Table of Contents

Introduction 1

Overview of the Department of Justice 1

The Need for Change 4

Meeting New Mission Requirements....4
Achieving Improved Performance....6

Vision and Goals 7

IT Infrastructure 8

Strategic Initiative: *Develop the infrastructure architecture layer of the DOJ enterprise architecture*....10
Strategic Initiative: *Provide a single, national data network*....10

Information Security 12

Strategic Initiative: *Strengthen and improve the DOJ information security program*....13
Strategic Initiative: *Design and implement a DOJ Public Key Infrastructure (PKI)*....15

Common Solutions 16

Strategic Initiative: *Create a blueprint for common solutions*....17
Strategic Initiative: *Develop and implement "e gov" plan*....20

Management Roles and Processes 22

Leadership Role of the CIO....22
Strategic Initiative: *Establish and implement an ongoing, collaborative strategic planning process*....23
Strategic Initiative: *Establish, refine, and implement DOJ IT policies, processes, and standards*....23
Strategic Initiative: *Continue to develop, refine, and implement a DOJ enterprise architecture*....24
Strategic Initiative: *Develop and implement an IT human capital plan*....26
Strategic Initiative: *Establish and implement improved investment management processes and practices*....27
Strategic Initiative: *Improve project management*....28

Summary of Strategic Initiatives and Next Steps **29**

Critical Success Factors **31**

Appendices

A. Statutory Framework for Managing IT
B. The Prospects for Technology Insertion
C. Department of Justice Infrastructure Strategy
D. Department of Justice Telecommunications Strategy
E. Public Key Infrastructure at the Department of Justice
F. Segment Architecture of the Law Enforcement Booking Process

Introduction

In the aftermath of the attacks of September 11, 2001, protecting Americans against threats of terrorism is the foremost challenge facing the Department of Justice (DOJ). Meeting this challenge - - and effectively and efficiently carrying out our responsibilities to the American people - - demands that the Department successfully exploit the transformative power of information technology to further the accomplishment of its mission.

This Information Technology Strategic Plan outlines how the Department is strengthening and refocusing its information technology program to meet the Department's new counter terrorism mission and support the achievement of its strategic goals. It describes the Department's IT vision and goals; sets forth new initiatives to upgrade infrastructure, improve security, and develop common IT solutions; and summarizes the underlying principles and general approach by which we will plan for and manage our IT resources.

This document is an initial version of the Department's Information Technology Strategic Plan. Although it provides overall direction, it is admittedly limited in scope and detail. Future versions will build on this initial effort as part of an ongoing, iterative, and collaborative strategic planning process involving the Department's component organizations.

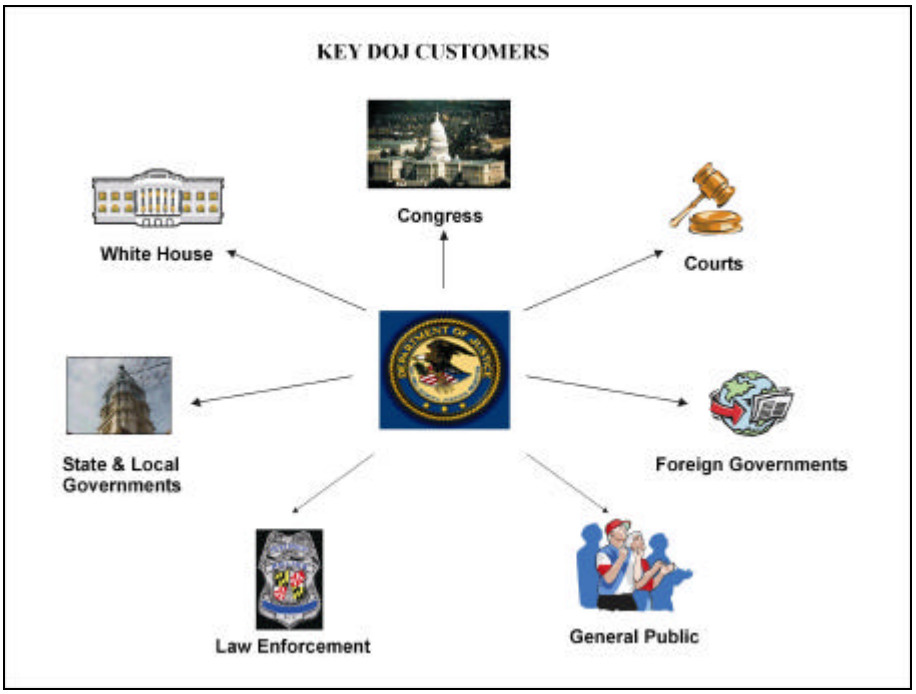
Overview of the Department of Justice

The Department of Justice is headed by the Attorney General of the United States. Its major component organizations include: the U.S. Attorneys (USAs) who prosecute federal offenders and represent the United States in court; the major investigative agencies - -the Federal Bureau of Investigation (FBI) and the Drug Enforcement Administration (DEA) - - which gather intelligence, investigate crimes, and arrest criminal suspects; the Immigration and Naturalization Service (INS) which controls the border and provides services to lawful immigrants; the U.S. Marshals Service (USMS) which protects the federal judiciary, apprehends fugitives, and detains persons in federal custody; and the Bureau of Prisons

(BOP) which confines convicted offenders.* Two components - - the Office of Justice Programs (OJP) and the Office of Community Oriented Policing Services (COPS) - - focus on providing grants and other assistance to state and local governments and community groups to support criminal and juvenile justice improvements.

The Department's varied and complex responsibilities involve myriad relationships and interactions with external entities, as illustrated in Figure 1.

Figure 1



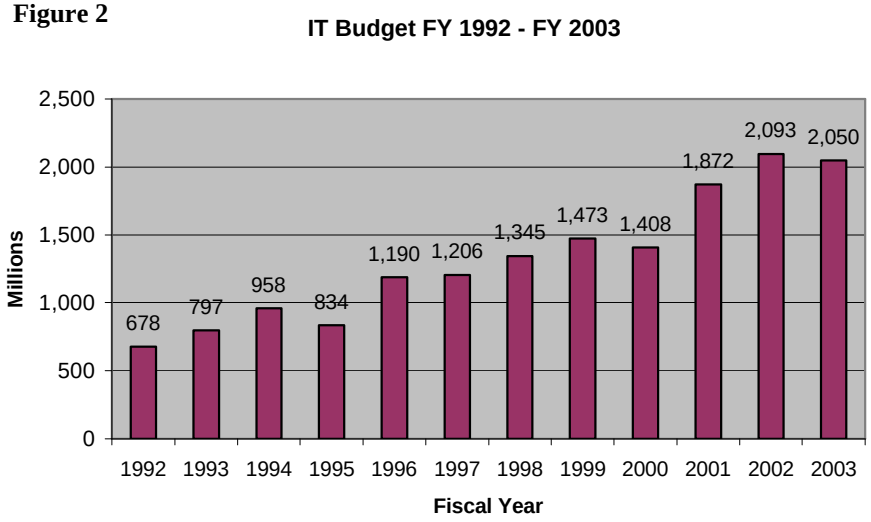
More than 130,000 persons are employed by the Department - - as attorneys, criminal investigators, border patrol agents, immigration inspectors, corrections officers, or any one of a host of other occupations. Although the Department is headquartered in Washington, D.C., most personnel work at locations outside Washington that range from one-or two person Border Patrol stations in sparsely populated regions to major metropolitan field offices. In addition to these domestic field locations, the Department has a number of personnel stationed at offices located in countries around the world.

