMD	• FBI Network Services • DEA Firebird • FBI Criminal Justice Information Services Division Wide Area Network (CJIS WAN) • JUTNET

Table 3-2: DOJ Segments, Major Components, and Representative Solutions

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. This analysis will identify the status and strategic alignment of each solution contained within a segment. As depicted in Figure 3-2: 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.

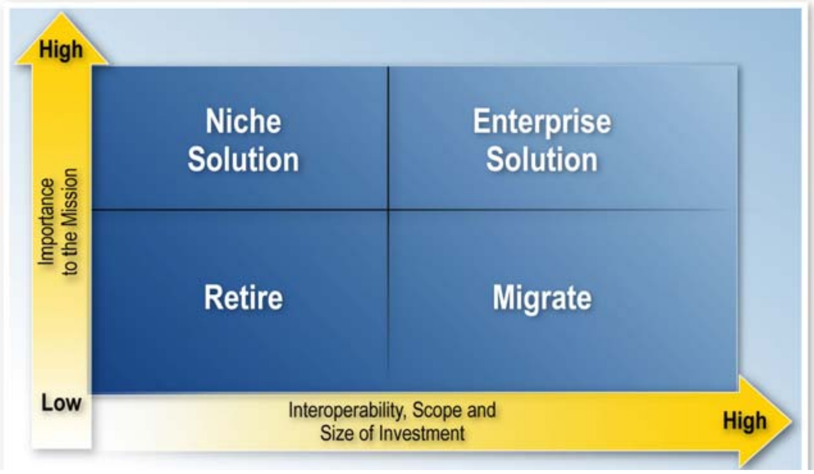
High
Importance to the Mission
Low
Niche Solution
Enterprise Solution
Retire
Migrate
Interoperability, Scope and Size of Investment
High

Figure 3-2: Program Evaluation Matrix

3.1.2. Align IT Governance to Mission Needs

To ensure IT investments are aligned with the strategic vision outlined in this plan, the Department continues to refine its IT governance processes as outlined in the DOJ IT Governance Guide. The emphasis is on refinement and better integration of the Department-level IT governance processes with the processes of the 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 of IT investments. This shared value helps inform governance and funding decisions to create a portfolio of IT 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 —** Defines the IT vision for DOJ, and describes the broad IT strategic goals and objectives that serve as the basis for the Department's enterprise architecture (EA) and IT investment planning.
- **Enterprise Architecture Transition Planning —** Describes architecture of in-progress initiatives, and lays out future and transitional states of the enterprise architecture to meet the long term vision described as a result of IT Strategic Planning.
- **IT Investment Planning (also called IT Portfolio Management) —** Identification and prioritization of the IT investments required to support the strategies outlined in the ITSP.
- **IT Budget Planning —** Process by which Components and the Department select and allocate budgetary resources to fund IT investments within the funding constraints and mission and program priorities dictated by the Department, the Administration, and the Congress. The IT Budget planning process runs for approximately 18 months, culminating with enactment and appropriation of program funding by the Congress.

- **IT Investment Oversight —** Lifecycle reviews through program/project self assessment, Component assessment and Department assessments, when appropriate, via the Department IT Investment Review Board (DIRB) and CIO Dashboard to monitor IT investment progress and adjust program/project plans, when necessary.
- **Performance Management —** Establishing performance metrics and tracking achievement of those metrics to accomplish the Department's varied mission.
- **Security and Privacy Oversight —** Evaluating the implementation and execution of security and privacy policies within a context of risk management. See also section 3.2.2 for more on Security compliance and Privacy.

The governance structure addresses the build-out of the Department's IT governance lifecycle with the integration of the Enterprise Architecture planning processes 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

Terrorist attacks, natural disasters, and large-scale 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 the following sections.

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 three primary drivers for DOJ information sharing are President Barack Obama's memorandum[5] to federal agencies, DOJ's Law Enforcement Information Sharing Program (LEISP) and the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004. President Obama has emphasized that "The global nature of the threats facing the United States requires that our Nation's entire network of defenders be able to rapidly share information so that those who must act have the information they need." 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

[5] The memorandum, "Classified Information and Controlled Unclassified Information", was released on May 27, 2009. It is available at: http://www.whitehouse.gov/the_press_office/Presidential-Memorandum-Classified-Information-and-Controlled-Unclassified-Information

Environment (ISE) to facilitate the sharing of terrorism information across various functional domains, as shown in Figure 3-3.

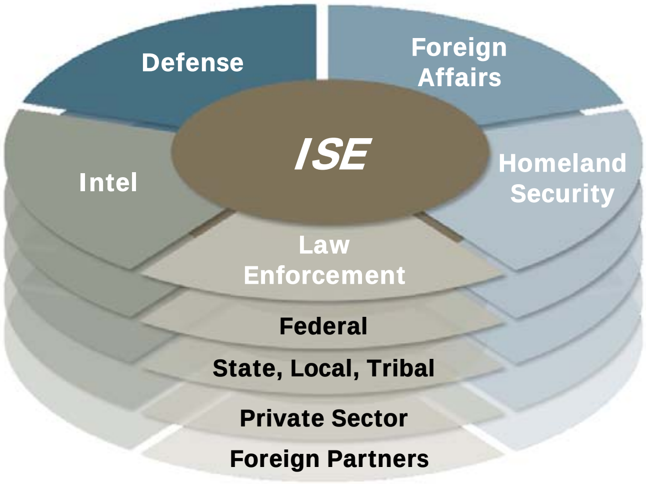

Figure 3-3: Information Sharing Environment (ISE)

3.2.1.1. OneDOJ and N-DEx Integration

LEISP is a program that was established to enable the collaboration and sharing of information across the law enforcement community. Oversight of LEISP is via the LEISP Coordinating Committee (LCC). OneDOJ (formerly the Regional Data Exchange or R-DEx) and the National Data Exchange (N-DEx) are the Department's first two programs implementing the LEISP strategy. As part of this strategy, the development of N-DEx and OneDOJ have been closely coordinated. The two systems will converge into a single system in 2011. This integration will provide law enforcement agencies with access to data from the ATF, BOP, DEA, FBI, and USMS and 20,000 local, state, federal, and tribal law enforcement agencies. N-DEx and OneDOJ currently offer two separately maintained systems for the law enforcement community. This will continue during integration efforts to provide uninterrupted information sharing among law enforcement agencies.

