U.S. Department of Justice
*Justice Management Division*

# Information Technology Strategic Plan

## July 2002

# A MESSAGE FROM THE CHIEF INFORMATION OFFICER

Recent events have highlighted as never before the strategic importance of information in protecting American lives and carrying out the fundamental purposes of government. The deadly terrorist attacks of September 11 have instilled in all of us a profound sense of urgency and a renewed commitment to ensuring that information relevant to our national security is gathered, properly protected, and shared.

Information technology is not a “silver bullet,” but it is a critical asset that must be strategically utilized in support of the new counter terrorism mission of the Department of Justice. It is central to our ability to gather and share intelligence, prevent persons who are national security threats from entering the United States, conduct surveillance, apprehend and prosecute suspects, or any one of a number of our other key functions.

The challenges before us are daunting but not insurmountable. This Information Technology Strategic Plan represents a starting point for what will be a long-term, sustained, and collaborative effort to significantly improve information technology in the Department of Justice. A great deal of work needs to be done. However, with the continued help and support of the skilled and dedicated men and women who manage and implement our information technology programs, I am confident that we will succeed.

Vance Hitch

# Table of Contents

# 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.

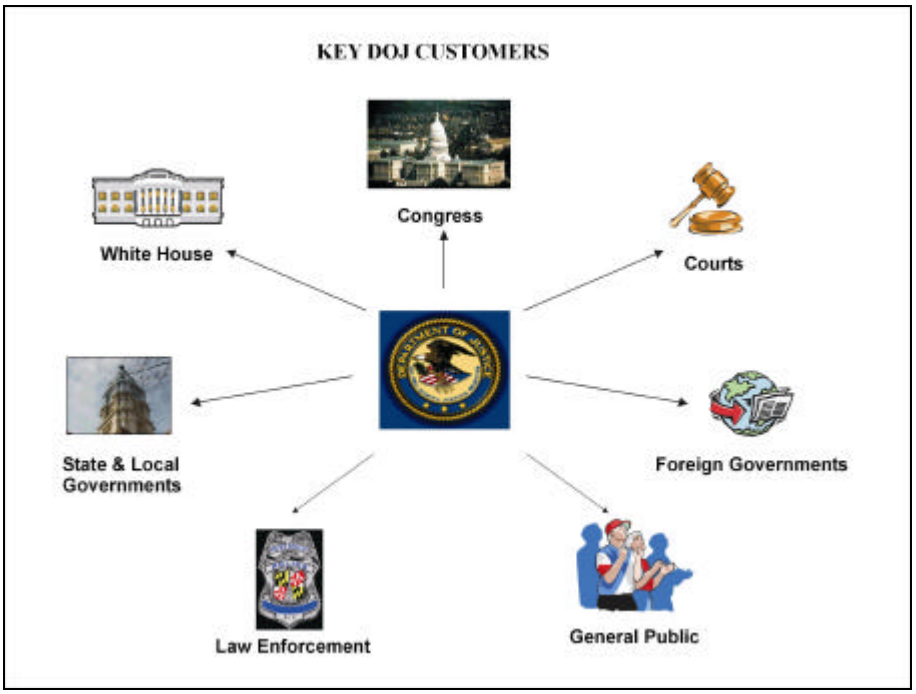
# Overview of the Department of Justice

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**



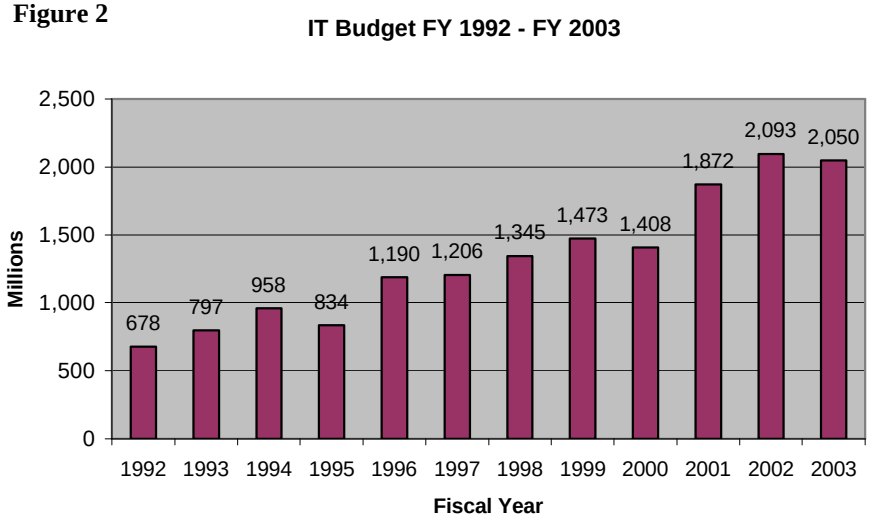

More than 130,000 persons are employed by the Department - - as attorneys, criminal investigators, border patrol agents, immigration inspectors, corrections officers, or any one of a host of other occupations. Although the Department is headquartered in Washington, D.C., most personnel work at locations 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.

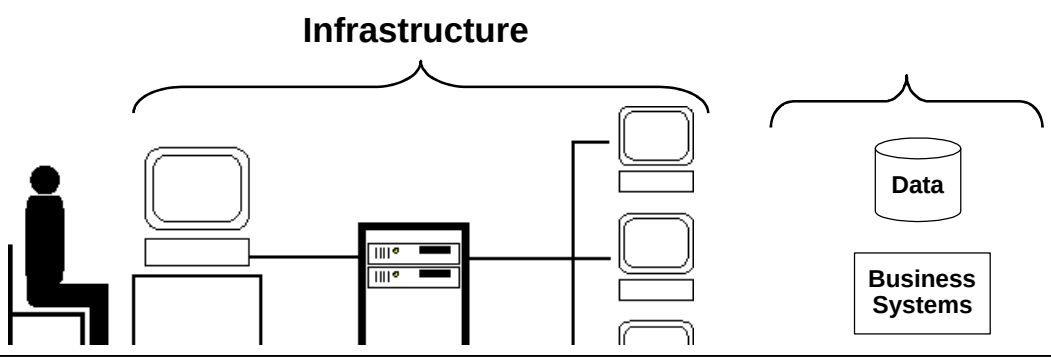
# IT Infrastructure

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*

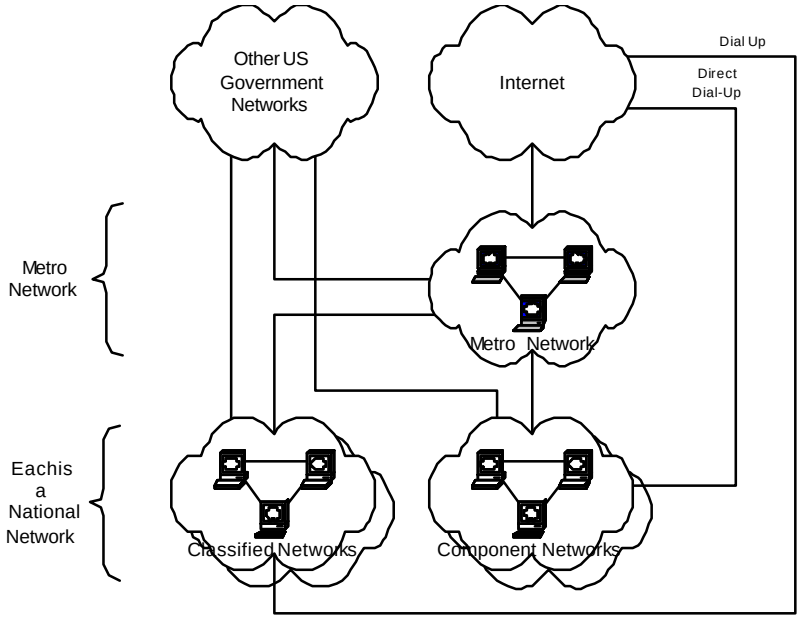
The Department will work with the components to develop a department wide infrastructure architecture - - a layer of the Department's overall enterprise architecture. The infrastructure architecture will provide a common conceptual framework to support technical interoperability, define a common DOJ 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.)

