# 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.

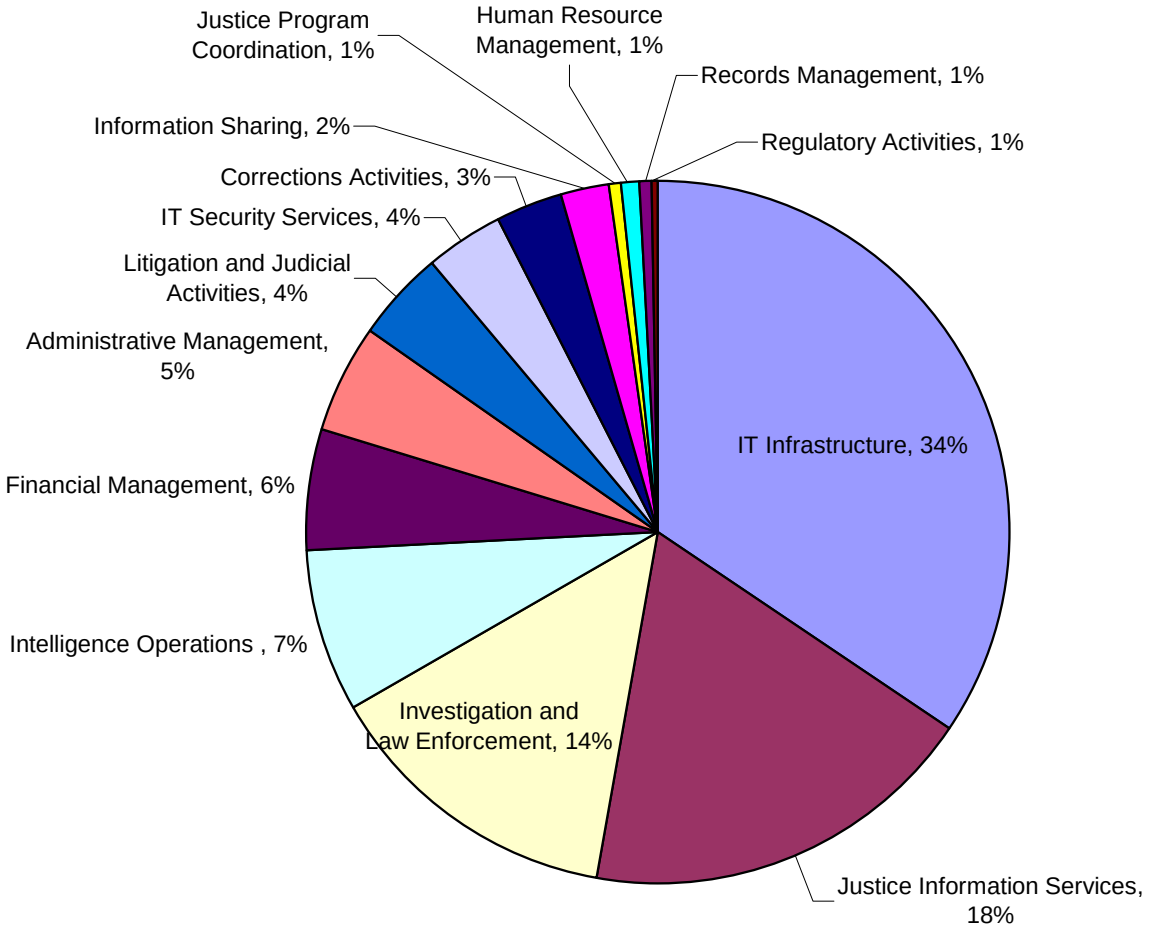


**Figure 2-2: FY09 DOJ IT Budget Allocation by Segment**

[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.