The purpose of transitioning of OneDOJ to N-DEx is to provide one seamless environment for law enforcement agencies to share information to combat crime and terrorism. Integration of the two systems will eliminate duplicative effort and promote reuse of infrastructure without degrading services provided by current systems. Figure 3-4 illustrates the data sources and law enforcement partners that will share information.

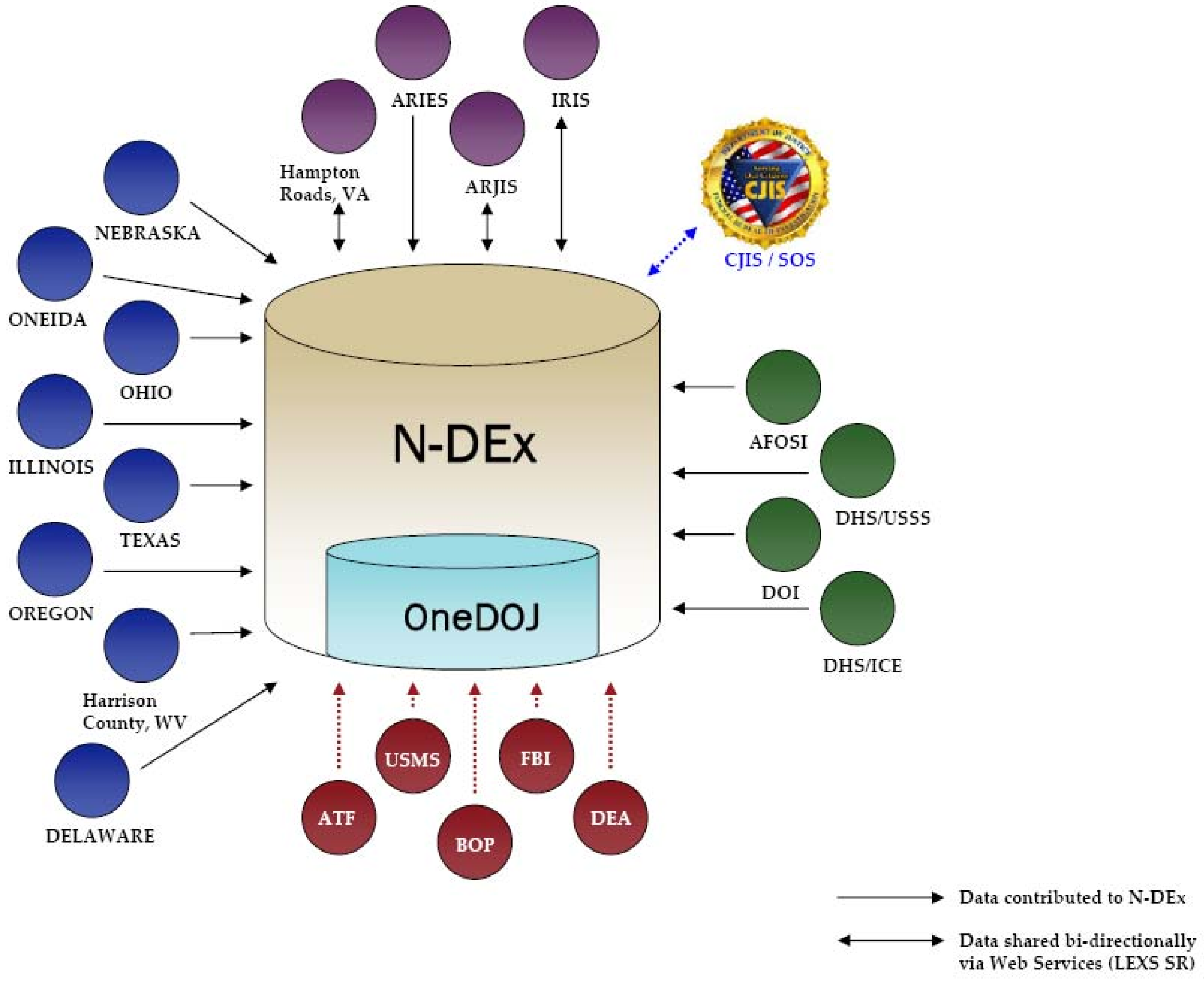

Figure 3-4: One DOJ and N-DEx Converged Capabilities

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, N-DEx, and other information sharing systems. The infrastructure uses the Logical Entity Exchange Specification (LEXS), which is based on the National Information Exchange Model (NIEM), to exchange information using a common XML-based approach. It 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.

3.2.1.2. Fusion Centers and Shared Spaces

By implementing the DOJ LEISP program and integrating internal activities with those of the PM-ISE, DOJ approaches information sharing from both an internal and external partner perspective. Specifically, a collaborative effort led by the DOJ and DHS, with participation from other Federal and SLT agencies, resulted in publication of the Baseline Capabilities for State and Major Urban Area Fusion Centers. Additionally, the DOJ's Bureau of Justice Assistance (BJA), PM-ISE, and SLT partners will continue the installation and activation of Shared

Spaces at fusion centers in Houston, Seattle, Los Angeles, and Las Vegas. Federal agencies will implement Shared Spaces, which are illustrated in Figure 3-5, as part of the ISE-SAR Evaluation Environment (EE), which uses LEXS. Agencies will begin to implement other Shared Space solutions as well.