* In June 2002, the President's called for the creation of a new Department of Homeland Security. Under the President's proposal, the INS would be transferred from Justice to the new department.

About 3,700 persons (3 percent of the total workforce) hold IT positions. However, contracts for IT services supplement career staff at a level roughly equivalent to 3,600 full time employees.

The Department currently spends slightly more than $2 billion on IT annually (see figure 2). Historically, IT spending has been a fairly constant 6-8 percent of the total DOJ budget.

Figure 2



The Department maintains four enterprise data centers that provide centrally operated and managed computing resources. These data centers offer high availability through the use of mainframe computers maintained by around-the-clock staff. The Department also maintains several communications networks, both classified and sensitive but unclassified (SBU). One of these, the Criminal Justice Information System (CJIS), supports federal, state, and local access to major databases such as the National Crime Information Center (NCIC) and the Integrated Automated Fingerprint Information System (IAFIS).

There are over 250 information systems, most of which are legacy systems developed and maintained by the component organizations to meet particular business needs. These systems range from small applications designed to track particular transactions to large-scale efforts such as the FBI's office automation modernization effort, TRILOGY. In recent years there has been some movement toward integrated and common systems. For example, the Joint Automated Booking System (JABS) maintains a core set of shared data elements used by departmental components that are involved in the booking of persons in federal custody.

The Need For Change

Meeting New Mission Requirements

On November 8, 2001, Attorney General John Ashcroft released the Department of Justice Strategic Plan for Fiscal Years 2001-2006. The Plan charts a new direction and lays out new priorities in the wake of the terrorist attacks of September 11, 2001. Preventing terrorism and bringing its perpetrators to justice is now, in the words of the Attorney General, "the first and overriding priority of the Department of Justice."

The Strategic Plan revises the Department's formal mission statement to emphasize the Department's role in deterring, preventing, and responding to terrorism. The revised mission statement reads as follows:

> "…to enforce the law and defend the interests of the United States according to the law; *to ensure public safety against threats foreign and domestic*; to provide federal leadership in preventing and controlling crime; to seek just punishment for those guilty of unlawful behavior; to administer and enforce the Nation's immigration laws fairly and effectively; and to ensure fair and impartial administration of justice for all Americans." (*emphasis added*)

The Strategic Plan reflects the realities of our post-September 11 world. Today, the United States increasingly faces new and diffuse 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) means in order 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 changed threat environment, the potential for harm has increased exponentially, new vulnerabilities have been exposed, and traditional law enforcement responses have proved inadequate.

To combat these threats effectively, the Department of Justice 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, state and local partners and cooperating foreign governments. Organizationally, it must be streamlined, agile, and technologically proficient.

The Strategic Plan identifies eight overarching strategic goals the Department will pursue in support of its new mission. In keeping with its priority status, the first goal is to "protect America against the threat of terrorism." Other strategic goals include:

- Enforce federal criminal laws.
- Prevent and reduce crime and violence by assisting state, tribal, local and community-based programs.
- Protect the rights and interests of the American people by legal representation, enforcement of federal laws, and defense of U.S. interests.
- Fairly and effectively administer the immigration and naturalization laws of the United States.
- Protect American society by providing for the safe, secure, and humane confinement of persons in federal custody.
- Protect the federal judiciary and provide critical support to the federal justice system to ensure it operates effectively.
- Ensure professionalism, excellence, accountability, and integrity in the management and conduct of Department of Justice activities and programs.

Information technology is key to the Department's success in meeting these strategic goals. It is a vital organizational asset that must be strategically deployed and utilized and 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; identify and prevent persons who are national security threats from entering the United States; better ensure compliance with the nation's immigration laws; securely share information with our federal, state, and local partners; efficiently manage our criminal and civil cases; provide accessible, speedy, and reliable services to our customers; and efficiently and effectively carryout our internal business practices. In addition, information technology

provides the communications and computing infrastructure that ensures continuity of operations and rapid response in times of crisis.

Achieving Improved Performance

Compounding the need to meet new mission requirements is the need to improve IT programs and services and obtain greater value from our IT investments. Members of Congress, leaders of the Executive Branch, oversight agencies, internal and external customers, among others, are rightfully demanding higher levels of performance.

Over the past several years, the Congress has enacted legislation that provides a broad statutory framework governing the management of IT in the Federal Government (see Appendix A). The centerpiece of this legislation is the Clinger-Cohen Act of 1996 (CCA), which requires federal agencies to follow a structured and rigorous approach in selecting, controlling, and evaluating IT projects. CCA specifically mandates that agencies appoint chief information officers (CIOs), implement a capital planning and investment control process, develop and maintain an information technology architecture, establish IT performance measures, and develop strategies for improving information resources management capabilities. Overall, it is clear that the Congress expects agencies to:

- Implement systematic planning and investment management processes in order to maximize the value and minimize the risks of IT investments;

- Adopt a results and performance based management approach; and

- Ensure the privacy and security of IT systems.

The Department has made significant progress in implementing the requirements of Clinger-Cohen and related legislation. Nevertheless, it is clear that much more needs to be done to fully comply with these requirements and meet congressional expectations regarding the Department's performance.

The effective use of IT is also central to the Administration's management agenda. Under the umbrella of electronic government ("e gov"), the Administration is sponsoring a series of initiatives to provide citizens and businesses easier and more timely access to government information and services, reduce paperwork, decrease

duplication of effort and cost, and improve interagency and intergovernmental information sharing. It has made IT funding contingent, at least in part, on consistency with an overall enterprise architecture, effective capital planning and investment control, and improved IT security.

Oversight groups, including both the General Accounting Office (GAO) and the Department's Office of the Inspector General (IG), are closely monitoring the performance of the Department's IT program. The IG has identified IT planning and implementation and IT security as two of the ten top management challenges facing the Department. Both the IG and the GAO have issued a series of reports citing various deficiencies in IT management and performance. Information security has been a primary focus of criticism by not only the GAO and IG, but also by congressional oversight committees and groups such as the Webster Commission.

The Attorney General has also voiced his expectation that the Department do more to effectively utilize IT, secure its IT systems, and increase information sharing. Perhaps the greatest force for change, however, is simply the pressing day-to-day needs of the investigators, attorneys, border patrol agents, immigration inspectors, state and local law enforcement officers, and others who are in the front lines in the war on terrorism and who must rely on information technology to do their jobs effectively.