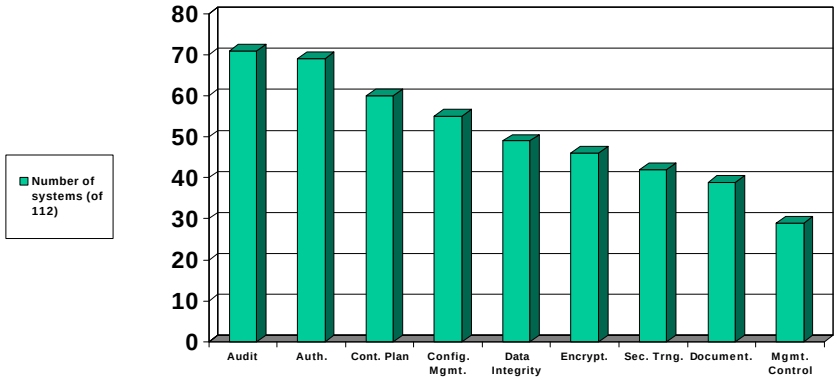
# Information Security

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.

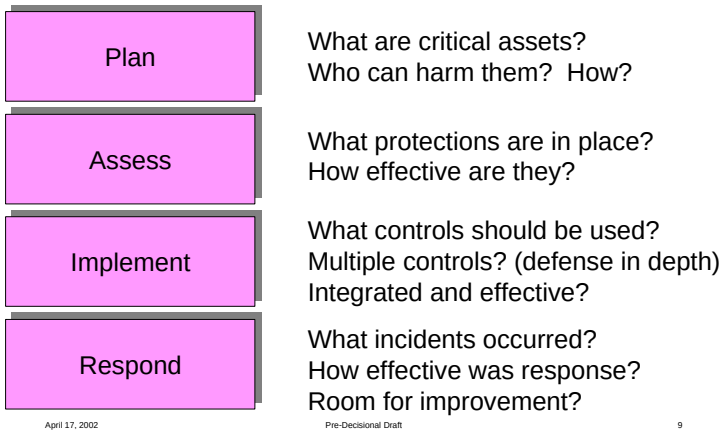
## Strategic Initiative: *Strengthen and improve the DOJ information security program*

### 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.

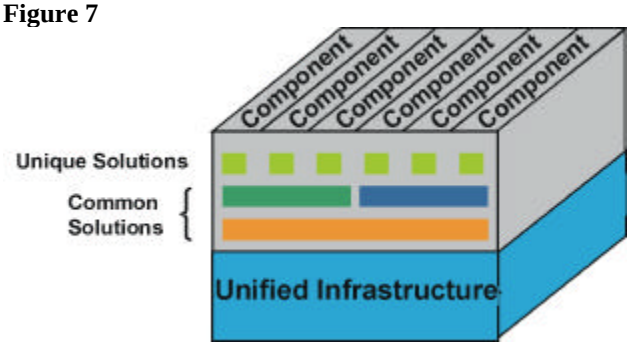
PKI is considered to be an important element in improving secure information sharing and implementing "e gov." The Federal Government, under the auspices of the OMB, has formed a federal PKI Steering Committee to lay the groundwork for government-wide use of PKI. In addition, several DOJ components have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

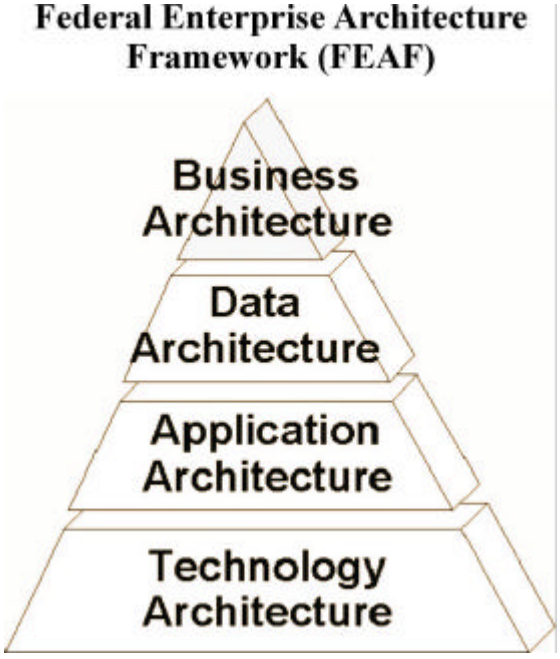
Working with the components, the Department's CIO will lead an effort to review and revise, as necessary, the existing set of policies, processes, and standards and to identify areas where new policies, processes, or standards should be developed. Initial efforts are likely to focus on developing more 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**

