2. KEY DRIVERS

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

2.1 Mission-Driven Information Technology

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

Figure 3: DOJ Customers

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

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

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

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

2.2 Federated Organizational Structure

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

Table 2: DOJ FY07 Programs Spending Categorization

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

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

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

2.3 OMB Direction and Government-wide Initiatives

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

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

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

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

2.4 Technology Trends

Technology advances are increasing performance and capability, and lowering costs, at an amazing and compounding rate. A well known fact from Moore's law describes the rapidly continuing advance in computing power per unit cost, approximately doubling every eighteen months. Retail price/performance for consumer telecommunications, computing, and electronics has been following a similar path. Something that is less well understood but as transformative is the availability today of reliable and secure computing, data storage, data communications, and

specific computing (web) services at very low and compelling pay-per-use rates. Further, the use of Internet-based standards for these services means that the cost to integrate is low and increasingly supported in vendor products and services.

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

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

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

2.5 Upholding the Public Trust

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

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

within the overall DOJ framework as outlined in the Enterprise Architecture to promote consolidation, standardization, and alignment with strategy.

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

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

2.6 Financial Challenges

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

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

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

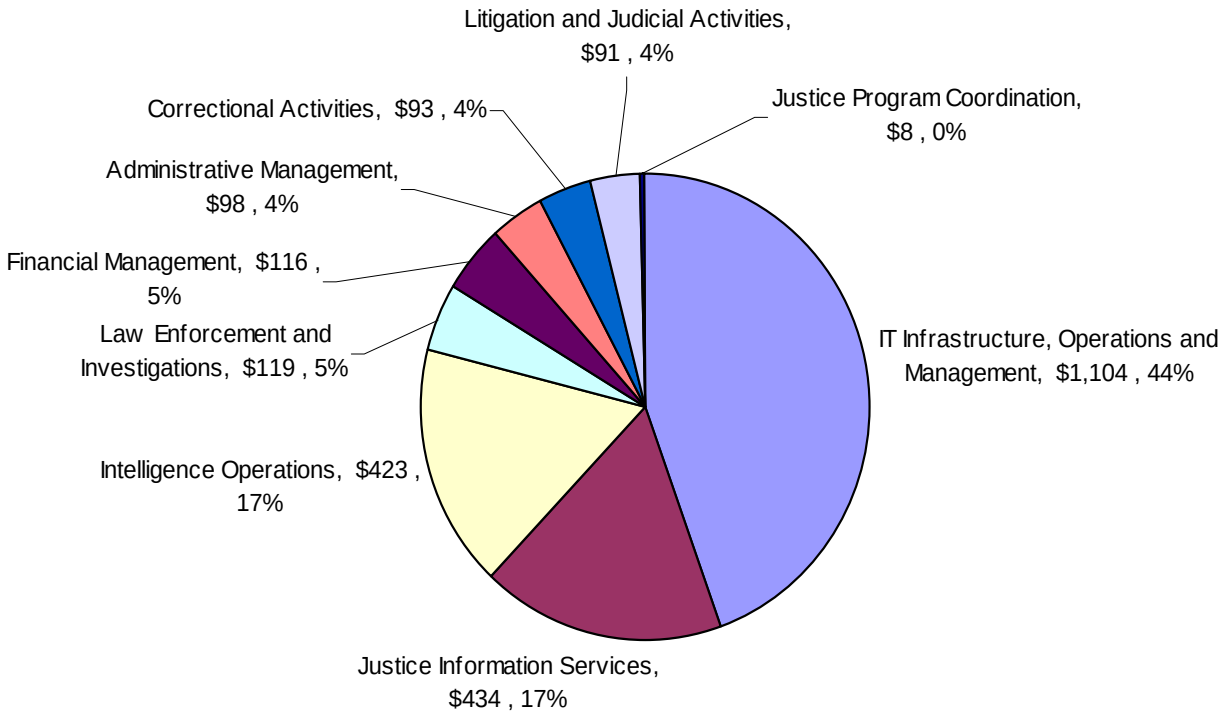

Figure 4: FY07 DOJ IT Budget Allocation by Segment ($2.486 Billion)