Vision and Goals

The Department's vision is that

> *"…IT will be a cohesive, forward-leaning enabler of enhanced DOJ mission accomplishment."*

This vision implies a fundamental reorientation of the role of IT within the Department of Justice. The vision shifts the paradigm. IT will no longer be simply a support service, but rather an active catalyst for change and a direct contributor to mission accomplishment. IT will no longer be largely decentralized, but rather an integrated, cohesive endeavor that builds on shared mission requirements and fosters a collaborative management environment. IT will no longer be only reactive, matching technology to an identified business need, but also proactive,

looking to how new and emerging technologies may be applied in support of the DOJ mission. (See Appendix B, *The Prospects for Technology Insertion*, for a discussion of how DOJ could approach the adoption of new technologies.)

The Department has established four broad IT goals:

1. Share information quickly, easily and appropriately- - inside and outside the DOJ

2. Secure and protect information

3. Provide reliable, trusted, and cost-effective IT services

4. Use IT to improve program effectiveness and performance.

To meet these goals, the Department is initially focusing on four key areas: IT infrastructure; information security; common solutions; and management roles and processes. These four areas have been chosen because, together, they constitute the core building blocks of the Department's IT program. In addition, they are areas where there are both significant problems and significant opportunities for improvement. The next sections of this Plan outline these areas and present specific initiatives for action.

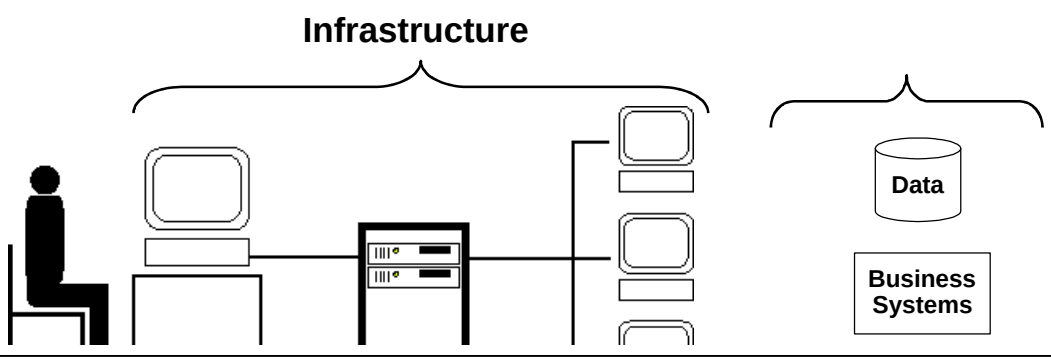
IT Infrastructure

The Department's capability to share information with people, organizations, and countries around the world begins with a unified and modernized infrastructure that is cost effective, reliable, accessible, interoperable, and secure. Currently, the Department's infrastructure is largely decentralized, fragmented, and outdated. It is essentially an amalgamation of infrastructures designed, developed and maintained by individual components to meet their specific needs. This approach has introduced an unnecessary level of complexity, cost, and risk, and inadvertently created technical barriers to sharing information. (For further discussion of the DOJ infrastructure strategy, see Appendix C.)

IT infrastructure is a broad term that includes equipment, networks, and general-purpose software. Specifically, infrastructure is a layering of selected services, physical products, and telecommunications technologies as a foundation for building

systems and sharing information. Users call on the capabilities of the infrastructure every day whenever an email is sent, a document is prepared, or a database is accessed to retrieve information. In short, the infrastructure is like a "black box" that sits between the user and information resource (see Figure 3).

Figure 3



Core infrastructure elements include:

- **Workstations**. The DOJ supports both desktop and mobile or laptop computing to provide productivity tools such as word processing, spreadsheets, and email. Some components have a standard desktop configuration, such as the Justice Consolidated Office Network (JCON). Other components support a more heterogeneous desktop environment.

- **Mainframes**. A mainframe is an enterprise computer with powerful processing and data storage capabilities. The DOJ mainframes support many computing models - - centralized, distributed, and client-server. In the client-server model, the mainframe is used as a server. Mainframes are versatile, scalable and stable and an important element of the DOJ infrastructure.

- **Servers**. A server is a shared resource - - a microcomputer, a minicomputer or even a mainframe - - supporting distributed computing on a local or wide area network. It is distinct from central computing because processing is split between the server and the workstation. The DOJ environment supports many different kinds of servers including application servers, communications servers, and Windows NT servers.

- **Networks**. The DOJ currently supports voice, data, and video networks. The data networks, connecting personal computers and other computer resources, include multiple local area networks (LANS), wide area networks (WANs), and a metropolitan area network (MAN) in Washington, D.C.

- **Remote Computing**. Remote computing refers to providing access to the DOJ network by users who do not have standard desktop access. Some remote users carry their computing environment with them on a laptop; other remote users access the network from a single location, such as their home. In all cases, these users require a level of performance equal to that available from the standard on-site desktop.

Strategic Initiative: *Develop the infrastructure architecture layer of the DOJ enterprise architecture*

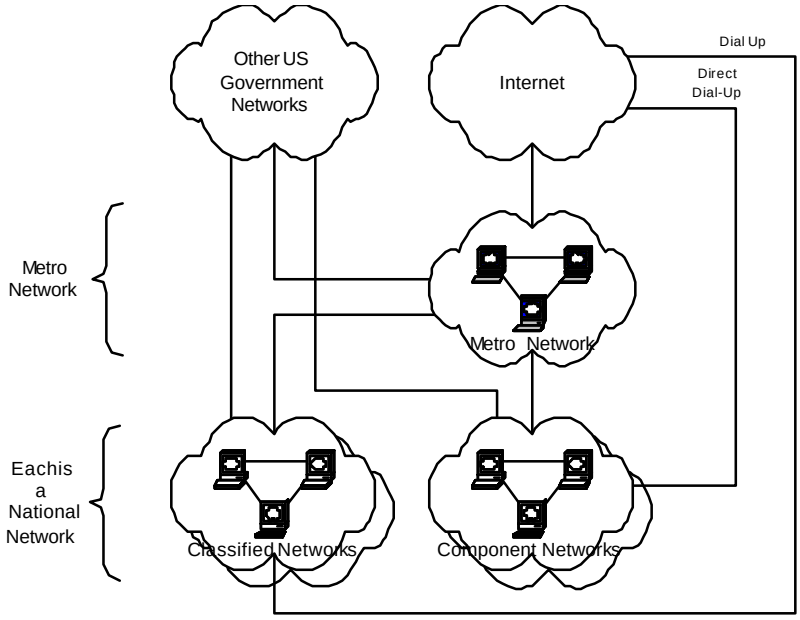
The Department will work with the components to develop a department wide infrastructure architecture - - a layer of the Department's overall enterprise architecture. The infrastructure architecture will provide a common conceptual framework to support technical interoperability, define a common DOJ vocabulary, and provide a high-level description of the information technology deployed throughout the Department. It will also define technical standards for acquiring and managing the infrastructure department wide. These standards will be documented in an updated Technical Reference Model. One of the next steps will be to define the guiding principles for infrastructure architecture, the scope of the DOJ wide initiative, and the information needed to effectively coordinate infrastructure technology in support of information sharing.