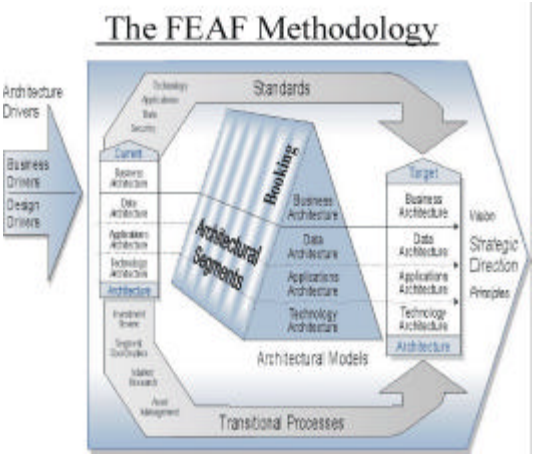


The CIO is responsible for developing, maintaining, and updating the DOJ department-level enterprise architecture, including the common systems and infrastructure portfolio. Because of its pivotal importance, continued and accelerated progress on enterprise architecture is a high priority for the Department. 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

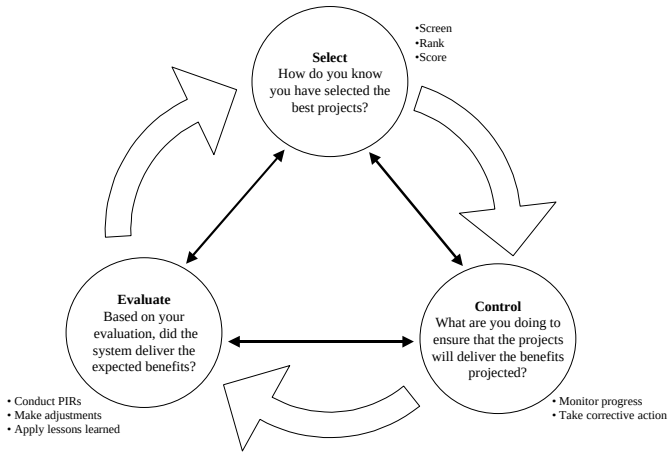
Department's new strategic direction. It will also assess which skills or core competencies should be provided within DOJ and which might best obtained through outsourcing arrangements. For some core competencies, one or two IT groups may be identified to develop the skill set and then share the skills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

# Appendices

# Appendix A

# Statutory Framework for Managing IT

## Appendix A
## Statutory Framework for Managing IT

| Year | Public Law | Title | Description |
|---|---|---|---|
| **1990** (November) | **101-576** | **Chief Financial Officers Act (CFO)** | The CFO Act lays a foundation for comprehensive reform of Federal financial management. The act establishes a leadership structure, provides for long-range planning, requires audited financial statements, and strengthens accountability reporting. Federal financial managers, auditors, and program managers at all levels of government will take necessary actions required under the CFO Act to improve financial management systems and information. |
| **1993** (January) | **103-62** | **Government Performance and Results Act (GPRA)** | Intended to improve Federal program effectiveness and public accountability by focusing on results, service quality, and customer satisfaction. Mandates adoption of strategic and annual planning processes-to be tied to the budget and authorization cycles, and based on established and measurable performance indicators-to inform Congress and the public of: (1) performance goals for agencies' major program and activities; (2) measures used to gauge performance; (3) strategies and resources-e.g. skills, technology, human, capital, information, and other resources-required to meet performance goals; (4) procedures used to verify and validate performance; and (5) performance compared with established goals, including reasons goals were not met, and action plans and schedules for meeting unmet goals. |
| **1994** (October) | **103-355** | **Federal Acquisition Streamlining Act (FASA)** | Requires agencies to define cost, schedule, and performance goals for Federal acquisition programs (to include IT projects) and monitor these programs to ensure that they remain within prescribed tolerances. If a program fails tolerance, FASA requires the agency head to review, take necessary actions, and, if necessary, terminate the program. |
| **1995** (October) | **104-13** | **Paperwork Reduction Act (PRA)** | Requires agencies to minimize the paperwork burden for individuals; small businesses; educational and non-profit institutions; Federal contractors; State, local and tribal governments; and other persons; resulting from the collection of information by or for the Federal Government. |

