DOJ INFORMATION TECHNOLOGY STRATEGIC PLAN

2010-2015

United States Department of Justice

December 9, 2009

For Official Use Only

This page has been intentionally left blank

Washington, D.C. 20530
December 9, 2009

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

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

The Department currently spends over $2.8 billion annually on information technology investments. This includes hardware, software, and personnel to manage a complex and secure infrastructure. It is imperative that these IT investments be undertaken in a cost-effective manner — they must be managed to bring the greatest return on investment and they must be secure. Everything we do within the Office of the CIO looks at the value of the IT investment, and ensures that what we build can be protected and utilized by our partners at all levels of government. As we move forward, our job is to make sure that every dollar invested in information technology provides the greatest return and makes the best possible use of our resources.

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

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

Sincerely,

Vance Hitch
Chief Information Officer

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. ROLES AND RESPONSIBILITIES

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

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

Figure 1-1: CIO Competency Areas

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

As depicted in Figure 1-2, the DOJ CIO also serves as both a leader and a coordination entity between the Justice Department and other key Federal agencies. This includes the Department of Homeland Security (DHS) and the Director of National Intelligence (DNI), but also State, Local, and Tribal (SLT) governments who have on-the-ground responsibilities for law enforcement, judicial processes, incarceration and first response in the event of a terrorist attack. Because of the importance of the central role in facilitating information sharing among these key entities, interoperable and integrated technology is needed to support these mission processes. To accomplish this, the DOJ CIO needs to lead the effort to both standardize and consolidate key infrastructure to allow intra-agency and cross-agency sharing of data, information and applications and to leverage the use of existing, and the creation of new, enterprise solutions that will improve mission results.

Figure 1-2: DOJ OCIO Key Relationships

To be successful at these broad and complex responsibilities, the DOJ CIO also provides leadership and coordination among the various Components within the Department, each of which has its own critical missions and responsibilities. In many cases the missions are unique to the Component and require specific solutions. The Component CIOs focus on meeting their respective mission IT requirements and providing high quality service to their business customers. However, in many other cases such as IT infrastructure, office automation, case management, administrative support systems, data and information sharing, and records management, there is a need for standardization, consolidation, and sharing of both infrastructure and solutions across the Department. The DOJ CIO provides leadership in facilitating the success of these initiatives by driving synergies and providing cross-cutting capabilities.

2. KEY DRIVERS

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

2.1. MISSION DRIVEN INFORMATION TECHNOLOGY

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

Figure 2-1: DOJ Partners

To combat these threats effectively, the DOJ must focus its limited resources on its mission priorities; improve its intelligence and investigative capabilities; and work more closely than ever before with its Federal and SLT partners and cooperating foreign governments as shown in Figure 2-1. Organizationally, the Department must be streamlined, agile, and technologically proficient. To meet these challenges, the DOJ Strategic Plan identifies three overarching strategic goals that the Department will pursue in support of its mission:

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

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

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

2.2. UPHOLDING PUBLIC TRUST

Maintaining public trust in the fair, efficient, and depoliticized administration of Justice is critical for DOJ. Aspects of this include responsible financial stewardship, appropriate use of authority, and securing the privacy of sensitive information. This is particularly important given DOJ's central role in Federal law enforcement and litigation.

As with any government agency, DOJ has an inherent responsibility to be a good steward of public funds, invest its budget wisely, and be above reproach in its disposition of resources. Another aspect of fiscal responsibility for the OCIO is to deliver quality products and services in a timely and efficient manner. Investments in IT programs need to be based on a sound business case which clearly demonstrates the value of the IT investments to the mission. IT programs must also be executed with discipline and in accordance with established IT governance policies and procedures. IT programs must also fit within the overall DOJ Enterprise Architecture to promote consolidation, standardization, and alignment with strategy.

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. The design and development of DOJ systems needs to always balance the priorities of providing quality, timely information while maintaining security and privacy of sensitive data.

DOJ must ensure that appropriate processes and policies exist to protect personal identifiable information (PII). DOJ must comply with all privacy and security laws, policies, and procedures. The Privacy Act of 1974 and the E-Government Act of 2002 are the two main statutes that establish privacy requirements for DOJ IT systems. Security principles, such as risk management concepts, are found in OMB Circular A-130, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-14, "Generally Accepted Principles of Practiceces for Securing Information Technology Systems" and General Accounting Office (GAO) Report GAO/AIMD-98-68, "Information Security Management — Learning from Leading Organizations."

2.3. FEDERATED ORGANIZATIONAL STRUCTURE

The Department's information technology function operates within a federated organizational structure, where multiple organizational components are responsible for multiple mission priorities (see Appendix F). The eight major DOJ Components, and several divisions, own and operate their own IT infrastructure and applications while leveraging enterprise or common solutions. This is reflected in the current DOJ IT portfolio which consists of diverse IT investments that cover a broad range Mission and Support functions. In addition, DOJ's IT portfolio can be categorized in terms of Component-specific IT investments, and Departmental or "Cross-Component" IT investments that support multiple DOJ Components.

Table 2-1 provides an overview of Component-specific versus Departmental cross-component Mission investments and IT Infrastructure investments[1]. The FY (Fiscal Year) 2009 IT budget of roughly $2.8 billion includes 200 IT Support investments and 100 Mission-focused IT investments. Of the 100 Mission-focused IT investments, 5 are Departmental[2], while 95 are Component-specific. The FY09 total for all Mission IT investments is $0.86 billion. Among the 84 Infrastructure Operations and Management IT investments (that are a subset of the 200 IT Support investments), 4 are Departmental cross-component IT investments and 80 are Component-specific. The FY09 dollar amount for these Infrastructure O&M IT investments is $1.10 billion.

IT Investment Type	Number of IT Investments			Total FY09 IT Budget Amount ($ Billions)
	Cross Component	Component Specific	Total	
Mission	5	95	100	$0.86
Support – IT Infrastructure, Operations and Management	4	80	84	$1.10
Support – All Other IT Investments	37	79	116	$0.86
TOTAL	46	254	300	$2.82

Table 2-1: DOJ FY09 Component vs. Department-Level Information Technology Investments

While DOJ has made significant strides in coordinating mission- and support-oriented IT investments across multiple components, there is still unnecessary redundancy across the Department. Addressing this redundancy and further leveraging enterprise solutions and shared IT services is essential to streamlining IT operations, lowering costs, sharing information, and meeting the Department's mission requirements.

2.4. GOVERNMENT-WIDE INITIATIVES AND OMB DIRECTION

DOJ is committed to supporting and leveraging government-wide IT policy objectives and cross-agency initiatives. These include OMB-sponsored initiatives such as Internet Protocol Version 6 (IPv6), government-wide initiatives such as Homeland Security Presidential Directive 12 (HSPD-12), and new government-wide initiatives focused on openness and transparency.

[1] An investment, according to OMB Circular A-11, is a system or an acquisition that has importance to the mission or function of the agency, a component of the agency or another organization. A "major" investment has significant program or policy implications; high executive visibility; high development, operating, or maintenance costs; is funded through other than direct appropriations; or is defined as major by the agency's capital planning and investment control process. Investments not considered "major" are "nonmajor."

[2] Departmental (or "cross-component") IT programs are funded and operated by the DOJ Justice Management Division (JMD). The budgeted amounts shown in this table do not include funding for cross-component IT investments that are funded by the DOJ Working Capital Fund (WCF).

In the fall of 2001, the OMB and Federal agencies identified 24 e-Gov Initiatives. Operated and supported by agencies, these initiatives have developed citizen-friendly and reusable government solutions for tax filing, Federal rulemaking, and e-training, among others. The President's E-Government Strategy has also identified several high-payoff, government-wide initiatives to integrate agency operations and information technology investments. The goal of these initiatives is to eliminate redundant systems and significantly improve the government's quality of customer service for citizens and businesses. The Department has successfully adopted several common solutions, such as E-Travel, E-Rulemaking, Grants.gov, and others. As we move forward in addressing the IT priorities of the new federal CIO, DOJ is committed to supporting and adopting existing and new cross-government efforts.

OMB initiated the development of the IT Infrastructure (ITI) Line of Business Initiative in 2006. Targeting the approximately $24 billion in IT infrastructure operations and management spent across the government, the purpose was to drive consolidation, standardization, and optimization through establishing benchmarks for cost and service levels and by holding agencies accountable for performance improvement against these benchmarks. As cross government initiatives have evolved over time, the ITI Line of Business has recently changed its focus toward Cloud Computing as a means to reduce the overall cost of acquiring and maintaining commodity IT across the federal government. As direction and guidance for Cloud Computing and other new federal IT priorities continues to develop, DOJ will collaborate with OMB and other federal agencies to improve the cost effectiveness and quality of our IT services.