Strategic Initiative: *Provide a single, national data network*

Telecommunications is a pivotal part of any infrastructure and an essential tool for enabling information sharing. The DOJ operates data networks, conventional voice networks, and wireless networks that include cell phones, radios, and data devices such as Personal Digital Assistants. The DOJ mission requires us to communicate classified and unclassified information securely among components and between components and external private and

public organizations. Figure 4 below depicts our current network environment.

Figure 4



As illustrated above, the DOJ network environment is an aggregation of a number of independent, national networks developed and operated by each of the major DOJ components. The MAN (operated by the Justice Management Division) provides transit for network traffic exchanged among DOJ components; common services such as an e-mail translation service, a gateway to the Internet, and external web servers; and access to shared data centers. This component-driven design tends to inhibit DOJ wide data sharing and lead to numerous direct connections to internal and external networks that bypass the MAN. Each of these additional points of interconnection with the Internet or other external network introduces added complexity, security risks, and costs to the overall DOJ data network configuration.

The Justice Consolidated Network (JCN) was originally conceived to promote information sharing while minimizing total DOJ costs for data network services. Conceptually, the JCN is a reseller of Sprint's national ATM backbone – a public network that carries non-DOJ and non-US Government traffic. The JCN also provides value-added services: a network operations center, managed network services (e.g., configuration and operation of network elements used to construct a DOJ component's network), and customer premises equipment for traffic aggregation. Today, JCN

services about two-thirds of all of the unclassified network locations, but cost savings have been marginal and components continue to share data primarily through file extracts governed by written agreements.

A key element of the Department's IT strategy is to replace the JCN and other separate data networks with one, new integrated network. This new DOJ data network will be designed to meet the collective needs of the DOJ components. It will continue to be based on the TCP/IP protocols, since this is the dominant industry standard for all applications, operating systems platforms, and network equipment. It will emphasize promoting information sharing, providing enhanced security across the board, and ensuring continuity of network operations. It will be viewed as a Department utility that serves *all* DOJ components. Service level agreements will be employed to assure that the supplier's network management services meet *all* DOJ requirements. (For more information on the DOJ telecommunications strategy, see Appendix D.)

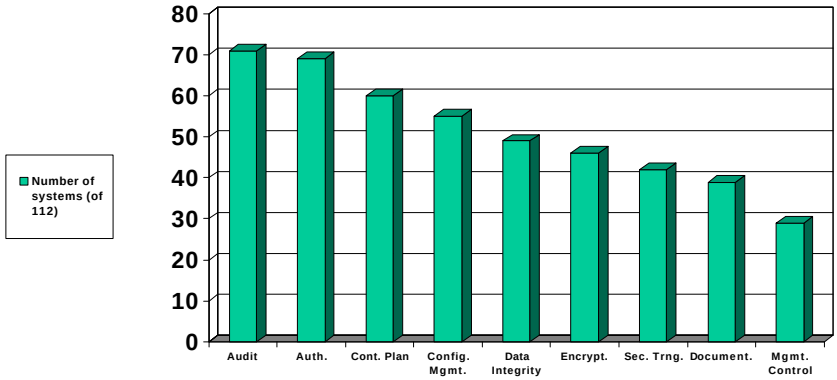
Information Security

Increasingly interconnected information technology systems and networks are critical to achieving the Department's mission. However, this widespread interconnectivity also poses new risks. Our growing dependency on these systems for law enforcement and national security purposes has increased the potential damage resulting from malicious attacks that undermine and disrupt services or expose sensitive information to misuse. Protecting our IT systems and networks and safeguarding the information they store, process, and transmit, is a cornerstone of the Department's IT strategy. Information security is an indispensable function and a prerequisite to meeting our IT and mission goals.

The Department has established minimum requirements for ensuring the security of the Department's classified and SBU systems and networks, including the requirement that all systems and networks be "certified and accredited" before becoming operational and re-certified and accredited periodically thereafter. These certification and accreditation activities, along with penetration tests, audits, and reviews, have identified a number of security weaknesses. The Department's Security Report for 2001 concluded that more than half of the 112 systems analyzed had

vulnerabilities in the areas of audit, authentication, contingency planning, and configuration management (see Figure 5).

Figure 5



High profile cases such as that of convicted spy Robert Hanssen have further illustrated glaring weaknesses in security policies and controls. Not surprisingly, congressional oversight committees, the GAO, and the IG, have all targeted information security as a major management concern within the Department.

To address this concern, the Department is implementing a multi-pronged strategy for strengthening and improving its information security program so that identified weaknesses are corrected and lasting and fundamental improvements are achieved.

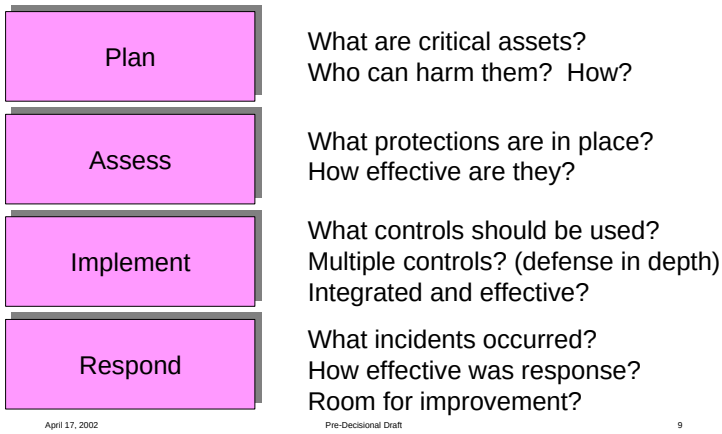
Strategic Initiative: *Strengthen and improve the DOJ information security program*

Assign High Level Responsibility

Information security is primarily a management function that requires the sustained commitment and attention of high-level officials at the Department and component levels. To this end, the Department's IT security function will be elevated and strengthened. A senior management official, reporting directly to the Department's CIO, will be assigned overall responsibility for ensuring that the Department takes a department wide strategic view of its information security program and developing and implementing a coordinated and effective IT security program that is continuous, iterative, and fully integrated with IT architecture

and investment processes. The program will involve four major activities: planning to ascertain threats and trust relationships; assessing the current levels of protection and their effectiveness; implementing and integrating controls; and responding to incidents, as shown in Figure 6.

Figure 6



Focus on Fixing Most Pressing Problems

The Department has developed a centralized database for tracking the remediation of security weaknesses. This database is a single repository of findings and corrective actions identified through the component certification and accreditation activities, IG audits, penetration testing, and other reviews (including the self-assessments required under the Government Information Security Reform Act).

The Department will continue to use this database to help prioritize and monitor the implementation of corrective actions. It will also increase its monitoring of compliance with departmental policy and ensure that costs for security are identified in IT capital plans. At the same time, it will continue to explore department wide solutions to cross-cutting problems. For example, the Department is implementing a common web-based security education and awareness program, available to all Department users.