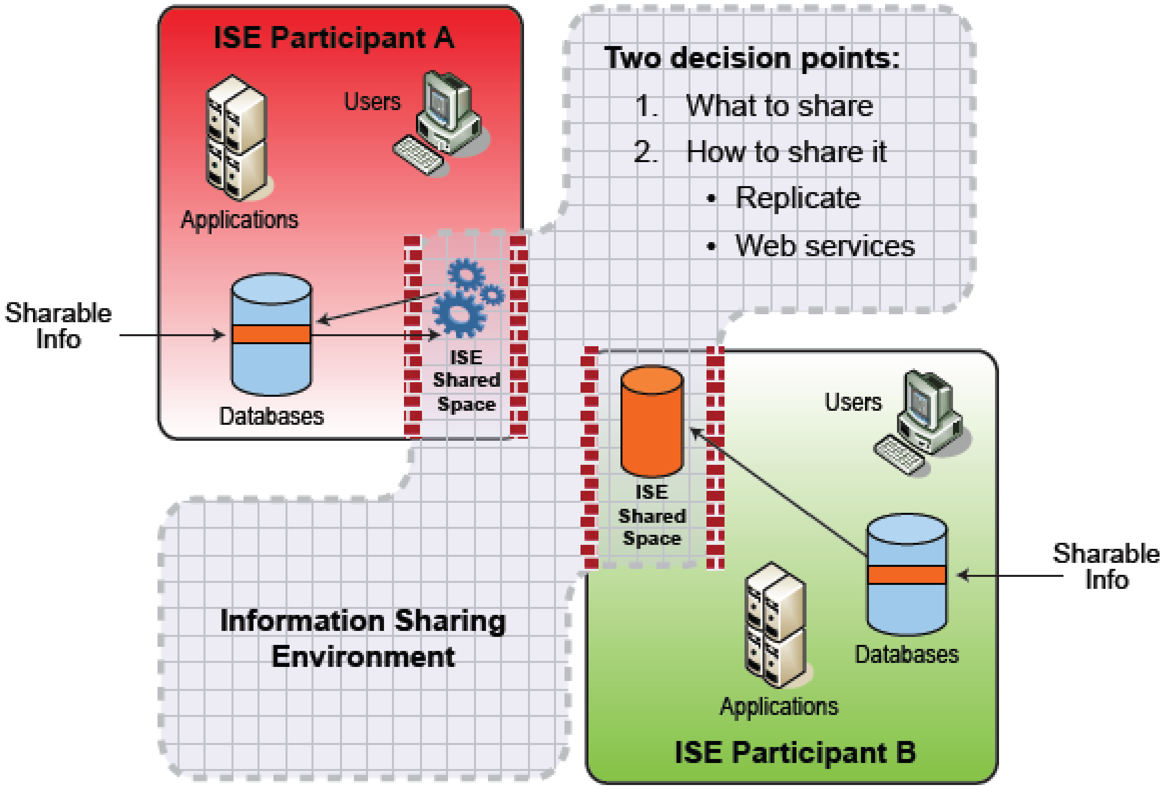

Figure 3-5: ISE Shared Spaces Concept

DOJ is successfully working to support the specialized needs of fusion centers. This includes access to our search applications for fusion center users and access to department data for specialized analytics. The goal of this effort is to share complete, accurate, timely & useful criminal justice information across jurisdictional boundaries and provide new investigative tools that enhance the Nations ability to fight crime and terrorism. Consequently, Fusion Centers are beginning to see increased access to new suspects entered into the system which allow them to compare against watch lists or notify/alert users of addresses that are known to be associated with other suspected terrorists.

3.2.1.3. Geospatial Services

DOJ recognizes the important contribution that geospatial information and technology plays in public safety, enforcing the law and strengthening our Nation's security posture. As such, the DOJ is developing a strategy for the creation, maintenance, and sharing of geospatial data to improve collaboration, to leverage existing resources, and to provide advanced geospatial capabilities for DOJ Components and for our external partners. DOJ's efforts continue to strengthen partnerships with other federal agencies in order to build enterprise geospatial services and establish opportunities for reuse.

The primary goal of this effort is to offer a common set of services that are able to provide geospatial data in a standard vendor-agnostic format. Additionally, the Department will also establish a governance process to evaluate emerging capabilities and to advocate for the inclusion of geospatial technology in policy, strategy, investments and processes. These geospatial systems will integrate and visualize data with any combination of imagery, maps and charts.

3.2.2. Develop and Implement Required Information Sharing, Data Security, and Privacy Policies

DOJ also has a responsibility to uphold the public trust in the information we collect, and the OCIO recognizes the dual concerns of security and privacy. Security includes confidentiality, availability, and integrity of data. Privacy deals with protection of individual privacy and sensitive data. As part of the overall information sharing approach, data security and privacy issues must be addressed in a proactive way to ensure that each party involved in sharing is assured that the data they provide and consume is reliable, is accurate, and is protected from unauthorized release. This entails a set of activities to reaffirm and extend the LCC, 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.

The discussion of privacy and security takes on renewed urgency amidst conspicuous instances of compromised data, such as stolen laptops containing personal information of over 26 million veterans. DOJ collects and stores a variety of personal information, from investigative case records to prisoner and personnel records, and we process and store Personally Identifiable Information (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.

3.2.2.1. Data Security

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

In June 2006, OMB issued Memorandum 06-16 in response to the theft of the US Department of Veterans Affairs 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 remote access solutions into compliance with departmental policies.

To further address the issue of data security, the department, in conjunction with the Office of the Director of National Intelligence (ODNI), National Institutes of Standards and Technology, and the Committee on National Security Systems, has made considerable progress in updating IT security policies and standards. This work continues to evolve in an effort to move towards a unified baseline of Federal systems as well as enable reciprocity with state, local, and tribal (SLT) governments and private partners. An example of this effort has included the DHS and FBI's adoption of a Reciprocal Physical Security Construction Standard that has created an environment where classified information may be stored, used discussed, or processed.

3.2.2.2. Data Privacy

Privacy policy issues need to be addressed in a formal way to ensure that sensitive data is protected. This requires reaffirming and extending protections for privacy of constituent data in accordance with policy and law. A key

Component of this is ensuring that the most appropriate technology solutions are brought to bear on this issue. Engineering support for privacy requirements, including the protection of PII, continues to be a requirement.

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 system upgrade, has on the privacy of the system's data. In a PIA, components must describe the basic use and purpose of the system, the information being collected, technical access and security protections being put in place, the degree to which data is shared, and how privacy risks are identified and mitigated. The PIA template is posted on the DOJ intranet for component use.

In addition, the Department has created an Initial Privacy Assessment (IPA) that must be completed for all new information systems or when any existing information system is being modified. The IPA process helps to ensure that legal and policy concerns are addressed in the IT development process. It allows the Office of Privacy and Civil Liberties to determine whether an information system requires any further privacy documentation, such as a PIA or System of Records Notice (SORN), or raises any privacy policy concerns.

Additionally, the DOJ has met with representatives of privacy and civil liberties advocacy groups to listen to their concerns and incorporate them into a revised Suspicious Activity Reporting (SAR) Functional Standard. This new standard incorporates stronger privacy protections into SAR data exchanges. In conjunction, a SAR Scenario was also developed to provide an accurate representation of how SARs are being shared today by state Law Enforcement Agencies (LEAs) and Federal Field Components such as a Federal Bureau of Investigation (FBI) Agent working on a Joint Terrorism Task Force (JTTF). In addition, it describes what actions the DOJ is taking to improve how it will share SARs in the future and interface with the ISE Shared Space.