In 2009, openness and transparency emerged as important themes in the federal government. To this end, several new Web-based initiatives, such as the Federal IT Dashboard, Recovery.gov, and Data.gov, have been introduced to inform the public about how the federal government is allocating taxpayer dollars towards federal priorities, and to open up government data for public use.

The Federal IT Dashboard (http://it.usaspending.gov) is a new initiative launched by OMB in 2009. Through the IT dashboard, agencies and the public have the ability to view details and progress of Federal IT investments. The IT dashboard provides Web-based access to IT investment-specific information such as the investment's description, awarded contracts, current and past performance measures, and cost and schedule information. Federal departments are required to provide monthly updates of cost and schedule data for all major IT investments. In addition, the IT dashboard provides a rating system for IT investments based on a Cost rating, a Schedule rating, a CIO rating, and an Overall rating. DOJ reports all Exhibit 53 IT investments to the IT dashboard, and includes additional cost, schedule and other metrics for major IT investments.

Recovery.gov (http://www.recovery.gov) allows visitors to "track the money" and meets a provision in the American Recovery and Reinvestment Act of 2009 that calls for establishing a website "to foster greater accountability and transparency in the use of funds made available in this Act." Its primary purpose is to allow taxpayers to see where federal Recovery Act money is going through user-friendly graphs, charts, and maps. DOJ has established a website (http://www.justice.gov/recovery) to provide the public with content on DOJ's Recovery Act programs.

Data.gov (http://www.data.gov) was established in 2009 to increase public access to datasets generated by the Executive Branch of the Federal Government. Improving access to Federal data has encouraged innovation by allowing the public to generate new ways of using the data through Web-based applications and other means. The website allows easy searching and downloading of federal datasets, and new datasets are added regularly. DOJ has made several datasets available on Data.gov, including crime statistics provided by FBI.

In addition, DOJ has addressed openness, transparency, and collaboration efforts through an expanded and updated Web presence in the new DOJ website, Justice.gov (http://www.justice.gov). Through a user-friendly design and new features, the new website focuses on tasks that members of the public can accomplish through the DOJ Action Center, official DOJ communications through the Briefing Room, DOJ-related news, and other content delivered using current Web 2.0 technologies. To expand its reach, DOJ has also established a presence on social networking sites (such as Facebook, MySpace, Twitter, and YouTube) to enhance its direct communications with the US public.

2.5. TECHNOLOGY TRENDS

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

Popular culture expects near instant access to complex data sets that are fully integrated and presented to Law Enforcement and Public Safety personnel in a format that can be translated into immediate action. Perhaps not as glamorous, but more real, is the fact that many private sector industries, from retail stores to banking, are using collaboration and self-service models that have become an accepted part of day-to-day experience . The DOJ OCIO understands the importance and expectations for information sharing between DOJ and its partners, and supports this priority through key initiatives such as the Law Enforcement Information Sharing Program (LEISP).

On the other hand, there is high demand for the most skilled technologists who possess the business transformation, architecture, security, management skills, and experience to leverage current and emerging technology trends to provide real benefits. The shortage of skilled professionals is acute for IT security – this may require innovative approaches to make the best use of resources by securing our systems in a centrally managed way, while continuing to support the collaborative, networked, flexible operations that are made possible by current technologies. For more on IT security trends, see section 2.7.

2.6. FINANCIAL CHALLENGES

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

IT infrastructure is an area of significant spending in DOJ's IT budget and includes technology such as networks, data center, end-user computing, and IT operations. As shown in Figure 2-2: FY09 DOJ IT Budget Allocation by Segment[3], IT infrastructure accounts for 34% of the FY09 DOJ IT budget. For enterprises with relatively low technology maturity, the percentage of their IT budget in technical infrastructure is typically 35 percent.[4] While government-specific requirements such as duplication of infrastructure across security enclaves do raise costs, there remains an opportunity to reduce the percentage of the DOJ IT budget dedicated to IT infrastructure operations and management and shift the IT budget towards direct mission support requirements. A full list of the DOJ EA Segments and their descriptions is available in Appendix A.

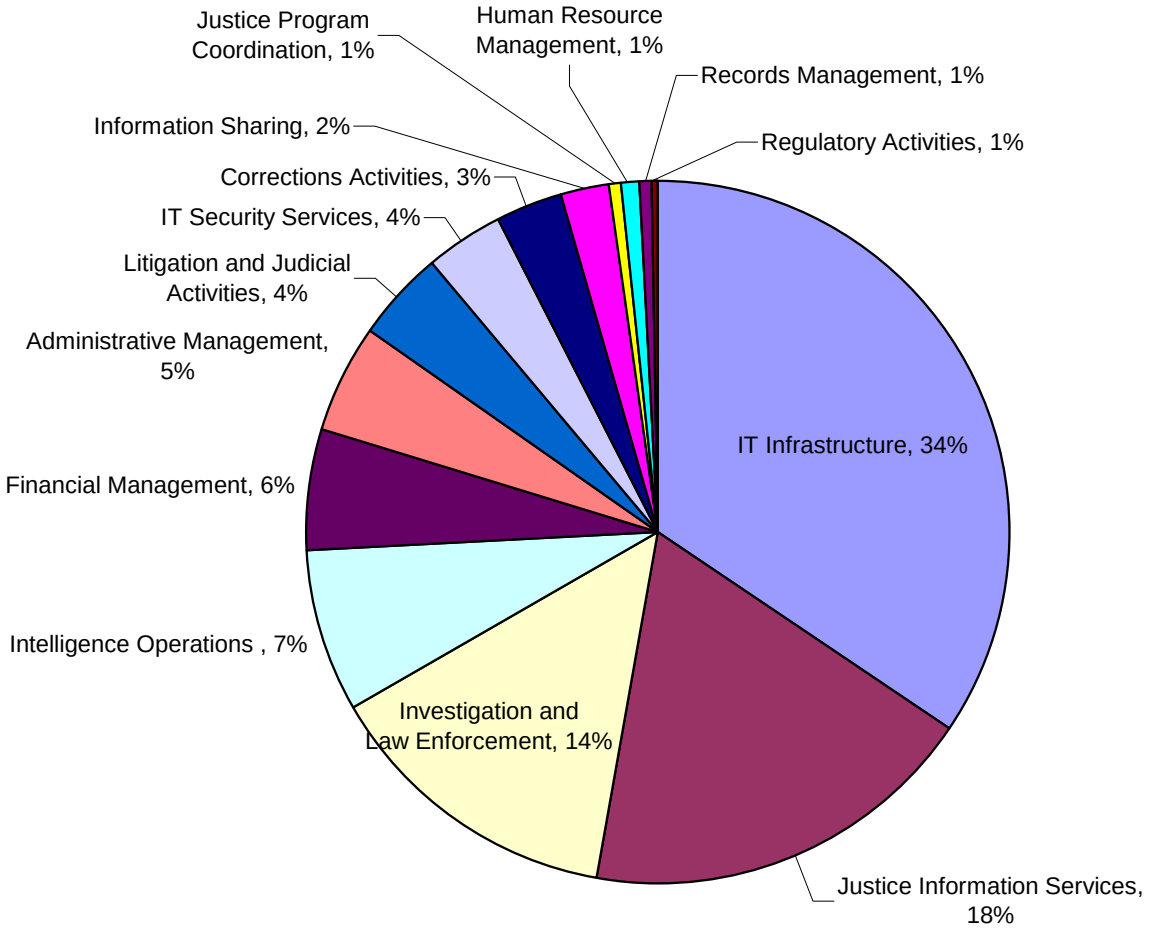


Figure 2-2: FY09 DOJ IT Budget Allocation by Segment

[3] Segment Architectures, as defined by OMB, are "subsets of the overall agency enterprise architecture, describing core mission areas (e.g., homeland security, health), business services (e.g. financial management), or cross-cutting enterprise services (e.g. Information Sharing)." (Source: OMB, EA Assessment Framework, Version 3.1)

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

2.7. EVOLVING CYBERSECURITY THREATS

The Department of Justice faces adversaries with tremendous skill and motivation to penetrate our network and infiltrate our data. Today's climate of rapidly evolving and changing technology is increasing and expanding our cyber-security vulnerability footprint. Threats to our IT systems have now evolved to a more sophisticated state that includes foreign nations, Organized Crime and thousands of others armed with tailor-made attacks targeting our staff and our systems. The traditional reactive defense mechanisms relied on in the past are no longer sufficient to mitigate the malicious activity of today and the future. The only assured means to counter this threat is a defense-in-depth architecture that includes solid information security policy and practices and aggressive detection and proportional response.