Develop a Security Architecture

A number of Justice components are looking to various technology solutions to improve the security of their IT systems. However, there is no overall departmental approach or architecture to guide

these efforts. As a result, these perceived solutions may simply offer an isolated and patchwork response and not an integrated and comprehensive defense.

To remedy this situation, the Department will develop a security architecture, employing a "defense in depth" model, consistent and integrated with the Department's overall enterprise architecture. The architecture will identify baseline and future security policies, standards and technologies. It will enable the Department and the components to better identify cross cutting security needs and possible common solutions, and eliminate inconsistent security approaches. The security architecture and policies will continually evolve in support of the security process. The process will contribute to their growth and change, and the continual analysis of the architecture and policies will suggest changes to the process.

Implement Common Security Tools

Today's emerging security technology enables a level of protection that only a few years ago was not achievable at any cost. For example, network based authentication and auditing tools are able to prevent and detect unauthorized access and use. Virtual private network (VPN) technologies improve boundary protection by funneling traffic through strong, professionally managed gates. The Department will focus on identifying and implementing common automated security tools, consistent with the Department's overall security architecture. The use of common security tools reduces costs and duplication of effort. It also helps to ensure a standard level of protection throughout the Department.

Strategic Initiative: *Design and implement a DOJ Public Key Infrastructure (PKI)*

Public key technology provides enhanced capability to protect the confidentiality, integrity, and authenticity of electronic information. It offers a uniform way to identify system users, encrypt protected information, and restrict access based on "certificates of trust." This technology relies on the use of two discreet keys - - a public key and a private key - - that, working together, implement cryptographic services, secure hashes, and digital signatures. The private keys are safeguarded by the person who will sign or decrypt the messages. The public keys are made available to other users to verify the signatures or encrypt documents. Since the public keys are made available to all users, a

certificate mechanism must be established to ensure that the keys are valid and associated with a particular individual.

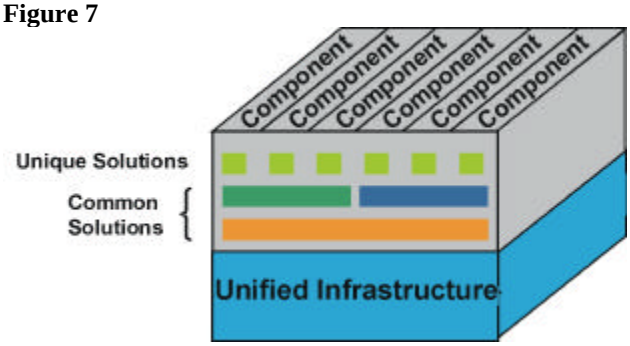
PKI is considered to be an important element in improving secure information sharing and implementing "e gov." The Federal Government, under the auspices of the OMB, has formed a federal PKI Steering Committee to lay the groundwork for government-wide use of PKI. In addition, several DOJ components have taken steps to implement their own PKI initiatives in response to their own particular requirements.

The Department will develop and implement a department wide PKI that will enable secure communications and information sharing across component organizational boundaries, provide a strong authentication mechanism department wide, support "e gov" initiatives, and establish a framework for communications and sharing with other federal, state and local agencies. A department wide PKI effort will ensure consistency in approach, minimize duplication of effort, and reduce requirements for cross component verification and validation. It will also provide a central point of contact for linking with the federal bridge. This link will allow cross certification of certificates with individuals from other federal agencies, foreign governments, state and agencies, and the private sector. (For additional information, see Appendix E, *Public Key Infrastructure at the Department of Justice*.)

Common Solutions

From a mission perspective, the most important benefits of information technology arise from its ability to enable and improve collaboration, secure information sharing, and work simplification. Common solutions help to achieve these goals through the use of shared applications and databases. Developing and implementing common solutions, where appropriate, is an important element of our IT strategy and represents a fundamental shift in approach. Although there will continue to be a need for unique applications that support a single component, the emphasis will be on migrating toward common solutions that cross component organizational boundaries (see Figure 7).

Figure 7



Strategic Initiative: *Create a blueprint for common solutions*

Common solutions reduce total costs, promote information sharing, improve information integrity, and accelerate business change cycles. Going forward, the DOJ wants to exploit common solutions wherever practical. Common solutions are application systems and databases used by more than one component. DOJ components will use a combination of common solutions and unique systems.

The DOJ has made a strong start in the direction of common solutions with projects such as JABS, which shares a database, and the planned Unified Financial Management System, which will deploy shared applications. The new Entry-Exit System is another example of a common solution. It will provide Justice components and other government agencies access to a shared database on foreign nationals entering, or seeking to enter, the United States, and will substantially improve our capability to fight terrorism and enforce the immigration laws.

However, there are many other potential opportunities where business processes transcend organizational boundaries, make use of identical or similar data, or utilize similar technologies. The table below lists areas where common solutions are currently being implemented or might be candidates for future consideration.

Common Solution	Components
Joint Automated Booking System	BOP, DEA, FBI, INS, JMD, USMS
Common Financial Systems	All components
Entry-Exit System	FBI, INS, Departments of State and Commerce, others …
E-Government	JMD, OJP, others …
Data Warehousing/Mining	All or most components
Collaboration Tools	All or most components, external public and private entities
Case Management	DEA, EOUSA, FBI, INS, others …
Human Resources	All components
Prisoner/Detainee Management	BOP, INS, ODT, USMS, others …
Other Candidates …	

Under the leadership of the Department's CIO and in collaboration with the components, the Department will develop a blueprint for assessing, selecting, scoping, and sequencing common solution projects. The transition from today's stovepipe environment to a more integrated and unified one, will require careful planning, in concert with enterprise architecture and investment management, and the forging of a strong partnership between IT and business process owners.

Advocate Shared Information

Common solutions share information through a shared database or the use of a common business system(s). Information sharing also occurs through the reuse of information and business systems, whenever possible and appropriate. Most importantly, common solutions, with shared data and applications, foster a self-regulating data quality program. Shared information is collected once, at the source, then reused and updated by many users according to established access privileges and procedures.

However, common solutions also introduce change and require substantial multi-year investments. IT investments in common solutions integrate different views of the same information - information that is similar, but not the same. Too often, they fail to

realize expected benefits because projects are not properly scoped and funded or do not align with program managers' expectations. The CIO will assure that common solutions projects are selected to align with business strategies and priorities, sequenced to take best advantage of technical capabilities, and given the needed project management resources. Business representatives will participate on project teams to ensure that transformed views of previously stove-piped information and systems meet the specifications for shared information and that the new information systems are deployed on schedule to realize expected benefits.

Redesign Work Processes

Business process reengineering (BPR) should drive common solution requirements and the supporting business case. A strong business change mandate and champion must exist where IT can be an enabler or catalyst. Major IT projects are substantial dollar investments and usually support a business change, not just business as usual. In many cases, the economic benefits, measured as return on the capital being invested, only can be realized through some combination of change or transformation within the business operation as well as IT.