## Appendix A
## Statutory Framework for Managing IT

| Year | Public Law | Title | Description |
|---|---|---|---|
| **1996** (February) | **104-106** | **Clinger-Cohen Act (CCA)** | Also known as the Information Technology Management Reform Act (ITMRA), requires Federal agencies to focus more on the results achieved through IT investments while streamlining the Federal IT procurement process. This act introduces much more rigor and structure into how agencies approach the selection and management of IT projects, and describes a Capital Planning and Investment Control process as a method for advancing this discipline. |
| **1998** (January) | **100-235** | **Computer Security Act of 1987** | Assigns the National Institute of Standards and Technology (formerly known as the Bureau of Standards) responsibility for developing standards and guidelines for Federal computer systems, including responsibility for developing standards and guidelines needed to assure the cost-effective security and privacy of sensitive information in Federal computers systems, drawing on the technical advice and assistance of the National Security Agency where appropriate; to provide for promulgation of such standards and guidelines; to require establishment of security plans by all operators of Federal computer systems that contain sensitive information; and to require mandatory periodic training for all persons involved in management, use, or operation of Federal computer systems that contain sensitive information. |
| **1998** (August) | **105-220** | **Electronic and Information Technology Regulations (Section 508 of the Workforce Investment Act of 1998)** | Requires the Federal government to provide accessibility, unless an undue burden would be imposed on the department or agency, in the development, procurement, maintenance, or use of electronic and information technology, so that the electronic and information technology allows, regardless of the type of medium of the technology--individuals with disabilities who are Federal employees and members of the public seeking information or services from a Federal department to have access to and use of information and data that is comparable to the access to and use of the information and data by such members of the public who are not individuals with disabilities. |

## Appendix A
## Statutory Framework for Managing IT

| Year | Public Law | Title | Description |
|---|---|---|---|
| **1998** (October) | **105-277** | **Government Paperwork Elimination Act (GPEA)** | Requires the Office of Management and Budget (OMB) to include alternative information technologies that provide for electronic submission, maintenance, or disclosure of information as a substitute for paper and for the use and acceptance of electronic signatures. The act also directs OMB to set procedures for use and acceptance of electronic signatures by Federal agencies, and to develop procedures to permit private employers to store, and to file electronically with Federal agencies, forms pertaining to their employees. Also, Federal agencies will eventually be required to accept those electronic submissions except when they are impractical or inappropriate. |
| **2000** (June) | **106-229** | **Electronic Signatures in Global and National Commerce Act** | Facilitates the use of electronic records and signatures in interstate or foreign commerce. |
| **2000** (October) | **106-398** | **Government Information Security Reform Act (GISRA) (Title X, Subtitle G of the Defense Authorization Act)** | Provides a comprehensive framework for establishing and ensuring the effectiveness of controls over information resources that support Federal operations and assets; recognizes the highly networked nature of the Federal computing environment including the need for Federal government interoperability and, in the implementation of improved security management measures, assure that opportunities for interoperability are not adversely affected; provides effective government wide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities; provides for development and maintenance of minimum controls required to protect Federal information and information systems; and provides a mechanism for improved oversight of Federal agency information security programs. |

# Appendix B

# The Prospects for Technology Insertion

# White Paper

## Appendix B
## The Prospects for Technology Insertion White Paper*

It would not be practical for DOJ's information infrastructure to be on the leading edge for every information technology vector. The reasons DOJ cannot be state of the art across all technology vectors include:

- It is unaffordable. Following technology too closely means discarding systems while they are still functional and economic, undertaking repeated installation costs, and putting users and administrators through continual retraining.

- It carries risks. The first few versions of new technologies are often flawed, not "industrial strength" and may have security weaknesses that are not initially apparent.

- It presents potential barriers to interoperability beyond DOJ to the extent that other groups (e.g., working on a given case) may not have such leading-edge capabilities.

- It is not always necessary. DOJ has many systems that work quite well today and which provide a stable baseline for coordinated improvements. Technology upgrade or replacement should be predicated on a business justification.

- It requires a workforce inconsistent with the compensation limitations imposed on DOJ.