3.2.3. Develop Information Sharing Architectural Standards

The Department's federated environment supports multiple networks and over 150 different systems that contain mission related information. The Department's architecture is guided by the following principles in order to share information effectively and efficiently within this environment:

1. The Department **supports both centralized and distributed models** for information sharing. DOJ Components can share information either by providing the data to a central repository, such as IDEA, or by implementing federated queries between systems.
2. The Department relies on **data standards to achieve interoperability** between existing systems that reside on disparate networks. Many of the exchanges leverage the LEXS IEPD and all exchanges incorporate the National Information Exchange Model (NIEM) model, discussed below. As a result, the Department can reuse information exchanges with multiple partners without recreating the exchange.
3. Enterprise information sharing **assets are distributed across multiple organizations**. DOJ relies on information sharing assets that are designed, developed and maintained by different DOJ components and reside on different networks.

3.2.3.1. Information Sharing Models

In order to foster an information sharing environment that is hospitable to multiple technologies, the Department encourages the use of multiple information exchange techniques and provides services and standards to meet the needs of the various approaches. As shown in Figure 3-6, the DOJ has published standards and provides services that support the following approaches to sharing information:

- **Application Access** allows authorized users to gain access to systems that contain information that is required to achieve their mission. This is one of the oldest information sharing techniques and has been implemented across the Department by creating user-accounts, co-locating resources, and installing remote terminals at external locations. In order to improve user access and facilitate single sign-on (SSO) capabilities, the Department has established Federated Identity Management (FIdM) to support the creation of trust relationships between information systems and networks.

- **Data Publication** allows information sharing partners to publish data in a single format that can be read by multiple systems. This approach is useful for the transfer of data across disconnected networks. DOJ has developed the LEXS-PD data exchange specification, which is used to describe the information, and the IDEA system, which can be used to automatically and securely distribute data over multiple networks and to multiple recipient systems.

- **Federated Query** allows a system to query data that is maintained and contained in separate systems. This approach is useful to connect partner systems and allow users to access a broad range of information without leaving the interface of their home organization. In addition, this technique supports information sharing without forcing organizations to maintain multiple instances of the same datasets. DOJ has developed the LEXS-SR data exchange specification, which supports sending and receiving queries between different search engines.

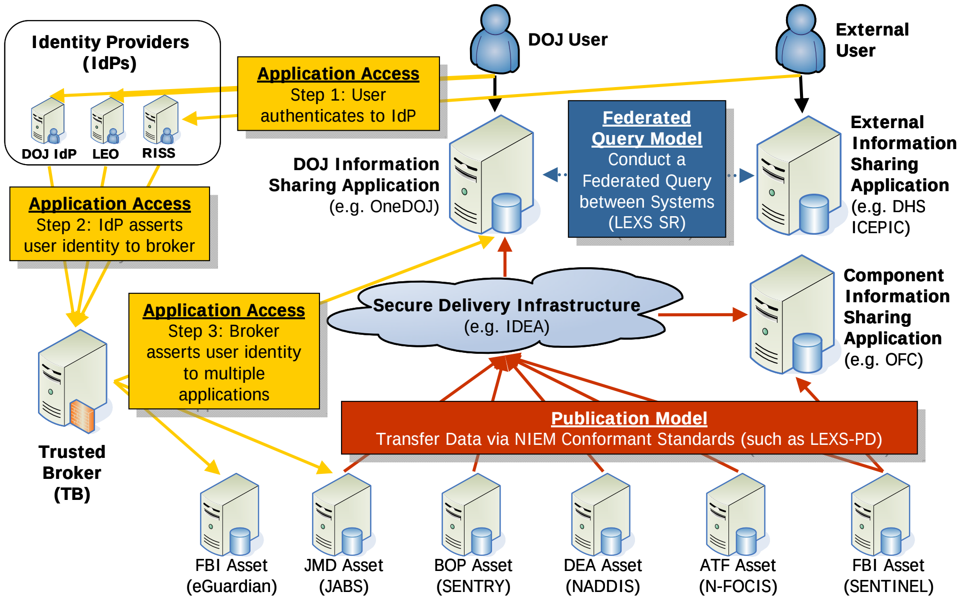
Identity Providers (IdPs)
DOJ IdP
LEO
RISS
Application Access
Step 1: User authenticates to IdP
DOJ User
External User
Application Access
Step 2: IdP asserts user identity to broker
DOJ Information Sharing Application (e.g. OneDOJ)
Federated Query Model
Conduct a Federated Query between Systems (LEXS SR)
External Information Sharing Application (e.g. DHS ICEPIC)
Application Access
Step 3: Broker asserts user identity to multiple applications
Secure Delivery Infrastructure (e.g. IDEA)
Component Information Sharing Application (e.g. OFC)
Trusted Broker (TB)
Publication Model
Transfer Data via NIEM Conformant Standards (such as LEXS-PD)
FBI Asset (eGuardian)
JMD Asset (JABS)
BOP Asset (SENTRY)
DEA Asset (NADDIS)
ATF Asset (N-FOCIS)
FBI Asset (SENTINEL)

Figure 3-6: Overview of DOJ Information Sharing Techniques

3.2.3.2. *NIEM Development and Support*

In support of information sharing, DOJ plays a leading role in maintaining the 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 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), and NIEM Outreach and Communication (NCOC). Other bodies that the NIEM program works closely with include the Global Executive Steering Committee (GESC), Global Advisory Council (GAC) and the CJIS Advisory Policy Board (APB) to achieve program goals.

Driven by IRTPA, the DOJ CIO is working in conjunction with the Information Sharing Interagency Policy Committee and participates in advisory groups that support this committee. Part of DOJ's involvement is to help create more NIEM-based exchange packages for use across the broader Justice and Counter Terrorism community. Specifically, DOJ led the development of the ISE Suspicious Activity Reporting (SAR) Functional Standard and the current operational study to implement it.

3.3. SHARE INFRASTRUCTURE

The Department employs an extensive IT infrastructure to support its diverse missions and organizational units. Over the years, DOJ's IT Infrastructure systems have been developed and deployed by various organizational units across the Department. Figure 3-7 illustrates the Department's highly diverse IT infrastructure.