Enterprise architecture models help identify opportunities for developing common solutions and eliminating redundancies. The deployment of a unified network enables cost-effective communications between people and organizations inside and outside the DOJ and common access to shared databases. These new capabilities challenge the assumptions about technology, people, and organizational goals that are inherent in current work processes across the Department. By using BPR methods and tools, the Department and components together can work toward common solutions by defining "end-to-end processes" that are measured by the product or service produced rather than by how well one activity within the process is performed.

Accelerate Change Cycles

The introduction of common solutions will create change – changes in the information resource, changes in the business process, changes in the technology, and changes in operational procedures. Components have different levels of IT resources and needs – and the impact of introducing common solutions will be different for each component. However, because common solutions are driven by the strategic business need to share

information and respond quickly to internal and external information needs, the Department must find ways to accelerate the development and implementation of common solutions in day-to-day business operations.

Major IT projects should not be launched without an effective business partnership that includes business executive sponsorship and buy-in to the overall change proposition, including the benefits to be achieved by the business operation. To be successful, core requirements need to be standardized while accommodating important flexibility. Adapting or changing existing component operations and/or organizations may be necessary to implement a common solution. If scope is not managed within the core set of requirements, then leverage and cost advantages may erode or disappear.

Under the leadership of the CIO, the Department will create and maintain a portfolio of common solutions. Through portfolio management, the DOJ will ensure that common solutions are selected managed, and evaluated to meet business needs, are consistent with the DOJ enterprise architecture, and follow the IT investment management policy. The organizational, funding, and project management responsibility for developing and implementing common solutions projects will rest with the most qualified or experienced component(s).

Taking advantage of common solution opportunities will require that common IT infrastructure and standards play even larger roles in the future. Network access and other technology will need to facilitate, not inhibit, fast and secure connectivity and communication across DOJ.

Strategic Initiative: *Develop and implement "e gov" plan*

As noted earlier, "e gov" is a central element of the Administration's management agenda and its objectives of improved information sharing, increased efficiency, and more citizen-centric services. Aggressive implementation of "e gov" is a priority. A multi-year "e gov" implementation plan will be developed and integrated into the Department's overall enterprise architecture. Essential building blocks for the Department's "e gov" efforts will include effectively implementing the requirements of the Government Paperwork Elimination Act (GPEA), participating in the Administration's "e gov" initiatives,

and improving the Department's web presence. Each of these is described briefly below.

Accelerate Implementation of GPEA Plans

The essence of GPEA is to provide citizens, businesses, and governmental agencies the option of conducting business with the Federal Government through electronic means. Implicit within GPEA is transforming business processes to make them faster, more efficient, and more citizen and user centric.

The Department has a myriad of responsibilities that require us to provide information to or collect data from individuals, businesses, and other public and private entities. The majority of these information transactions can and should be accomplished Aon-line." Under GPEA, the Department has developed a plan for converting these information transactions to electronic media. However, progress in implementing these plans has been slow. The CIO, working with the components, will develop and implement an approach to accelerate the implementation of these plans.

Participate in E gov Initiatives

The Department of Justice currently is participating in a number of the priority "e gov" initiatives identified by the Administration. Under the leadership of the CIO, the Department will continue and enhance its participation on joint projects such as SAFECOM as well as others related to the Department's mission. Active Justice participation in these initiatives will help break down organizational barriers, reduce costs, and improve information sharing.

Improve Web Presence

A comprehensive but easy to navigate Internet world wide web site is a prerequisite for providing information and services to individual citizens and public and private entities, including state and local governments, the media, schools, community groups, and others. The Department is committed to making its web site a powerful tool for acquiring information, assistance, and services by improving the site organization and search tools, adding dynamic and substantive content, and making it easier for Department components to publish and manage content. Starting in FY 2002,

the office of the CIO will initiate a three-phase web site upgrade to accomplish these goals.

Management Roles and Processes

Leadership Role of the CIO

Achieving our IT vision presents a formidable challenge. It will be a multi-year effort requiring a strong and unified leadership team, skilled personnel, and adequate funding.

In March 2002, the Attorney General selected a new Department CIO with a strong mandate to provide department wide leadership in the IT arena, ensure that the Department makes effective use of IT in its war against terrorism, and upgrade the Department's IT capabilities and services. The CIO reports to and advises the Attorney General on the Department's IT portfolio and budget and other IT matters of departmental interest.

To carry out the Attorney General's mandate, the Department CIO has several major responsibilities. Among these are: promulgating departmental IT policies, processes, and standards; formulating departmental IT strategic plans; developing, implementing, and maintaining an enterprise architecture; developing guidance for, reviewing, and making recommendations concerning, component IT budget requests; reviewing and monitoring the design and implementation of major IT projects; and providing shared departmental services. In executing these responsibilities, the CIO will work to ensure that the various processes by which the Department manages its IT resources (e.g., strategic planning, architecture, investment management) constitute a coordinated and integrated whole.

The Department CIO will also work closely and collaboratively with the Justice components. Only by working together can we effectively leverage our collective capabilities and resources, minimize duplication, improve efficiency and effectiveness, and ensure consistency of practices. Strengthening our IT program requires a team effort where there is not only a unifying vision, but also complementary organizational roles, a willingness to share knowledge and expertise, and an openness to change.

Strategic Initiative: *Establish and implement an ongoing, collaborative strategic planning process*

IT strategic planning, if it is to be effective, must be a dynamic, ongoing effort. Ideally, it should not only provide an overarching framework for guiding and linking multiple and diverse activities, but also a structured means for looking ahead and anticipating new opportunities and requirements. It should also be an inclusive effort that involves both the providers and customers of IT services throughout the Department.

As noted earlier, this Strategic Plan provides general direction but is admittedly limited in scope and detail. Under the leadership of the Department's CIO, a strategic planning process will be developed and implemented that is collaborative, continuous, and substantive. This process will produce future iterations of the strategic plan, each complementing and building on the other, and, over time, will evolve, mature, and be fully integrated with other core planning and management processes of the Department.

Strategic Initiative: *Establish, refine, and implement DOJ IT policies, processes, and standards*

The CIO is responsible for establishing, refining, and overseeing the implementation of department wide IT policies, processes, and standards. The aim is to establish a more comprehensive and uniform department wide framework to guide IT planning and management and promote an integrated and standards-based IT program.

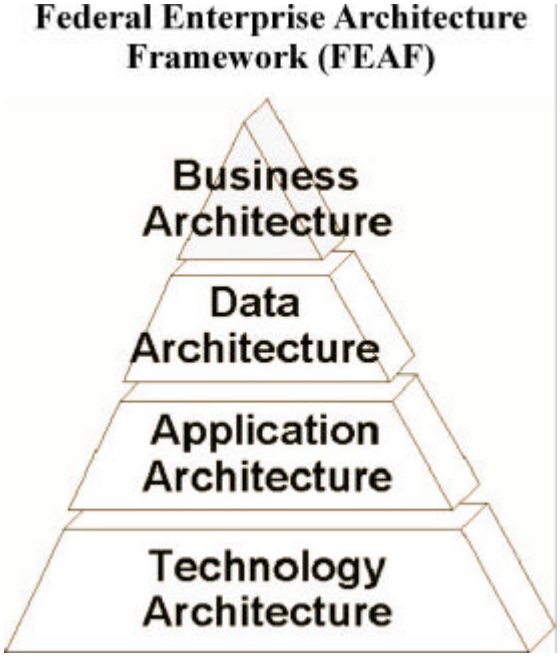
Working with the components, the Department's CIO will lead an effort to review and revise, as necessary, the existing set of policies, processes, and standards and to identify areas where new policies, processes, or standards should be developed. Initial efforts are likely to focus on developing more complete and specific security policy, providing greater uniformity in core processes (such as investment management) and refining the technical standards contained in the Department's Technical Reference Model. The components will continue to be responsible for augmenting departmental policies, processes, and standards, as appropriate.