As our IT enterprise evolves and changes, cyber attackers adapt and change their mode of operation with seemingly equal agility. Over time, attacks against the Department and the US Government have become more focused, sophisticated and concentrated. Social networks consisting of cyber attackers allow information, attack patterns and the tools of destruction to be quickly transmitted and proliferated. Today's attacks use everyday communication channels, such as e-mail and web browsing, to facilitate their attacks. These services are inherent within our IT enterprise and render traditional cyber-defense practices insufficient to address our need.

These problems are compounded by the existence of multiple entry points and an increasingly more mobile workforce. These in turn increase our vulnerability footprint, which attackers can successfully exploit.

The federal government has taken various steps to improve IT security, with Congress passing the Federal Information Security Management Act of 2002 (FISMA), the National Institute of Standards and Technology (NIST) providing security standards and guidance, and with federal agencies establishing Information Security / Cyber Security programs, headed by Chief Information Security Officers (CISOs). While the effectiveness of these past activities can be debated, the broader federal government and DOJ must continue to take action against security threats that are constantly evolving to exploit both old and new vulnerabilities.

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).

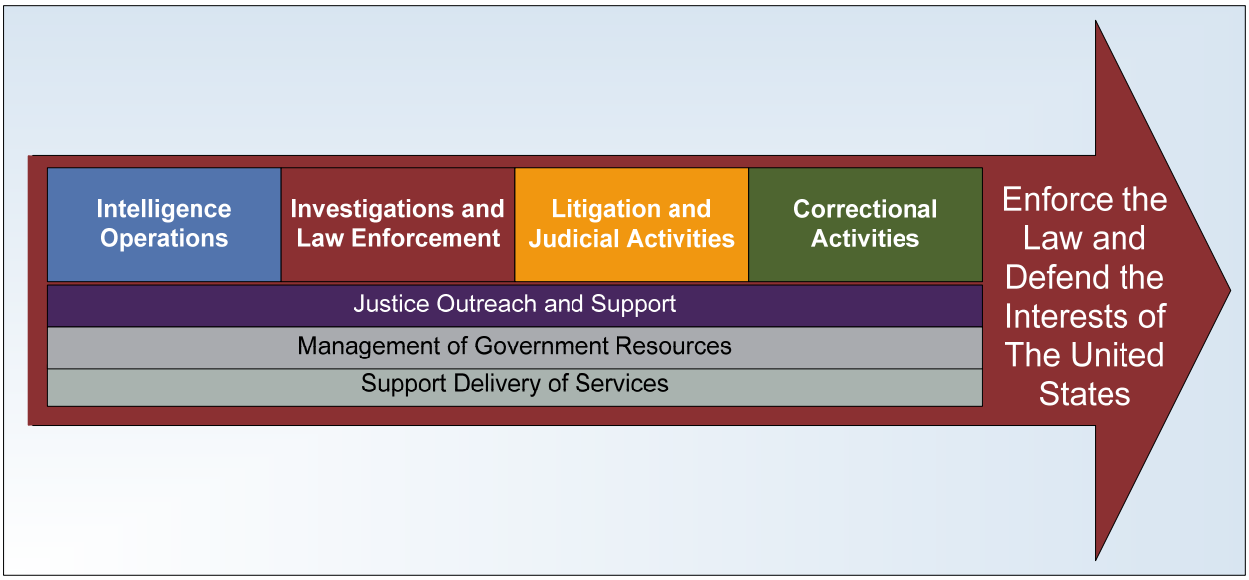


Figure 3-1: DOJ Value Chain

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.

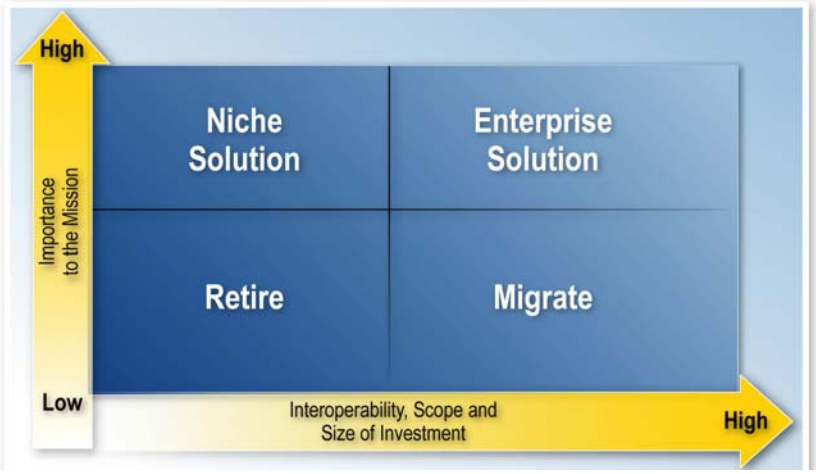


Figure 3-2: Program Evaluation Matrix

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.

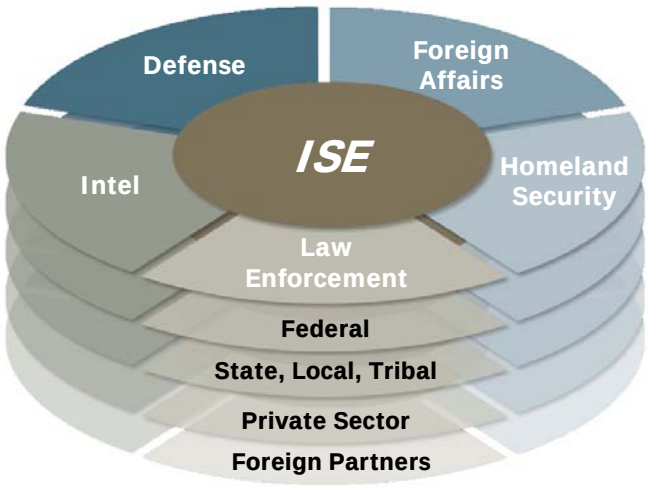


Figure 3-3: Information Sharing Environment (ISE)

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.