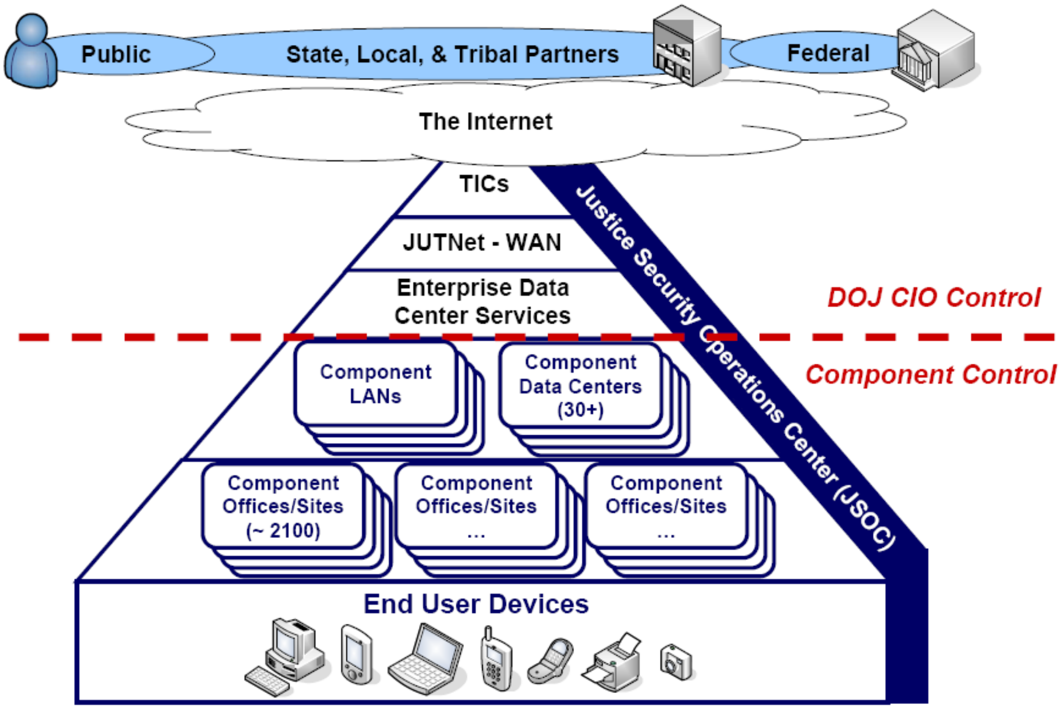
Public
State, Local, & Tribal Partners
Federal
The Internet
TICs
JUTNet - WAN
Enterprise Data Center Services
Justice Security Operations Center (JSOC)
DOJ CIO Control
Component Control
Component LANs
Component Data Centers (30+)
Component Offices/Sites (~ 2100)
Component Offices/Sites …
Component Offices/Sites …
End User Devices

Figure 3-7 DOJ IT Infrastructure

IT Infrastructure is an area of significant expenditure (see Figure 3-8) 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 over the years has highlighted the need for a consistent enterprise infrastructure approach suitable for all DOJ organizations and applications. Investments in centralized IT Infrastructure solutions can provide the required infrastructure services to DOJ Components ideally at lower cost, but standardization and consolidation will be necessary. IT programs can leverage new or existing infrastructure services that are provided by any DOJ Component, are provided centrally by DOJ OCIO, or are provided by a qualified third party, 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 and across the Government, DOJ can reduce overall IT infrastructure expenditures while providing consistent quality services to the mission Components. A good example of where this has been achieved is with JUTNET, the Department's OCIO-provided wide-area network service. JUTNET provides a common, safe, secure, centralized wide-area network managed service to over 80 percent of the Department. By utilizing JUTNET, the Department and its Components decrease the overall costs associated with the design and deployment of multiple networks, while ensuring safe and secure network transport and interoperability over a managed service.

In recent years the very definition of IT infrastructure has expanded as certain services have become more commoditized and are now available in a variety of ways that can be more cost and operationally effective than before. Services such as basic email, instant messaging, directory services, collaboration services, Blackberry support and other common utility services can be readily shared between components to meet DOJ strategic objectives.

Finally, expanding the scope of DOJ shared infrastructure services to include the operations of these systems provides the opportunity to not only capture value in leveraging our common purchasing and design/architecture work as we did with the original JCON program, but also to leverage our operations staffs, datacenter assets and other underlying technology infrastructures to everyone's benefit. Diminishing resources makes it difficult to find experienced people to operate our increasingly integrated systems without combining forces in some areas.

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 with government mandates already addressed by the shared service.
- **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 Service Level Agreements (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 SLAs and Memoranda of Understanding (MOUs).

Sections 3.3.1 through 3.3.3 describe the primary actions for achieving these long term benefits.

3.3.1. Improve the 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 are consistent, meet their performance objectives, and are 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. In order to ensure the highest degree of services is available to customers, the Department has developed a series of initiatives to improve customer service and operational efficiency. Among these is the Operational Support Services (OSS) organization process improvement program. This is an ongoing program that will improve process discipline and deliver outstanding customer service to the Department's IT Infrastructure customers.

3.3.2. Increase the Resilience and Quality of Our Infrastructure

A key aspect of quality infrastructure services delivery is the ability to support expected levels of system restoration and execute a 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 a level of redundancy and responsiveness 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. Three 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 Guides, and develop and implement both enterprise security services and a world-class enterprise security management and monitoring capability to implement the Plan. To ensure quality, IT infrastructure products will be designed, built, and configured to meet the Component service level requirements.

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. Figure 3-8 depicts the current (FY 2009) breakout of IT Infrastructure Investments by End User Support Systems (EUSS), Mainframes and Servers – Systems and Support (MSSS), and Telecommunications Systems and Support (TSS).