Strategic Initiative: *Continue to develop, refine, and implement a DOJ enterprise architecture*

An enterprise architecture (EA) is the explicit description and documentation of the current and desired relationships among business and management processes and IT. It describes the "current architecture" and the "target architecture" and provides a gap analysis and transition plan. An enterprise architecture is intended to reduce redundancy in databases, hardware, and software; leverage existing IT investments; develop a consistent, standards-based framework for future investments; promote interoperability and resource and data sharing; and ensure that IT is properly aligned with core business functions.

The Department has adopted the Federal Enterprise Architecture Framework (see Figure 8) for its architecture and developed initial versions of its current architecture for the business, data, and applications levels. Development of the technology (infrastructure) layer as well as a security architecture are specific strategic initiatives set forth in this Plan. The Department has also selected an automated tool, the Enterprise Architecture Management System (EAMS), to provide a central repository for its architecture data. Components vary greatly in the extent to which they have developed and applied component-level architectures.

Figure 8

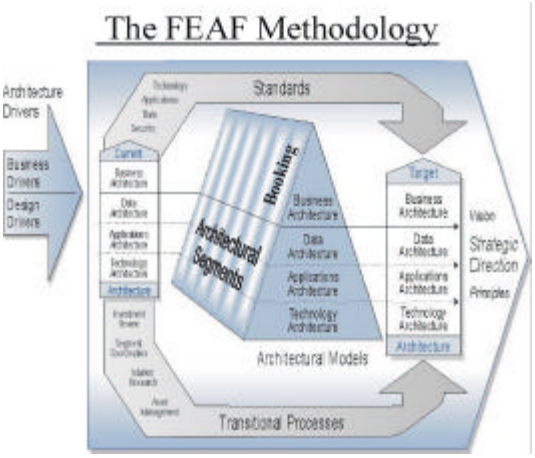


The CIO is responsible for developing, maintaining, and updating the DOJ department-level enterprise architecture, including the common systems and infrastructure portfolio. Because of its pivotal importance, continued and accelerated progress on enterprise architecture is a high priority for the Department. Our goal is to have an enterprise architecture that is cost-effective, provides a strategic view of our business and IT environment (current and future), is useful in making decisions, "fits" within the emerging federal enterprise architecture, and provides a framework to accommodate and guide more detailed architectural work at the component level or within specific segments.

The CIO, working with the components, will ensure that enterprise architecture is linked with strategic planning, investment management, and portfolio assessment processes at both the departmental and component levels with defined exchanges between component and departmental level efforts and results. The components will be responsible for performing their IT planning efforts within the broader framework of departmental plans, policies, and standards.

Appendix F provides an example of a segment architecture using the process for booking persons in federal custody. This Appendix demonstrates not only the architecture methodology, but also the tiered relationships that exist between the enterprise level architecture and the architecture of a particular segment. In this example, the booking process links directly back to the Department's business architecture. It is a subset of the function "arrest suspects" and the more general business area of "enforcement." The segment architecture describes the current and future state according to the four architectural levels: business, data, applications, and technology, as illustrated in Figure 9.

Figure 9



Strategic Initiative: *Develop and implement an IT human capital plan*

IT workforce issues have been the focus of considerable debate and discussion throughout the Federal Government in the last several years. The U.S. General Accounting Office (GAO) has termed agency efforts to address IT human capital issues as limited and sluggish. It has urged agencies to inventory and assess their knowledge and skill needs; develop and implement strategies and plans to fill the gap between requirements and current staffing; and continuously evaluate their progress.

The National Academy of Public Administration (NAPA), in a study undertaken at the request of the federal Chief Information Officers Council, concluded that the federal system for recruiting, retaining, compensating and developing information technology employees must change if the Federal Government is to have a quality IT workforce. The NAPA report cited two converging factors: significant retirements of older, more experienced federal IT personnel projected to occur over the next several years; and a growing inability to attract younger IT workers, in part because of the pay gap between the Federal government and the private sector and in part because of other factors such as opportunities for continuous learning. Both GAO and NAPA have offered a series of recommendations on a range of topics, including compensation, personnel policies, and career development.

DOJ generally faces the same problems addressed in the GAO and NAPA studies. In August 2000, a study entitled “Evaluation of the DOJ Information Technology Workforce,” made a series of findings and recommendations largely consistent with those offered by GAO and NAPA. These included the need to conduct formal workforce planning; better exploit hiring flexibilities; and develop a cadre of qualified project managers. The study also found that the DOJ IT workforce is “stagnating,” with attrition rates averaging between 3-5 percent and dropping to nearly zero among older workers. This is an indication of not only an aging workforce, but also one that is not being sufficiently reinvigorated by younger workers.

Implementing the Department’s IT vision requires skilled and dedicated people and a culture that nourishes and rewards good performance. The Department’s CIO will work with the components to develop and implement an IT human capital plan. This plan will identify workforce needs, including possible changes in required skills sets and resource levels based on the

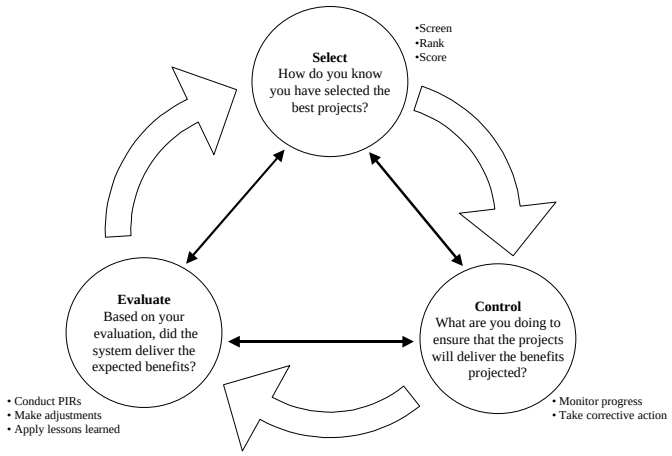
Department's new strategic direction. It will also assess which skills or core competencies should be provided within DOJ and which might best obtained through outsourcing arrangements. For some core competencies, one or two IT groups may be identified to develop the skill set and then share the skills with other components when needed.