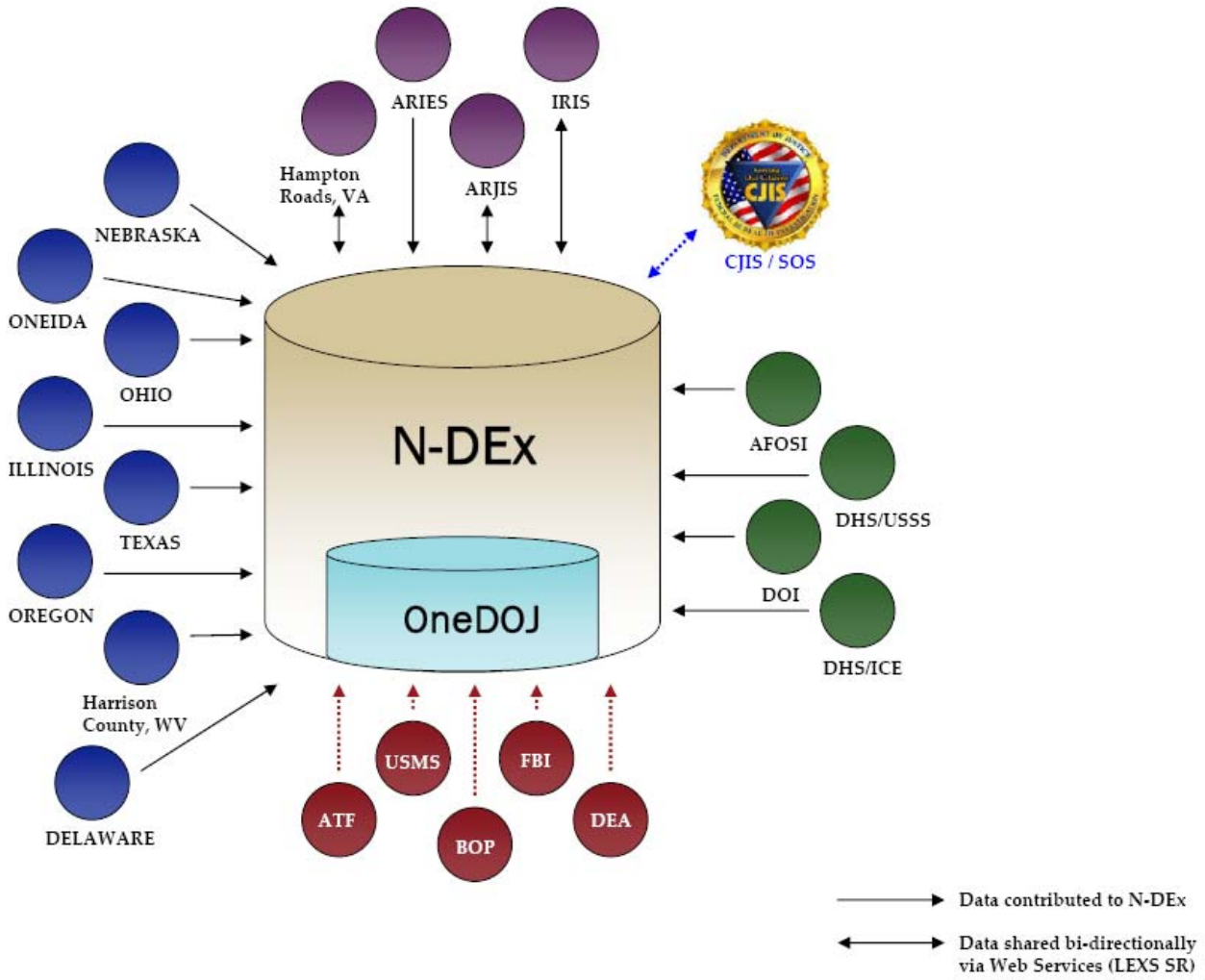


Figure 3-4: One DOJ and N-DEx Converged Capabilities

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.

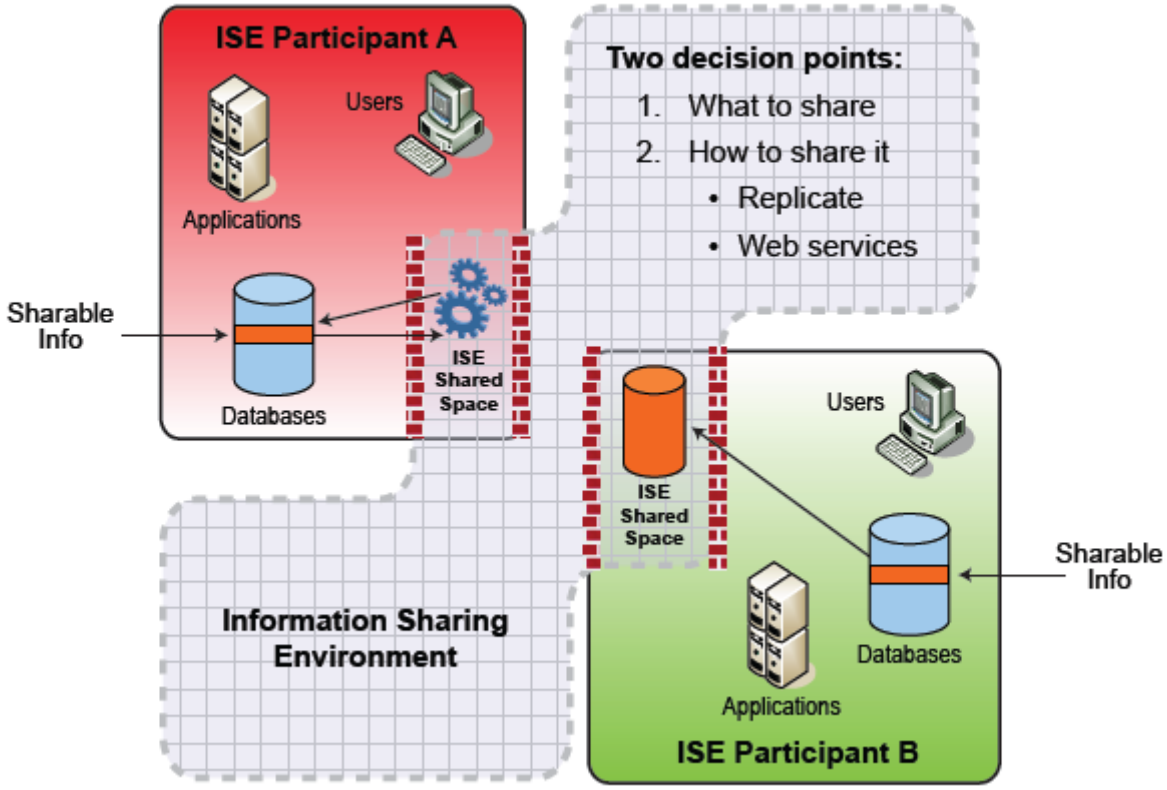


Figure 3-5: ISE Shared Spaces Concept

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.

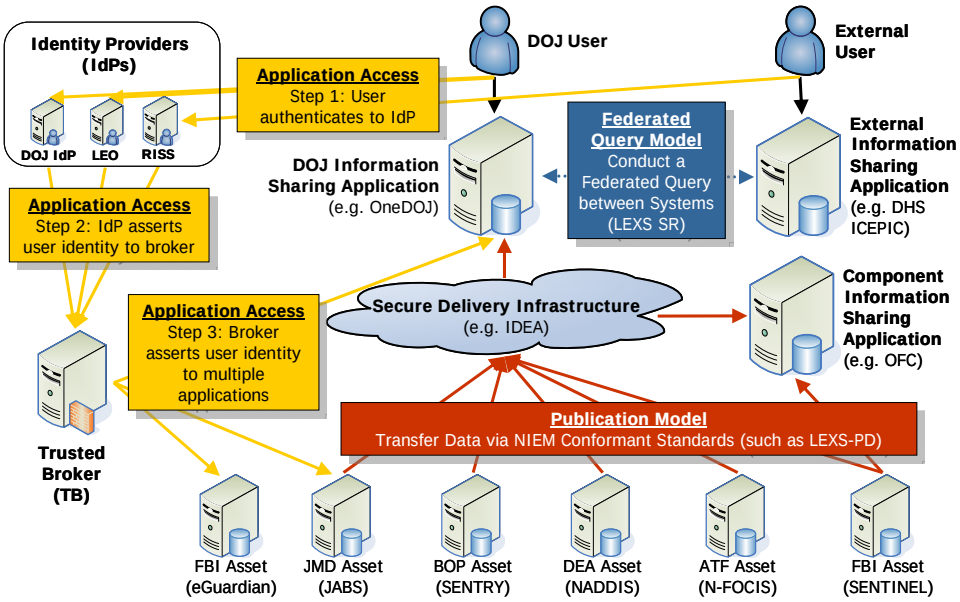


Figure 3-6: Overview of DOJ Information Sharing Techniques

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.

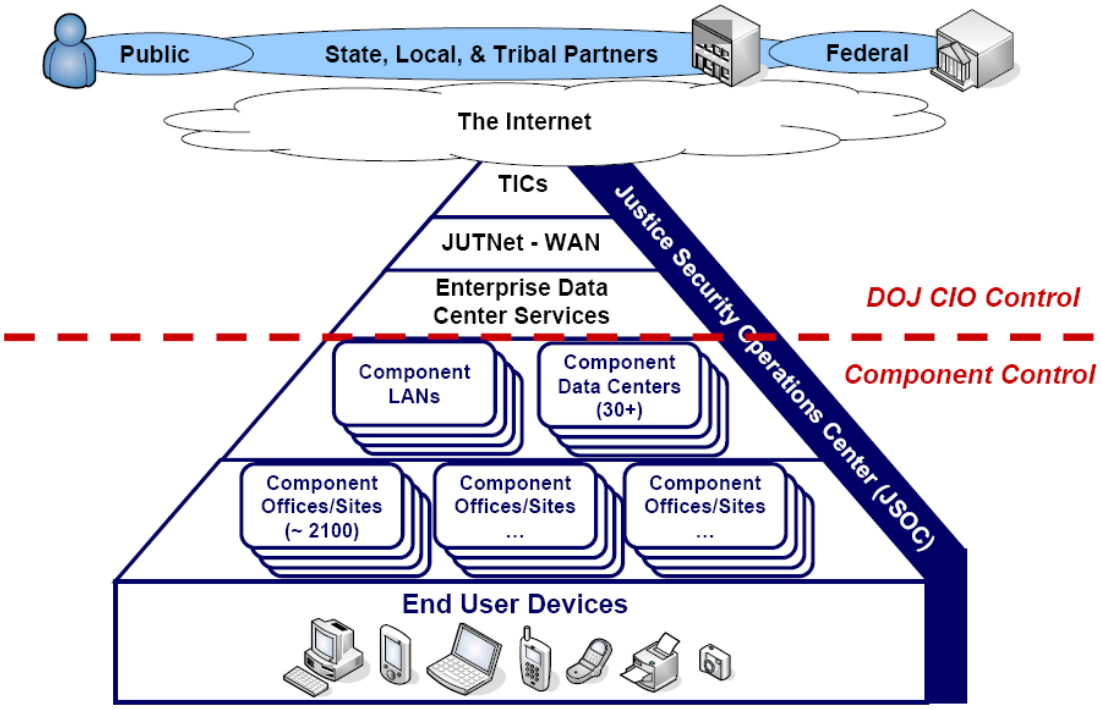


Figure 3-7 DOJ IT Infrastructure

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).