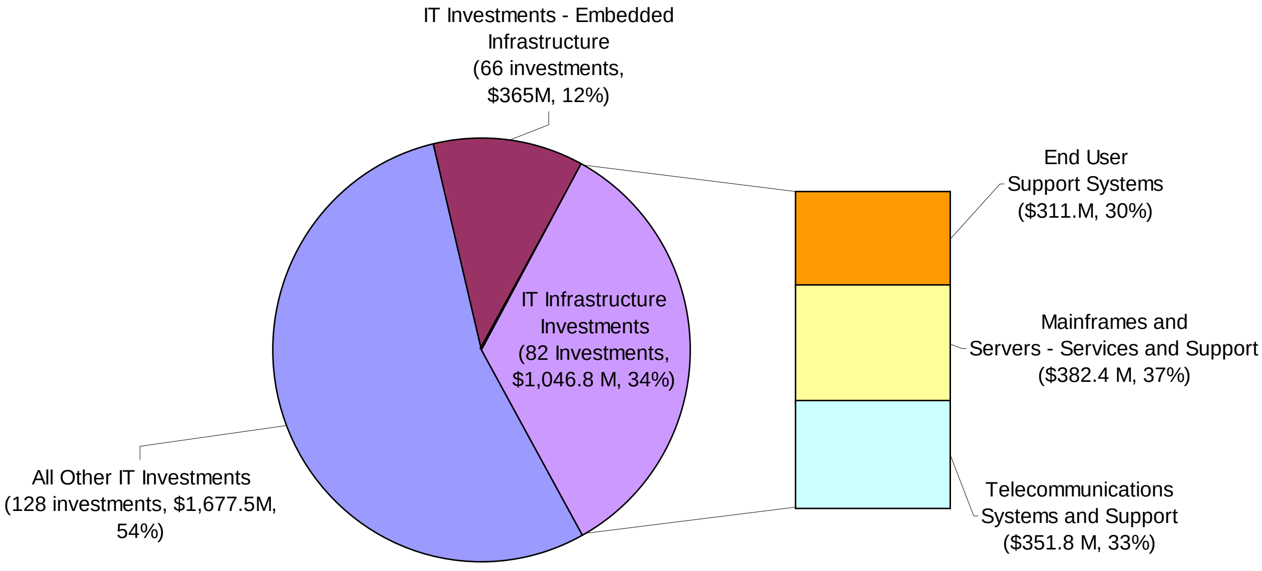

Figure 3-8: FY09 Infrastructure Investment Breakout

The analysis of the IT Infrastructure Segment spend helps determine the appropriate program synergies and consolidation candidates. Another issue that is identified from analyzing this financial data is that a very large percentage of IT spending (over 45%) is infrastructure related (**Figure 3-8**). This analysis shows the potential for investing in existing infrastructure programs and the opportunities for consolidating duplicative infrastructure services.

To achieve this strategy, the Department has taken steps to ensure use of common IT Infrastructure Shared Services by components across the Department. Among these are the development of common, centralized, shared services such as JUTNet, JSOC, the Justice Data Centers, the Classified Information Technology Program (CITP), and Justice Secure Remote Access (JSRA). In the future the department needs to develop ways to expand this list of shared services, and to deliver these services to an even wider customer base.

3.4. STRENGTHEN IT SECURITY

Strengthening DOJ's IT security involves a multi-pronged approach based on accomplishing several objectives. First, information assurance and cybersecurity must be institutionalized across DOJ. Identity, credential, and access management programs across the Department must also be integrated. The Department must establish and continue to maintain a trusted and reliable information and communications infrastructure. Finally, DOJ must acquire IT products, solutions and services with a known level of assurance and accessibility.

3.4.1. <u>Institutionalize Information Assurance, Security, Privacy, and Accessibility</u>

Institutionalizing and formalizing cybersecurity at DOJ involves the coordination of governance, policy, oversight, training, and technology-based tools to ensure that the Department continuously strengthens its IT security. The key objectives of this strategy are described below.

3.4.1.1. Governance

The Department's IT Security Governance Committee (ITSGC) and the IT Security Council (ITSC) serve as the coordinating groups for IT security across the Department. The ITSGC and ITSC coordination activities include: developing Department-wide IT security policy, standards, guidelines; discussing the security implications of new technologies before they are purchased by the Department and; researching potential threats, vulnerabilities and security controls and disseminating this information to DOJ Components. The ITSGC integrates enterprise risk management into the monitoring and maintenance of IT security initiatives to ensure alignment against the Department's strategic objectives given mission impact and priority. Issues such as limited resources, competing and conflicting requirements and limitations associated with current capabilities are addressed within the ITSGC.

3.4.1.2. Policies, Procedure, and Implementation

The Department's IT security policy is contained in DOJ Order 2640.2, Information Technology Security. The Order establishes policy, responsibilities and authorities for the implementation and protection of the Department's IT systems.

Policies need to clearly address the Department's IT security needs and are the foundation of a security program. Policies also are the primary mechanism for the Department's senior management to communicate its IT security requirements to the Components. IT Security policies are adjusted, as required, and evaluated against the risks that the Department or Components may not be able to perform their functions if the strictest possible security measures are put in place. Standards and guidelines provide detailed rules for implementing policy and should be practical to implement.

The Department has developed 18 IT security standards based on NIST SP800-53, Revision 2, "Recommended Security Controls for Federal Information Systems." The current version of the IT security standards is shown in Table 3-3.

Classified Laptop and Standalone Computers (Version 1.2)	Maintenance (Version 2.0)
Access Control (Version 2.2)	Media Protection (Version 3.1)
Audit Accountability (Version 2.1)	Personnel Security (Version 3.2)
Awareness and Training (Version 3.1)	Physical and Environmental Protection (Version 3.1)
Certification, Accreditation, and Security Assessments (Version 3.2)	Planning (Version 3.2)
Configuration Management (Version 1.1)	Risk Assessment (Version 3.1)
Contingency Planning (Version 2.1)	System and Communications Protection (Version 1.1)
Identification And Authentication (Version 2.1)	System and Information Integrity (Version 2.0)
Incident Response (Version 3.0)	System and Services Acquisition (Version 3.1)

Table 3-3: DOJ IT Security Standards

3.4.1.3. *Component Oversight and Coordination*

To provide oversight of Component compliance with applicable Federal and DOJ security policies and standards, the ITSC prepares a "Program Progress Report Card" for all DOJ Components that develop or operate IT systems. The Report Card provides the status of Components' accomplishments in achieving FISMA objectives. It is updated online for the ITSC, DOJ CIO and Component Heads, using the Cyber Security Assessment and Management (CSAM) Toolkit, which is described below. Scores are based on performance as it relates to the specific control measures in each project area.