A major focus of the plan will be improving career development opportunities so that Justice IT professionals can hone their skills, learn from others, and work on high priority projects. Career development paths should facilitate the assignment of DOJ IT professionals on projects across components so that the Department can bring the right skills to bear on priority projects and provide effective professional development opportunities for career IT employees.

Strategic Initiative: *Establish and implement improved investment management processes and practices*

The Department has established a formal IT investment management (ITIM) policy and process to ensure that investment decisions are aligned with the strategic goals of the Department, are well-planned and justified, fit within the Department's overall IT strategy and enterprise architecture, and are managed effectively throughout the life cycle. The Department's ITIM generally follows the OMB/GAO Select-Control-Evaluate Model, as shown in Figure 10.

Figure 10



The three phases of the Select-Control-Evaluate Process Model are viewed as part of a continual, interdependent management effort. Information from one phase is used to support activities in the other two phases. The phases in turn prescribe specific processes and analyses that must be completed

The ITIM is designed to ensure disciplined management of IT investments and the involvement of Department and component leadership in the assessment of cost, risk, and return for all proposed expenditures on IT. The Department's CIO will work with the components to implement, strengthen, and improve the ITIM process. Possible focus areas include: adopting more uniform procedures and practices department wide; developing standardized methodologies for capturing financial and performance information; and establishing a Department level ITIM.

Strategic Initiative: *Improve project management*

Managing information technology projects so that they meet cost, schedule, and performance goals, is a complex and challenging task even for the most skilled and experienced IT professionals. Yet good project management is absolutely key to the successful completion of projects and to the effectiveness of the Department's overall IT program.

The Department will improve its management of IT projects through a variety of means, including: more structured and detailed reviews by the Department's CIO of component projects; improved financial and performance reporting; a more standardized systems development life cycle methodology and program management model; increased career development opportunities for project managers; and greater identification, utilization, and sharing of core competencies.

The Department's CIO will have a business and technical oversight role on every major and significant project. The intent of the oversight role is to ensure that actual project work is aligned with the overall Department IT strategy and enterprise architecture, complies with Department standards, stays within the project's business case (e.g., scope, cost/benefits, schedule), and proactively manages risks that could inhibit success. The degree of departmental oversight will vary depending upon a project's

profile, e.g., its strategic impact, scope, risk assessment, and relationship to or dependency on other projects.

The components will be responsible for successfully delivering their IT projects. The CIO organization, in its oversight role, will participate at design reviews and all other significant project quality assurance checkpoints. Projects affecting more than one component may either be managed directly by the Department or by a component acting as "executive agent" because of its particular competencies and expertise. The Department may also directly manage IT projects on behalf of smaller components. Projects managed by the Department's CIO will be subjected to independent verification and validation.

Summary of Strategic Initiatives and Next Steps

This section of the Plan lists the strategic initiatives described earlier and identifies near term actions that are either already underway or are planned.

Strategic Initiative: ***Modernize and Unify the IT infrastructure***

- Develop and implement a Technical Reference Model to govern the acquisition of new infrastructure

Strategic Initiative: ***Provide a single, national data network***

- Develop an integrated set of departmental and component requirements as the basis for an outsourcing arrangement for the design, deployment, and management of a single, national data network

Strategic Initiative: ***Strengthen and improve the DOJ information security program***

- Establish CIO organization; elevate security function
- Monitor the implementation of corrective actions; enhance centralized database and tracking system
- Implement common security education and awareness program
- Initiate development of security architecture

Strategic Initiative: ***Design and implement a DOJ public key infrastructure***

- Establish Program Management Office
- Initiate initial requirements definition

Strategic Initiative: ***Create a blueprint of common solutions***

- Develop a project plan that lays out a series of BPR projects, near-term and longer term, to implement common solutions where appropriate

Strategic Initiative: ***Promote e-government***

- Accelerate implementation of the Department's Government Paperwork Elimination Act plans
- Participate in the Administration's e-gov initiatives
- Upgrade the DOJ web site

Strategic Initiative: ***Design and implement an ongoing, collaborative strategic planning process***

- Define scope, roles and timeframe for developing more comprehensive and detailed strategic plan

Strategic Initiative: ***Establish, refine, and implement DOJ IT policies, processes, and standards***

- Identify priority areas for assessment and possible change

Strategic Initiative: ***Continue to develop, refine, and implement a DOJ Enterprise Architecture***

- Further test and deploy EAMS
- Define and implement collaborative enterprise architecture process
- Complete current and target architectures and initial transition plan

Strategic Initiative: ***Develop and implement an IT human capital plan***

- Initiate baseline assessment
- Define and implement collaborative process for DOJ wide IT human capital planning

Strategic Initiative: ***Establish and implement improved investment management processes and practices***

- Review and approve FY 04 IT budget requests
- Establish performance metrics

Strategic Initiative: ***Improve project management***

- Establish process for periodic reviews

Critical Success Factors

This Plan lays out the Department's IT vision and goals and identifies a series of specific initiatives designed to move the Department closer to its vision of IT as "a cohesive, forward-leaning enabler of enhanced DOJ mission accomplishment." The goals and initiatives entail substantial change. The following factors will be critical to success.

- **Establish an environment that is conducive to change.** There will be a large number of changes introduced so DOJ should take steps to increase its capacity to successfully adopt to change. The culture must embrace and reward change attributes, such as flexibility, adaptability, innovation, and resiliency.

- **Engage business partners.** The IT projects will be a catalyst to help transform business processes and enhance results. To achieve the desired result will entail a business partnership where the operations and program groups are driving change in their environments.

- **Obtain resources and funding for multi-year projects.** Most of the strategic changes being made will span several years from concept to full rollout. The DOJ must take the steps necessary to arrange for adequate, uninterrupted flow of resources and funding needed to get the job done. In addition, the operating base of IT assets should be viewed as a non-discretionary funding level tied to specific performance and service level metrics in the fund allocation process. Any changes to the funding level needs to be linked to a corresponding change in the services provided.

- **Develop a strong, unified leadership team**. IT leadership across DOJ needs to aligned and focused on delivering the changes required to support operations and programs needs. As more emphasis is placed on sharing solutions and services across DOJ, IT leadership will have to work closely together on the more strategic priorities.

- **Drive the change agenda through teamwork, collaboration and communication.** IT groups across DOJ need to be more tightly coupled, avoid re-inventing the wheel, and share ideas, solutions and resources. At the same time, the operations and

program groups need to work more closely across components and with IT so the IT projects and baseline services address their higher priorities and can be leveraged.

- **Build an institutional IT capability to sustain the changes needed.** A critical mass of core skills, best practices, and well-defined processes must be in place within DOJ IT.

- **Focus on the higher priorities and then follow through with operational delivery.** The myriad of changes and projects required over the next several years will need to be phased. Projects will be assigned to a phase based on some combination of business priority, integration dependencies (i.e., other projects may be required to precede it), and resource/funding bandwidth. Establishing, and keeping current, a solid integration plan that recognizes dependencies between projects and factors in what is required to move from the old stove pipe legacy will be important. Once scheduled, higher priority projects should be constructed and deployed as soon as practical.