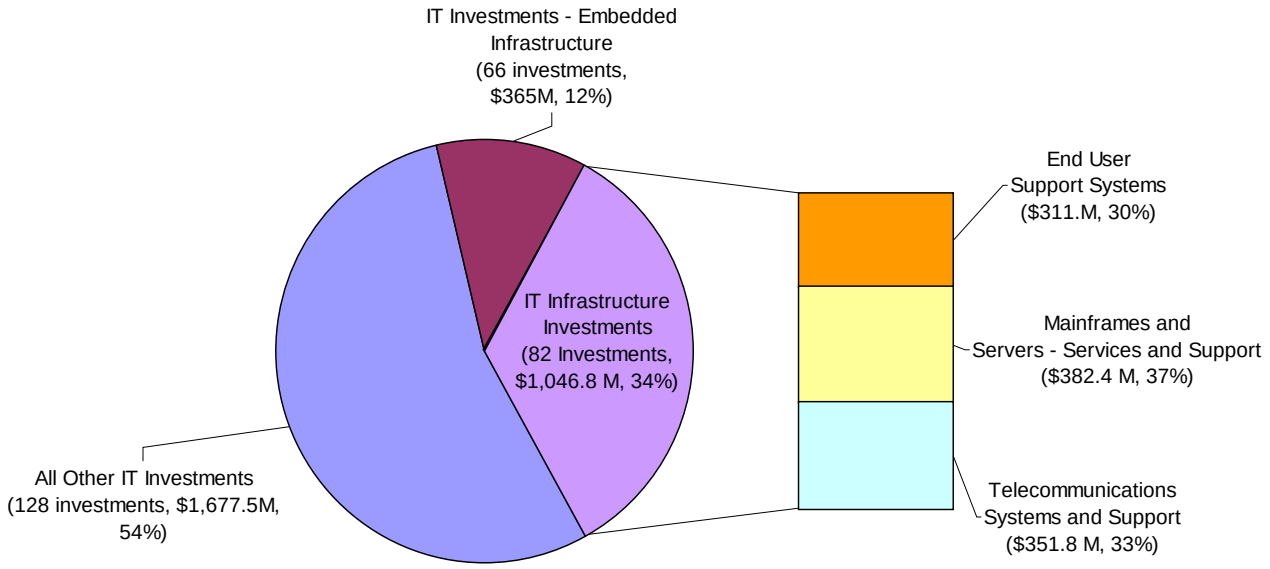


Figure 3-8: FY09 Infrastructure Investment Breakout

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. Institutionalize Information Assurance, Security, Privacy, and Accessibility

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.

4. KEYS FOR IMPLEMENTATION

To implement the IT strategic goals and related initiatives, we see the following as key to ensuring the Department's ability to deliver:

- Evolving the business model of IT
- Stronger cross-organization coordination, governance, and policy support
- Maintaining quality IT operations during change

Together with our stakeholders, DOJ OCIO will evaluate the trade-offs between our ability to absorb change, the value enabled by the change compared to the risk, and the level of executive sponsorship and available funds required to make it happen.

4.1. EVOLVING THE BUSINESS MODEL OF IT

Much of government IT exists in stove-piped silos – meaning that applications and infrastructure are funded, developed, and operated in a manner independent of other IT efforts across the government or even within the same federal agency. This is also true in the DOJ environment. To change this behavior, DOJ needs to fundamentally change its business model for funding, building, and operating IT. The focus of IT initiatives should be on enterprise solutions; interoperability across those solutions; and consolidated, optimized, and, when appropriate, centralized common services.

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

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

With infrastructure shared services in particular, OMB is driving federal agencies toward the use of cloud computing services – which are essentially shared computing resources that can be purchased and used as needed from a designated provider. There are many things that will have to happen before DOJ can use the cloud computing model, including further maturation of cloud computing offerings in the marketplace, further refinement and implementation of the Law Enforcement Sensitive designation of Controlled Unclassified Information (CUI), as well as further policy clarification about the appropriate use of cloud computing resources to handle government-owned and citizen-owned data. DOJ will continue to monitor and contribute to the cloud computing efforts that are underway across government and industry, and will consider the use of cloud computing alternatives after policy, technical, financial and other details of it are more mature.

4.2. STRONGER CROSS–ORGANIZATION COORDINATION, GOVERNANCE, AND POLICY SUPPORT

Currently, IT is organized across the Department as relatively independent Component-based entities. Among the Components, JMD is focused on the delivery and operation of DOJ-wide Enterprise Solutions and IT infrastructure, although there are notable pockets of shared activity elsewhere including Terrorist Explosive Device Analytical Center (TEDAC) with Bureau of Alcohol, Tobacco, and Firearms (ATF) and Federal Bureau of Investigation (FBI) and the Organized Crime Drug Enforcement Task Force (OCDETF) with the Drug Enforcement Administration (DEA). However, as the Department moves toward increasing the development and use of shared solutions, information and infrastructure, it is important to assign clear responsibility for operating and delivering these shared capabilities. In some cases, such as Privacy Policy, there is already a DOJ organization that has clear policy and oversight responsibility Department-wide (Office of Privacy and Civil Liberties), and where the overall cross-Component model works well and can be further extended.

Governance concerns for cross-Department solutions include those to manage and oversee product management, as well as joint issue resolution for cross-Department solutions. Product management is forward looking and includes the processes for ensuring stakeholder input and buy-in for solution requirements and implementation approaches. Issue resolution includes both operational issues as well as forward-looking concerns that cannot be addressed via conventional product management activities and need to be escalated through standard and repeatable processes. Currently the model is program- or Component-specific. Governance structures will need to be put in place for the management and evolution of shared assets, with membership to include personnel from each Component that uses the asset. The DOJ CIO Council and the Department Architecture Advisory Board (DAAB) can provide the necessary forums for establishing shared standards and oversight processes, and to provide guidance and resolution for cross-Component issues.

4.3. MAINTAINING QUALITY IT OPERATIONS DURING CHANGE

Evolving the business model and improving coordination, governance, and policy support will both need to happen without interrupting existing IT operations. As computing power and network connectivity have increased workplace productivity and access to information over the years, the availability of these resources has become essential to daily operations. In most environments, we can no longer do our jobs without them.

Upgrading and improving the way in which we deliver and manage IT services across DOJ will need to happen with little or no impact on the daily support we provide to many thousands of headquarters and field users across the Department. The increasing commoditization of IT further underscores the need for a seamless transition from old models to the new, in order to meet customer needs in an increasingly competitive IT marketplace. DOJ OCIO is organized into several operating units, as are many other Component IT organizations, in order to develop new capabilities while continuing to manage and maintain existing IT services. Changes to the IT business model, coordination, governance, or policy will be executed by these organizations, and these organizations will be restructured as needed in order to effectively and economically provide IT services for DOJ users.

5. CONCLUSION

Information technology plays an important role in enabling DOJ's core mission – preventing terrorism and promoting the nation's security; preventing crime, enforcing federal laws, and representing the rights and interests of people; and ensuring the fair and efficient administration of justice. The five strategies in this DOJ IT Strategic Plan are designed to ensure that IT supports and enables the delivery of mission-oriented results. The Department requires a well-coordinated approach to sharing business solutions, sharing information, making better use of existing IT infrastructure, enhancing IT security, and strengthening IT management practices. Implementing the strategies requires continuously evolving the IT business model and maturing IT governance processes, while maintaining a high quality of service for DOJ's on-going IT operations.