3.4.1.4. *Cyber Security Performance Measures*

The Department is committed to identifying risk-based performance measures and establishing a program for regularly reporting on effectiveness of agency security programs. Performance measurement can support the advancement of an effective and efficient enterprise IT security management program.

Currently, the Department is reporting on three performance measures designed to assess the effectiveness of the DOJ's security posture. These include Incident Response Plans Exercised, which measures the percentage of IT systems that conduct annual incident response tests; Incident Responders Trained, which tracks the percentage of DOJ staff trained annually on security awareness; and Program Risk, which measures the percentage compliance for each security goal attained by an IT system.

In addition, other risk-based measures allow the Department to perform effective risk assessment of IT systems, continuously monitor security controls to assess the Department's security posture, and address weaknesses identified in IT Systems.

3.4.1.5. *Security Management and Support Tools*

The Department provides Components with a suite of tools that are designed to help with prioritizing security improvements and making cost-effective risk-based IT investment decisions. The primary solution is the Cyber Security Assessment and Management (CSAM) Toolkit, which is a suite of technologies providing automation to achieve compliance with the Federal Information Security Management Act (FISMA) and other mandated requirements. The CSAM Toolkit serves as the formal system of record for DOJ's inventory of information systems for FISMA. It supports FISMA report generation and management oversight of Department, Component and system IT security postures, and significantly reduces the time and cost of the certification and accreditation (C&A) process. It also helps to ensure consistency across the C&A documentation for a system. Based on the success of the CSAM tool, DOJ has been selected by OMB as a shared service center for conducting C&A activities and FISMA reporting activities for federal agencies through OMB's Information Systems Security Line of Business.

In addition to CSAM, the Department utilizes a full range of automated tools to support incident detection, as well as the related areas of configuration management, and vulnerability assessment. These include but are not limited to firewalls, antivirus software, incident detection systems, end-point computing security, and network scanners.

3.4.1.6. *Security Training for the DOJ Workforce*

Promoting user awareness is essential to successfully implementing information security policies and ensuring that security controls are working properly. The Department's IT security awareness and training program addresses current security threats and vulnerabilities through on-going user awareness training and IT security professional training. The program also verifies that DOJ Components have reviewed, updated, and distributed their Component-specific security training plans.

IT security awareness and General User Rules of Behavior modules are offered under an automated learning management system, the Computer Security Awareness Training (CSAT). CSAT is the primary delivery and tracking system for computer security awareness training. IT Security Professional Training includes developing and deploying social engineering and "phishing" exercises. Some training is conducted using formal instruction methods, while others, such as the phishing exercises, are conducted without the users' knowledge to simulate a real attack - this can be a very effective way to train users to identify and resist such attacks.

In addition to awareness and education efforts, the Department convenes a Cyber Security Conference that brings together DOJ personnel and representatives from other federal agencies, industry, and academia to discuss new DOJ IT security programs and share the latest information on cybersecurity topics.

3.4.1.7. *Protecting Personally Identifiable Information (PII)*

The Department ensures protection of PII data by updating and reviewing the DOJ PII processes, policies, and technological controls for systems that store PII. This includes the Initial Privacy Assessment (IPA) process, System of Records Notice (SORN) process, Privacy Impact Assessment process, privacy reporting, and procedures for handling PII data breaches.

3.4.2. Integrate Identity, Credential, and Access Management Programs

There is a need for DOJ to develop risk-based and cost-effective solutions for enabling secure access to DOJ facilities and systems. Drivers such as Homeland Security Presidential Directive (HSPD)-12 and E-Authentication have prompted DOJ to define a roadmap and guidance for identity, credential and access management. The Department is establishing a framework for consistent application of Federal identity management requirements with the Department's logical and physical access systems. In addition, the Department is working towards ensuring appropriate controls for web applications used for services to citizens, business and other governments.

To this end, the Department is working to achieve HSPD-12 compliance, by issuing Personnel Identity Verification (PIV) compliant credentials to DOJ employees and contractors. It is anticipated that PIV-compliant identity badges will be distributed to all DOJ personnel in major metropolitan areas by the end of 2010. DOJ's Identity Management Services program is developing the Department's federal identity, credential, and access management (FICAM) roadmap transition plan and is evaluating the impact of HSPD-12 requirements. Formal DOJ guidance FICAM transition planning is expected to be released to Components by the end of 2009.

3.4.3. Assure a Trusted and Resilient Information and Communications Infrastructure

Strengthening and securing the Department's information and communications infrastructure involves several activities. These include compliance with the OMB Trusted Internet Connections (TIC), which is focused on establishing a secure communications architecture through the Department's Trusted Internet Gateways. DOJ's various networks must be standardized and consolidated, and infrastructure resilience must be increased. There are also numerous on-going efforts designed to increase the resilience of DOJ's IT infrastructure, including configuration management, change control, and implementation of the Federal Desktop Core Configuration (FDCC). In addition, the Justice Security Operations Center (JSOC), as the primary DOJ source for real-time security events across all DOJ networks, offers a variety of detection, response, reporting and engineering services that serve to strengthen the DOJ IT infrastructure.

3.4.3.1. Configuration Management and Change Control

The DOJ Configuration Management Program maintains consistent Configuration Management monitoring procedures across the Department. The program is focused on implementing policy and procedures for tracking and approving changes to systems. It identifies controls, audits all changes to systems, addresses hardware and software changes, network changes, or any other changes affecting system configuration and security accreditation. The overall objective is to improve the efficiency of the existing DOJ security program by incorporating automation for operations and maintenance of DOJ's IT systems in the areas of patch management, auditing, and related activities.

In addition, the Department has Change Control Boards (CCBs) in place to develop, maintain, and promulgate accepted secure configuration standards for commonly deployed information system component technologies.

3.4.3.2. Federal Desktop Core Configuration (FDCC)

The Department is in the process of implementing FDCC for all desktop systems, with a target completion date in late 2009. It includes deploying an FDCC-compliant Internet web browser and a personal desktop firewall. FDCC implementation requires that DOJ components utilize the FDCC standard configuration, have a plan for completing deployment, and be in the process of deploying it to all systems within their network.