Consequently, DOJ needs to evaluate various technologies broadly and determine which ones appear to have the largest impact on DOJ and its mission. Technology areas that offer potential breakthroughs for DOJ effectiveness and efficiency will warrant more attention and risk taking than those that do not. Figure 1 is a heuristic spectrum of five technology strategy choices that range from being a technology driver to being a follower or, in the case of special requirements, a laggard.

- DOJ would be a *driver* of a technology if its requirements were unique, singular, or clearly leading-edge enough to pay for their development. For the Department of Defense (DoD), many technologies (largely those without civilian application) fall into this category. DOJ has far fewer such requirements; forensics is the most obvious example of a unique technology requirement.

- DOJ would be a technology *leade*r if it had sufficient need for a technology that it were willing to (1) pay the high cost of acquiring such a technology when it was introduced and (2) suffer through the inevitable difficulties in using and securing such technologies. For some technologies, the DOJ and its components may need to drive its advancement through establishing standards and funding development either directly or indirectly (e.g., biometric scanning). For others, the DOJ will not assume this leadership role but may decide to be out in front with an advanced but commercially available technology (e.g., data mining tools).

- DOJ would be a technology *early adopter* if it had a strong requirement for the technology and could make use of it early. An early adopter would deploy a technology once it is commercially

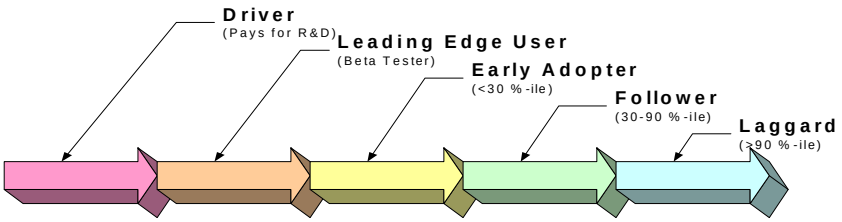
* This White Paper is based on unpublished material prepared by the Rand Corporation for the Department of Justice.

available and proven but not widely installed. Generally, the business benefits would justify an earlier adoption and offset the higher costs and risks of early adoption versus deferring until the technology matures.

- DOJ would be a technology *follower* if its requirement for the technology were no stronger than that of comparable organizations. Waiting until other organizations have deployed the technology usually reduces the time, cost and risks involved and allows one to take advantage of others' lessons learned.

- DOJ would be a deliberate technology *laggard* if it had special requirements that were either met only by previous but not current generations of technology (e.g., applications available only for older operating systems) or because it needed extensive maturity in technologies to prove their rock-hard stability.

**Figure 1**
**When Should Technology be Adopted?**




Six technology areas are discussed below. The discussion is in two parts: the first part is a quick tutorial of the potentials and maturity of the technology; the second is an examination of ways DOJ might use the technology. Because DOJ is composed of components and subcomponents, a general assessment of DOJ's stance on a technology (e.g., DOJ should be an early adapter of this and a follower of that) does mean that such assessments necessarily apply to all components equally.

### *Sensors and Biometrics*

Sensors and biometrics acquire a large component of all information collected from the ambient environment (in the case of sensors) or from individuals (in the case of biometrics). Both involve the conversion of physical facts into information (in some cases without further

interpretation). As with any sensing technology, the percentage of all information so acquired that, later, becomes useful for law enforcement is random and small.

*State of the Art and Current Trends*

Although the U.S. Army has made tremendous strides in the development of unmanned ground sensors, the relevance of its work to DOJ requirements is tangential inasmuch as many of DoD's parameters (e.g., well-funded applications to support short-term usage in territory without uncontested access) do not apply to DOJ. Tactical unmanned aerial vehicles under development for the Army and the U.S. Marine Corps may have applicability to DOJ once they become sufficiently reliable and under human control to share the nation's air spaces. Perhaps the most useful trends in sensors has been in the consumer sector. One aspect has been the proliferation and sharply falling costs of devices such as digital cameras, night-vision optics, infrared detectors (as intrusion detectors), and high-gain microphones. Another has been the rapid decline in the cost of so-called "smart tags," global positioning system (GPS) devices, and low-power transmission gear (controlling bovine herds electronically is becoming increasingly feasible). Combining cheap electronics and low-cost networking promises to improve the efficiency of wide-area surveillance networks.