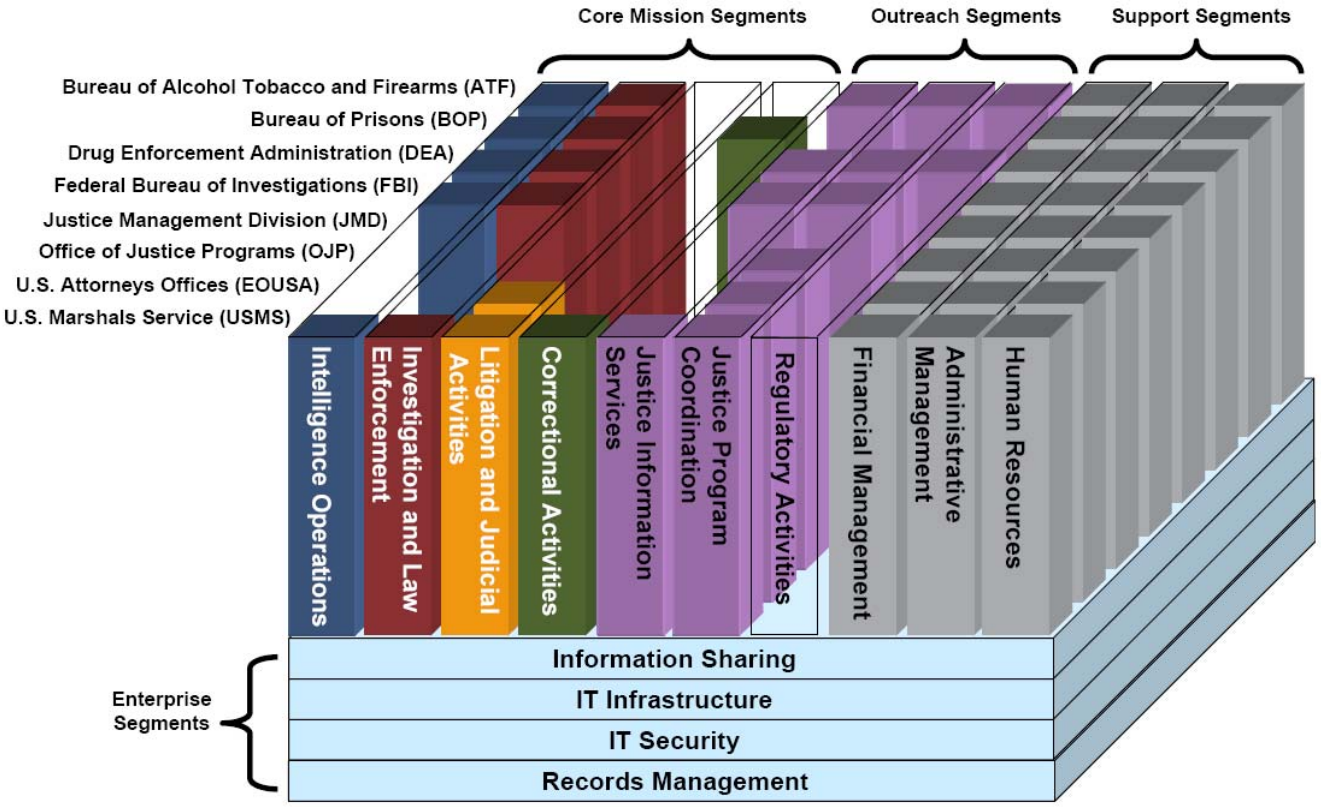
The Department is implementing the five strategies through IT investments that are designed to execute on the DOJ mission and achieve specific performance objectives. Ultimately, IT at DOJ is effective if it supports:

- DOJ's partners' and employees' ability to successfully execute on the DOJ mission, based on the delivery of enterprise solutions and the alignment of IT governance to mission needs
- Information sharing across the extended justice enterprise, coupled with policies to protect security and privacy, and the use of standards
- A better customer experience with DOJ's IT infrastructure; improved infrastructure resiliency and quality; and optimized use of infrastructure to improve cost efficiency
- A strong security posture for the Department. This consists of information assurance, security, privacy and accessibility; well-integrated identity, credential and access management; a trusted IT infrastructure; and acquisition approaches that incorporate IT security considerations in the purchasing of IT products, solutions and services.

The above will be achieved through the use of shared acquisition power, increased IT staff collaboration, a skilled and committed IT workforce, and discipline in carrying out IT processes and governance across the Department.

The DOJ mission, and much of the direct IT support for executing on the mission, resides in the Department's Component organizations. The Department's federated structure underlines the need for IT to operate effectively across multiple mission areas and organizational boundaries. IT needs to continue to support higher levels of mission performance in a flat or shrinking IT budget environment. It is also important to derive better value from the Department's enterprise solutions by leveraging them to address similar Department-wide business problems. Using enterprise solutions, as well as innovative technologies and approaches, DOJ will be better positioned to effectively serve business users and citizens alike.

Appendix A: DOJ ENTERPRISE ARCHITECTURE SEGMENTS



Enterprise Architecture "segments" are the focus areas of the DOJ enterprise architecture. Rather than attempting to address the full scope of issue that the Department is facing all at once, a segment approach within an overall EA allows specific data gathering and analysis in support of improved decision-making and better performance outcomes.

Segments are defined as *mission delivery* (lines of business) or *cross-cutting enterprise* segments.

Mission Delivery Segments are including similar activities that contribute to the success or failure of DOJ as viewed by the Executive branch, Legislative branch, and U.S. citizens. Examples of mission delivery segments are the "Core Mission" and "Outreach" segments as shown above. These segments include the activities and information systems we use to deliver on key performance metrics tracked in the DOJ Performance Accountability Report (PAR).

Cross-Cutting Enterprise Segments include support activities and common solutions that have the potential to address cost efficiencies and improved operations across the Department. Examples of cross-cutting enterprise segments are the "Support Segments" and "Enterprise Segments."

The graphic displays the DOJ component organizations (on the left) that own IT investments that are aligned to the Mission Delivery and Enterprise segments shown in the colored vertical bars and the yellow horizontal bars.

EA Segment Definitions:

- **Administrative Management:** Involves activities associated with the day-to-day management and maintenance of the internal infrastructure, and the critical policy, programmatic and managerial foundation to support federal government operations.
- **Corrections Activities:** Involves all federal activities that ensure the effective incarceration and rehabilitation of convicted criminals.
- **Financial Management Segment Architecture (FMSA)**: Summarizes the department's goals, objectives, programs, and information technology investments and systems that address current and future financial management practices.
- **Human Resources:** Involves the strategic management of human capital within the Department. This includes all activities associated with the acquisition and management of DOJ personnel, compensation, benefits, performance management, HR strategy, and the implementation of solutions and services from the HR LoB across the Department.
- **Information Sharing Segment Architecture (ISSA)**: Documents the DOJ's communications activities and describes the necessary policies, processes, architecture and governance needed to improve information sharing.
- **Intelligence Operations:** Involves collecting and analyzing information to meet the national security challenges of the U.S. by processing reliable, accurate foreign intelligence, and disseminating intelligence products to policymakers, military commanders, law enforcement entities, and other consumers.
- **Investigations and Law Enforcement:** Includes the activities to protect U.S. national interests, people, places, and things from criminal activity resulting from non-compliance with U.S. laws (e.g., deterrence, patrols, undercover operations, response to emergency calls, as well as arrests, raids, and seizures of property).
- **IT Infrastructure Segment Architecture (ITISA)**: Includes all the information technology resources such as hardware, software, networks, facilities, and services that are required to develop, test, deliver, monitor, control, support, or manage IT Services used to support or deliver the department's mission. It consists of End User Systems and Support (EUSS), Mainframes and Servers Services and Support (MSSS), and Telecommunications Systems and Support (TSS) and includes both direct (costs that produce tangible IT products or services for business users) and indirect (costs not leading to a tangible product or direct support of business users) such as IT management costs.
- **IT Security Services Segment Architecture:** Summarizes Information Technology (IT) security in the DOJ enterprise architecture (EA), as stated in recent guidance from OMB regarding the "Trusted Internet Connections" (TIC) initiative.
- **Justice Information Services Segment Architecture (JIS):** Presents the "core mission area" segment architecture that focuses on the creation and dissemination of information to assist state, local, tribal and federal law enforcement entities with background checks, identification services and criminal statistics.
- **Litigation and Judicial Activities Segment Architecture:** Presents the "core mission area" segment architecture that establishes the vision for a single case management solution to support litigative and judicial activities.
- **Records Management Segment Architecture (RMSA)**: Describes strategy and methods used to make and preserve electronic and print records of documents.

- **Regulatory Activities:** Involves activities that support the Department's regulatory responsibilities pertaining to controlled substances and firearms, including licensing, issuing permits, and reviewing companies for compliance under government regulations.