3.4.3.3. Identification and Response to Emerging Threats and Security Incidents

Under the Justice Security Operations Center, DOJ operates DOJCERT (Department of Justice Computer Emergency Readiness Team), a centralized incident reporting and response center. The center is responsible for collecting all incident information, providing alerts, and ensuring systems are patched. DOJCERT is also responsible for reporting all incidents to US-CERT (United States – Computer Emergency Readiness Team) and Federal law enforcement officials. JSOC includes a Cyber Defense Operations Program which provides an enterprise-level capability to detect and respond to cyber threats. JSOC also manages Incident Response Plan Testing to develop and implement a Department-wide Incident Response Plan, and develops process improvements for Incident Handling. Additional JSOC services include detection (event analysis, incident coordination, threat mitigation, monitoring), response (malware analysis, forensics, on-site incident response), reporting and communications (trend analysis, cybersecurity alerts, user awareness, custom and metrics reporting), and engineering support. JSOC is also involved in proactive network defense measures through use of a Vulnerability Management Program. In addition, JSOC is involved in Vulnerability Assessment & Penetration Testing to independently verify and validate the security of DOJ systems and networks.

3.4.4. Acquire IT Products, Solutions, and Services with a Known Level of Assurance and Accessibility

Acquiring secure IT products is a key objective in strengthening the Department's IT security. In addition to establishing common security requirements for IT acquisition, and incorporating standardized security-specific language into IT contracts, the Department is focused on identifying solutions to address issues such as protecting "data at rest", end point life cycle management, and defending against supply chain threats. For example, the Department has a requirement to implement "data at rest" solutions to protect DOJ information stored on mobile IT equipment. To address this, DOJ has implemented full disk encryption for all Department-issued, JCON-based laptop computers. Another example is utilizing an enterprise solution to monitor the Department's inventory of end point equipment, automate system patching, and validate Federal Desktop Core Configuration (FDCC) settings.

The White House and the National Security Council, through its cybersecurity policy development effort, have identified global supply chain risks as a contributing factor that may impact the federal government's IT security posture. New manufacturing, design, and research centers around the world raise concerns about possible subversion of computers and networks through hardware or software manipulations. This is compounded by the existence of counterfeit IT products. DOJ will monitor these policy developments and engage with key actors in this effort to ensure that the Department's security posture addresses supply chain related threats.

3.5. STRENGTHEN IT MANAGEMENT

The Department's IT community must make the best use of collective purchasing power, effectively collaborate across the Department, and attract and retain well-qualified IT professionals, to continue to improve DOJ program performance through the use of information technology. 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 required to assure the security and privacy of the data that the Department holds in its custody and uses to fulfill its responsibilities, including joint operations with Federal, SLT, and international partners.

3.5.1. Share Acquisition Power

DOJ will continue to improve the collective buying power of the Department. In the past, various Components within DOJ have procured software, hardware, and IT support services separately, and often large programs within the Components have made discrete IT procurements as well. While this is still common, both the Components and the Department have made progress in establishing enterprise-wide IT acquisition vehicles that are more cost effective than smaller, individually negotiated purchases. The process of identifying key products and services being used by two or more DOJ Components helps drive towards consolidated enterprise licensing agreements (ELAs) and blanket purchasing agreements (BPAs) with product vendors. These are developed and tracked by product or service type. For example, the BPA for printer purchases initiated and managed by the Executive Office for United States Attorneys (EOUSA) has been made available for use by other DOJ components; it offers a standard product list of printers and related hardware for better prices than what can be negotiated by individual US Attorney's Offices. EOUSA achieved savings of $11.3 million after the first year of using the printer BPA. Similarly, usage of the GSA NETWORX contract for future JUTNet and other telecommunications purchases offers similar opportunities for savings. Adoption of strategies such as these should help lower the cost of products and services for Components, thereby achieving greater levels of consistent support across the Department and vendor community.

The DOJ OCIO's Contracts Management Services (CMS) office plays an important role in improving the Department's buying power. CMS offers a convenient and economical means to acquire commercial software products and support, and commercial online databases. Enterprise licenses that have achieved measurable savings include Microsoft and Oracle. The goal is to implement a true enterprise management process by pooling requirements and presenting a single negotiating position to leading vendors, resulting in pricing advantages and volume discounts that would not be available to individual DOJ components. All CMS services are available for use by any DOJ component and should continue to be leveraged to achieve cost efficiencies and promote the sharing of Departmental acquisition power.

3.5.2. Increased Collaboration Among IT Staff

To guide the implementation of this strategy, IT staff from across the Department needs to work together collaboratively and effectively. To this end, the DOJ CIO Council has been restructured to become a key forum for discussion and agreement on key policy directions, technical strategies, and organizational issues required to effectively implement the goals in this IT strategic plan. 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. In support of the restructured CIO Council, other groups also continue to provide forums for cross-Component collaboration. These include the IT Security Governance Council and the Department Architecture Advisory Board (DAAB), as well as specific technology domain working groups such as the Standard Infrastructure Working Group (SIWG).

3.5.3. Attract and Retain a Skilled Workforce

Government staff must continue to provide key leadership and direction to the Department's IT programs, as most technology implementation and operational work is being outsourced to commercial and other government service providers. The Department continues to recruit and retain qualified staff in key IT positions such as IT security, program and project managers, architects, contracting staff, and staff who would like to move into key managerial and executive positions in the future.

Competition for quality talent at all grade levels is increasing with commercial providers as well with other government agencies. This competition is high for qualified IT security professionals, for which current demand far exceeds the availability of skilled personnel. 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, staff members need 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 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 an important supporting role in delivering on the Department's goals for those programs.

Further details on human capital management goals and objectives can be found in the DOJ Human Capital Strategic Plan: http://www.usdoj.gov/jmd/ps/missionfirst.pdf.

3.5.4. Improve Process Discipline

As part of the departmental strategy for improving process discipline and delivering outstanding customer service the Operational Support Services (OSS) organization has developed a series of initiatives to improve customer service and operational efficiency. These initiatives began in the summer of 2006, are ongoing, and have included the development of the OSS Strategic Plan, reengineering of core processes, and reorganizing the reporting structure of the OSS.

OSS's initiative to improve process discipline and leveraged learning will lead to better planning, cost efficiencies, outstanding customer service, and cutting-edge technology implementation. This renewed focus on new business development and customer relationship management will include a clearly defined organizational strategy to guide IT investment decisions, resource allocations, projects, tasks, and outputs. The commitment to this process discipline emphasizes that OSS will continue to work with customers in partnerships to meet customer requirements while efficiently supporting the overall DOJ mission.