*How Can Technology be Used?*

Sensors come in stand-alone forms (e.g., bomb-sniffing machines) and networked mode; the latter is relevant to DOJ's information strategy, notably for border control. INS runs a fully-sensored network, the Integrated Surveillance Information System (ISIS), that monitors the southwestern border of the United States to detect movements that may indicate illegal immigration or narcotics smuggling. DOJ should be a technology *early adopter* in the area of wide-area sensors and their integration into fully developed situational awareness suites. In this regard, it should stay abreast of the DoD as it develops similar technology for military purposes so that it can step in to adapt such sensors to the exigencies of its target physical and legal environment. The overall strategy for such a network is to push in the direction of increased acuity and coverage, as well as faster response-times and lower maintenance and installation costs.

Biometrics is another rapidly developing field in which DoD, again, has taken the lead (notably through the Defense Advanced Research projects Agency's (DARPA) human-ID-at-a-distance program). DOJ should be a technology *driver* in the application of biometrics to forensics, notably in (1) pushing the state of the art in making effective use of continually smaller and less-than-perfect biometric samples, and (2) making faster determinations of matches between collected and archived biometrics. DOJ should be a technology *leader* in the application of identifying people at a distance and in the exploitation of other biometric techniques such as signatures, voiceprints, and associated metrics.

DOJ should pursue an aggressive strategy of acquiring fingerprint reader devices. Modular upgrades to the JABS program may provide the correct vehicle for such acquisition for the USMS, BOP, and DEA.

## Appendix B
## The Prospects for Technology Insertion White Paper

### *Case Support Tools*

Investigators, prosecutors, and litigators must all cope with vast heterogeneous collections of information that must be accessible in near real time and may yield further results if they can be correlated (much as data mining promises for sufficiently structured data). Tools that would assist in this process include those that support:

- Case management,
- Automatic voice and handwriting recognition,
- Automatic language translation,
- Assisted content-tagging,
- Data visualization,
- Data mining, and
- Knowledge management.

*State of the Art and Current Trends*

Legal cases are multi-faceted and complex. They require tailored software to assist in its management. Case management systems entail the management of documents, which can include: securing documents; handling and maintaining different versions of them; searching through and retrieving them based on words or phrases. These systems can also assist in time and relationship management with calendaring, contacts files, "ticklers" for reminders of upcoming deadlines and events, and so on. To serve the specialized needs of large law firms, vendors[1] have developed a variety of products.

Case management software typically includes one or more of the following:

- *Relationship management (link analysis)*: can track an indefinite number of contacts, each with an unlimited number of addresses, phone numbers, and related cases; integrate contact information with telephone system (e.g., "click to dial"); integrate contact information with office automation address books; and use online "notes" attached to contact information.

- *Document management*: can support document scanning; full-text indexing of word processing documents (including the ability to search for words by phonics, word stems, or synonyms); document check-in and check-out facilities (so only one person on a case can modify a document at one time); control over read-only, modification, and check-in/check-out rights for specific documents.

[1] A representative set includes: Prolaw Software (www.prolaw.com), LegalEdge Software (www.legaledge.com), Legal Files Software Inc. (www.legalfiles.com), Gavel & Gown Software Inc. (www.amicusattorney.com), Abacus Data Systems Inc. (abacuslaw.com), Software Technology Inc. (ww.stilegal.com), and ADC Legal Systems Inc. (www.adclegal.com.). A broader index can be found at www.netesmartinc.com/software.htm). This listing in no way implies endorsement of such products by the DOJ.

- *Rules-based calendaring*: can manage deadlines for a particular case, event and meeting arrangements, docket event tracking, reminders, and integrate itself with office automation calendars.

- *Records management*: can track the complete history of every file; integrate with bar codes for document tracking; and access scanned files.

- *Conflicts searching*: can check all other cases that case-related parties have been associated with.

- *Time tracking, billing and accounting*: can track time spent on various tasks, integrated with billing and accounting systems if needed.

- *Report generation*: can design custom reports through "drag and drop" of fields.

- *Web accessibility*: can support access to case information via a World Wide Web page ("portal") with access control, for remote (home, hotel, office) access to common case files.