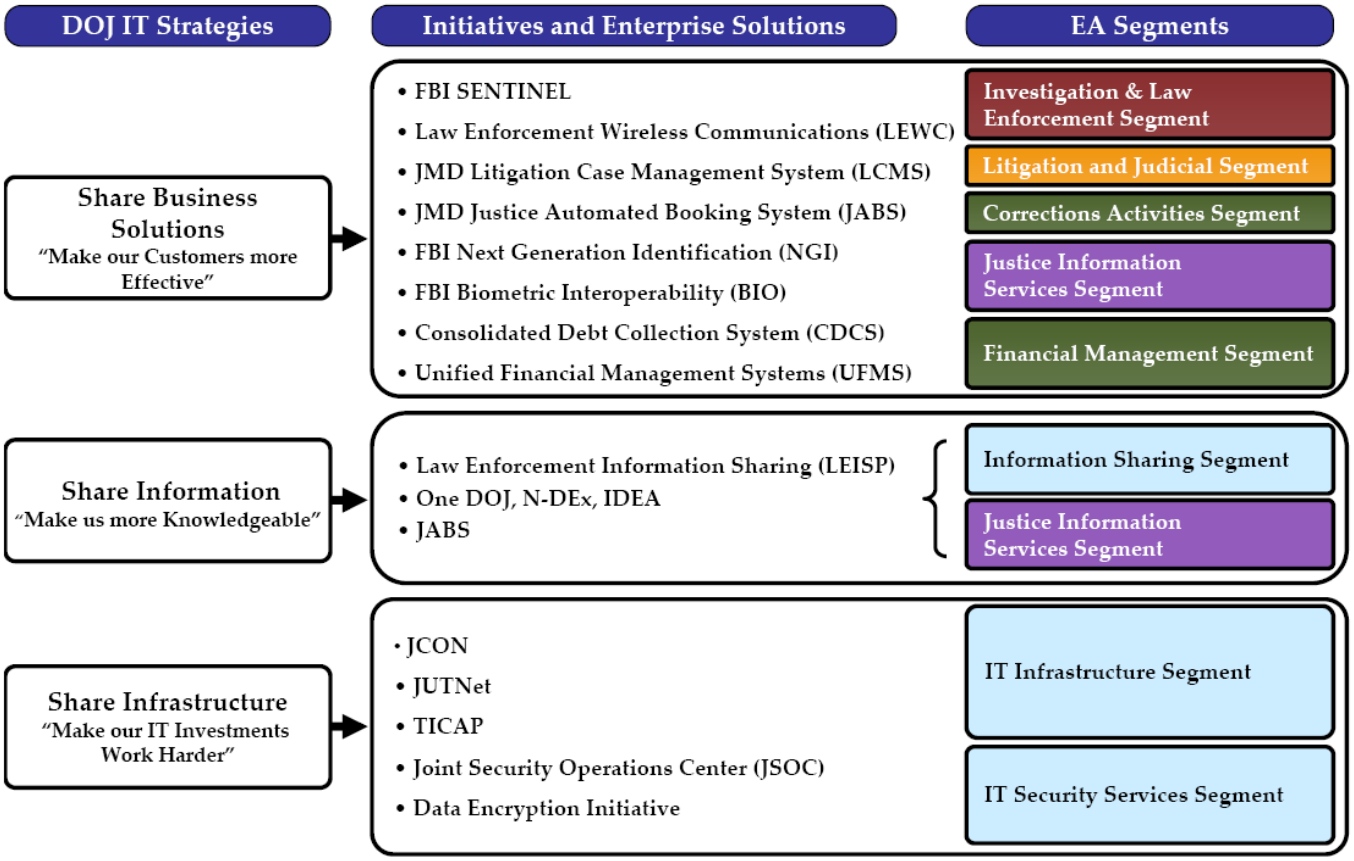
Appendix B: CROSS-WALK OF STRATEGY WITH ENTERPRISE ARCHITECTURE

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

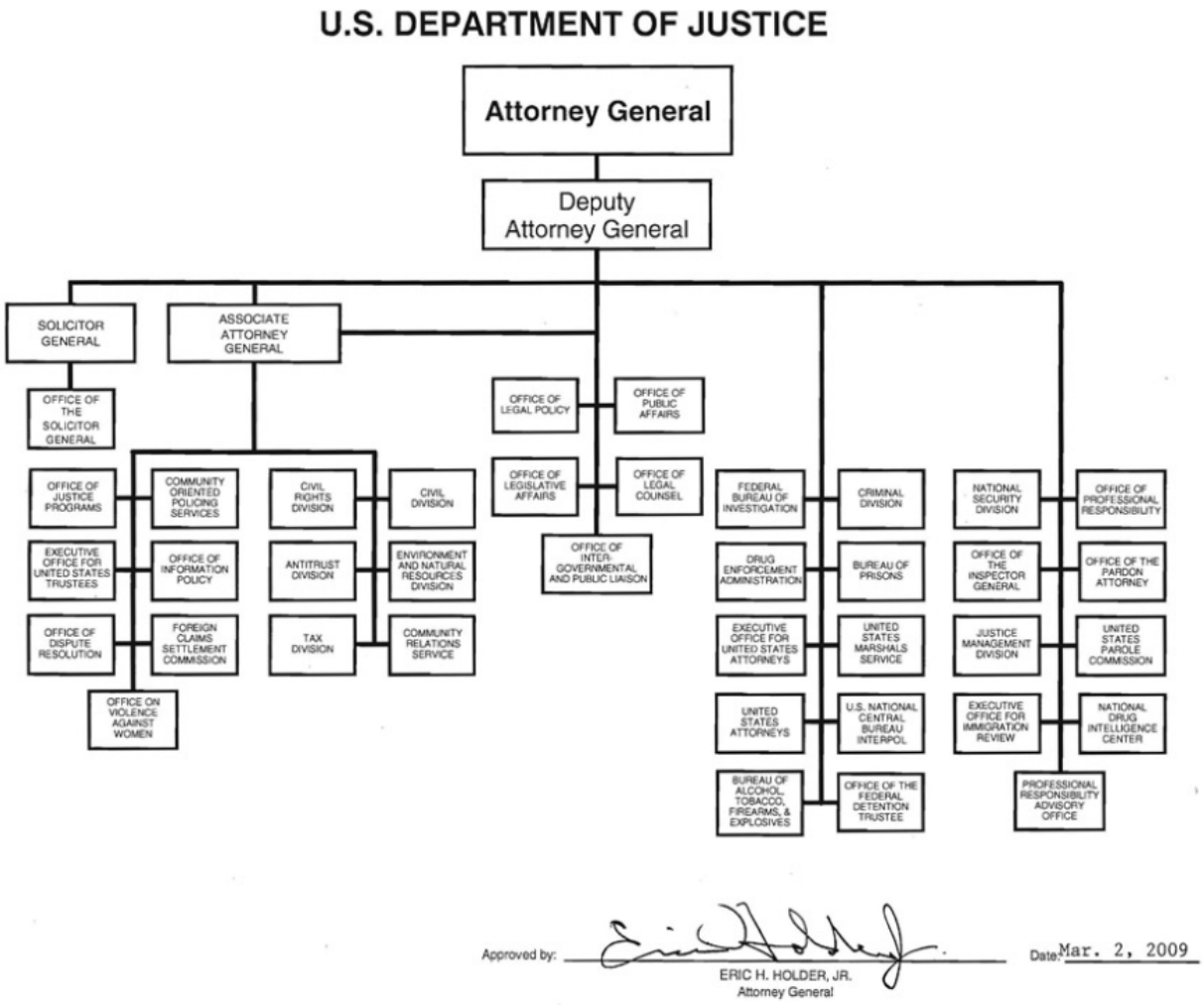
Strategy	Document Reference	Document Section
Share Information	Information Sharing Segment Architecture	**Entire Document:** 3 Volumes - Executive View, Program View and Architecture View
	DOJ Transition Strategy & Sequencing Plan	**Section 13** – Information Sharing Segment Architecture
	Enterprise Architecture Framework and Methodology	**Section 2.2.4** – Information Sharing
	Program Managers User Guide	**Section 3.2** – IT Strategic Plan **Section 4.1** – Information Sharing
Share Business Solutions	Justice Information Service Segment Architecture	**Entire Document**
	Litigation and Judicial Activities Segment Architecture	**Entire Document**
	DOJ Transition Strategy & Sequencing Plan	**Section 3** – Intelligence Operations **Section 4** – Investigations and Law Enforcement **Section 5** – Litigation and Judicial Activities **Section 6** – Correctional Activities **Section 7** – Justice Information Services **Section 8** – Justice Program Coordination **Section 10** – Financial Management
	Enterprise Architecture Framework and Methodology	**Section 2.2.3** – Enterprise Solutions
	Program Managers User Guide	**Section 3.2** – IT Strategic Plan
Share Infrastructure	DOJ Transition Strategy & Sequencing Plan	**Section 14** – IT Infrastructure
	Enterprise Architecture Framework and Methodology	**Section 2.2.5** – Infrastructure Shared Services
	Program Managers User Guide	**Section 3.2** – IT Strategic Plan
Strengthen IT Security	IT Security Architecture v1.0	**TBD**
Strengthen IT Management	DOJ IRM Policy	**Entire Document**

Appendix C: ENTERPRISE SOLUTIONS ADDRESSING STRATEGIC PRIORITIES

The Department's IT strategies are executed through a broad range of initiatives and enterprise solutions. These initiatives and solutions are grouped together using Enterprise Architecture segments as shown in the colored rectangles on the far right of the graphic. A segment perspective supports the coordination of cross-departmental IT initiatives and promotes the best use of DOJ's IT budget towards implementing the Department's IT strategies and goals.



Appendix D: DOJ ORGANIZATIONAL CHART

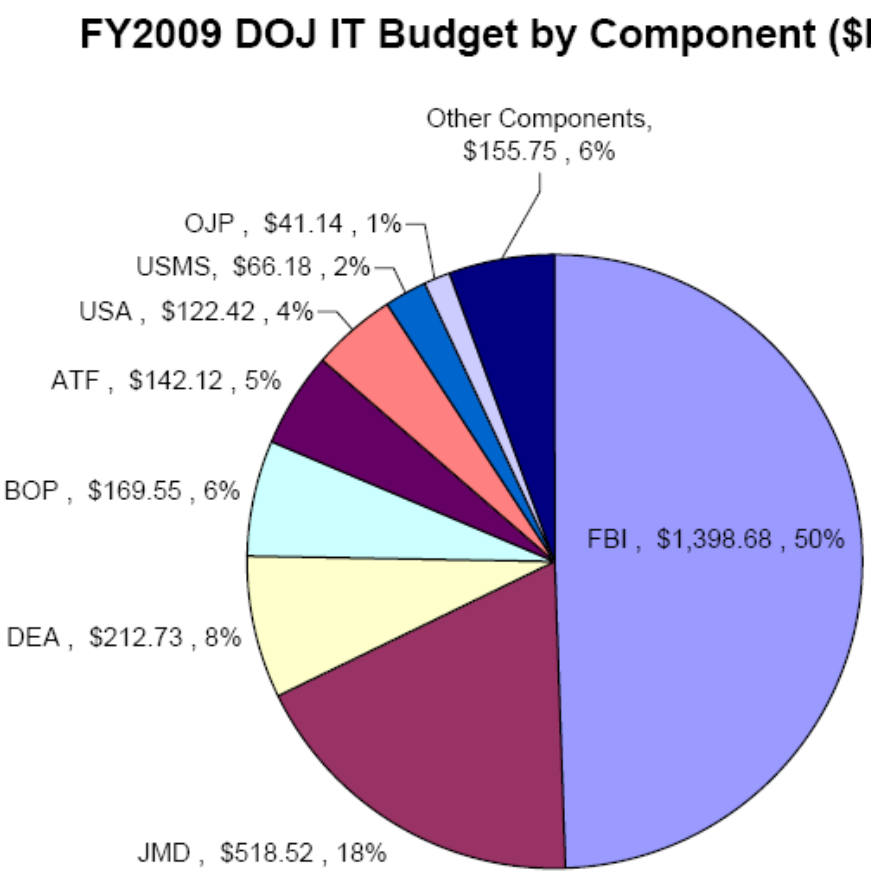


Appendix E: DOJ COMPONENTS LIST

DOJ Components include the following organizations:

Antitrust Division (ATR)	Office of Community Oriented Policing Services (COPS)
Bureau of Alcohol, Tobacco, and Firearms (ATF)	Office of Dispute Resolution (ODR)
Civil Division (CIV)	Office of the Federal Detention Trustee (OFDT)
Civil Rights Division (CRT)	Office of Information and Privacy (OIP)
Criminal Division (CRM)	Office of the Inspector General (OIG)
Community Relations Service (CRS)	Office of Intergovernmental and Public Liaison (OIPL)
Drug Enforcement Administration (DEA)	Office of Justice Programs (OJP)
Environment and Natural Resources Division (ENRD)	Office of Legal Counsel (OLC)
Executive Office for Immigration Review (EOIR)	Office of Legal Policy (OLP)
Executive Office for United States Attorneys (EOUSA)	Office of Legislative Affairs (OLA)
Executive Office for United States Trustees (EOUST)	Office of the Pardon Attorney (OPA)
Federal Bureau of Investigation (FBI)	Office of Professional Responsibility (OPR)
Federal Bureau of Prisons (BOP)	Office of Public Affairs (PAO)
Federal Prison Industries (UNICOR)	Office of the Solicitor General (OSG)
Foreign Claims Settlement Commission (FCSC)	Office on Violence Against Women (OVW)
INTERPOL - United States National Central Bureau (USNCB)	Professional Responsibility Advisory Office (PRAO)
Justice Management Division (JMD)	Tax Division (TAX)
National Drug Intelligence Center (NDIC)	United States Marshals Service (USMS)
National Institute of Corrections	United States Parole Commission (USPC)
National Security Division (NSD)	

The FY2009 DOJ IT Budget of $2.8 billion is allocated by component as follows:



Source: FY2009 DOJ IT Exhibit 53

Appendix F: ACRONYM LIST

Acronym	Definition
APB	Advisory Policy Board
ATF	Bureau of Alcohol, Tobacco, and Firearms
BPA	Blanket Purchase Agreement
BPWG	Business Process Working Group
CCB	Change Control Boards
CDCS	Consolidated Debt Collection System
CIO	Chief Information Officer
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CJIS	Criminal Justice Information Services
COI	Communities of Interest
COOP	Continuity of Operations
CPIC	Capital Planning and Investment Control
CPCLO	Chief Privacy and Civil Liberties Officer
CTISS	Counter Terrorism Information Sharing Standards
DAAB	Department Architecture Advisory Board
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DIRB	Department Investment Review Board
DNI	Director of National Intelligence
DOJ (or Justice Department or Department)	Department of Justice
DOJCERT	Department of Justice Computer Emergency Readiness Team
e-Gov	E-Government
EAPMO	Enterprise Architecture Program Management Office
EAWG	Enterprise Architecture Working Group
ELA	Enterprise Licensing Agreement

Acronym	Definition
EOUSA	Executive Office for United States Attorneys
FIDM	Federated Identity Management
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FTF	Federal Transition Framework
GAC	Global Advisory Committee
GAO	General Accounting Office
GESC	Global Executive Steering Committee
Global	Global Justice Information Sharing Initiative
HSPD-12	Homeland Security Presidential Directive 12
IDEA	Intra-DOJ Information Exchange
IEPD	Information Exchange Package Documentation
IPV6	Internet Protocol Version 6
IRTPA	Intelligence Reform and Terrorism Prevention Act
ISE	Information Sharing Environment
ISSA	DOJ Information Sharing Segment Architecture
IT	Information Technology
ITI LoB	IT Infrastructure Line of Business
ITSP	Information Technology Strategic Plan
JABS	Joint Automated Booking System
JCON	Justice Consolidated Office Network
JMD	Justice Management Division
JRA	Justice Reference Architecture
JSOC	Justice Security Operations Center
JSRA	Justice Secure Remote Access
JUTNET	Justice Unified Telecommunications Network
LAN	Local Area Network
LCMS	Litigation Case Management System
LEA	Law Enforcement Agency

Acronym	Definition
LEISP	Law Enforcement Information Sharing Program
LEO	Law Enforcement On-Line
LEXS	Logical Entity Exchange Specification
LoBs	Lines of Business
MOU	Memorandum of Understanding
N-DEx	National Data Exchange
NBAC	NIEM Business Architecture Committee
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
NPEP	NIEM Priority Exchange Panel
NTAC	NIEM Technical Architecture Committee
O&M	Operations and Maintenance
OCDETF	Organized Crime Drug Enforcement Task Force
OCIO	Office of the Chief Information Officer
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
OneDOJ	Regional Data Exchange (Formerly R-DEx)
OSS	Operational Support Services
PDA	Personal Data [or Digital] Assistant
PIA	Privacy Impact Assessment
PII	Personal identifiable information
R-DEx	Regional Data Exchange (now OneDOJ)
SAR	Suspicious Activity Reporting
SCAP	Security Content Automation Protocol
SIWG	Standard Infrastructure Working Group
SLA	Service Level Agreement
SLT	State, Local, and Tribal
SRM	Service Reference Model
TEDAC	Terrorist Explosive Device Analytical Center

Acronym	Definition
TIC	Trusted Internet Connection
TRM	Technology Reference Model
UFMS	Unified Financial Management System
US-CERT	United States Computer Emergency Readiness Team
VA	Department of Veterans Affairs
WAN	Wide Area Network
WCF	Working Capital Fund
WG	Working Group