As a general rule such software can be integrated with word processing packages, a variety of operating systems, E-mail clients, palmtop clients, spreadsheet-scanning systems and they support the Legal Electronic Data Exchange Standard (LEDES) developed by PriceWaterhouseCoopers. Although the capabilities mentioned above are important functions of relevance to law enforcement, they come with substantial requirements for initial implementation, subsequent maintenance, and integration with other software systems.

The improvement of *voice and handwriting recognition products* has been and is likely to remain gradual; a breakthrough in either is unlikely. Major software houses (e.g., Microsoft) are eager to incorporate such technologies into their offerings once they reach a certain level of reliability; the growing ubiquity of palmtops and smart cellular telephones is likely to push progress forward somewhat faster. Within a five to ten year period such products may overcome the current obstacles so that the cost and hassle of entering information by voice or hand and then manually correcting the output of such products drops below the cost of entering such information by keyboard.

*Automatic language translation* is also characterized by slow steady progress, but without the handheld market to drive it forward. Given the amount of computing power and data stores required for automatic language translation, it may be better provided as a subscription service hosted on heavyweight servers and accessed via a Web-client than as standalone products. In the United States, this market is being driven in large part by the needs of DoD and the intelligence community.

*Automated tagging tool*s are used to annotate free-form text and other such data so that it can be machine-processed for search and retrieval, as well as publishing. The advent and widespread acceptance of XML (eXtensible Markup Language) has created a grammar and method for

tagging. The corresponding development of standard tag sets has proceeded slowly . The prospects are good, however, that within a few years, there will be a standard tag set for the litigation and investigation community.

*Data visualization tools* convert data into graphical artifacts in order to enhance human understanding of their contents. As with speech and handwriting recognition, progress is slow but steady; what works for one may not work as well as for another; and tool standardization is not really needed for such tools to work together (data may have to be in standard format for such tools to work, however).

*Data mining tools* comprise another set of techniques to help uncover insights from large volumes of structured data. Six techniques are commonly used: neural net analysis (capable of "learning" from given examples to make plausible predictions), decision tree analysis (which uses binary dichotomy methods), clustering algorithms (to discover like features within data sets), affinity analysis (to generate if-then rules), case-base reasoning (class-matching algorithms; but losing favor as a technique), and genetic algorithms (that gradually improve prediction fitness; not yet ready for general use). Two general rules should be noted. First, data mining tools assist analysis but users have to know what they are looking for first. Second, such tools have to be specific both to their data sets and to their inquiries; a tool that shows, say, that disposable diapers and beer are often purchased in the same shopping trip is not the same as one that can build patterns of association among criminals.

*Knowledge management* promises organizations that it can collectively know the sum total of what its employees individually know. It comes in two flavors: one helps to organize information (e.g., find me a report on the involvement of parking enforcement in the drug trade), the other organizes people (e.g., find me a person(s) who knows about this subject, experience, etc.). Sometimes a knowledge management system is as simple as a culture (and a network) that lets people pose questions to the community as a whole and expect a cogent response. As a rule of thumb, in any field with less than 200 professionals, people will know of each other well enough to abjure automated systems for acquiring such information.

*How Can Technology be Used?*

As a general rule, the seven technologies of this section are rapidly evolving tools rather than mature, integrated product suites. As such, while there may be a long-term goal to equip DOJ with the latest case support tools, given the fluid nature of the environment at this time, this is not an area in which DOJ should make elaborate long-term plans. The likely (and preferred) scenario calls for purchasing such tools, as compelling needs and opportunities are defined by groups within DOJ. Many of the first purchases will be pilots or experiments and some experiments will not pan out. Others will work; people will be satisfied and/or more effective with the experience and recommend others do the same. At some point, the successfully applied tools will become more mature and will warrant establishing standards and broader rollout.

## Appendix B
## The Prospects for Technology Insertion White Paper

With regard to case management tools, DOJ would be a technology follower because their needs are unlikely to differ significantly from major multi-office, multi-national law firms, in this area. In light of the expected difficulties of owning such complex software, DOJ strategy should put a heavy emphasis on site visits to large distributed users of different systems under consideration prior to adopting such tools.

With regard to voice and handwriting recognition tools, DOJ would be a technology follower. What is important is not that each tool interoperate with each other but that each work well (e.g., produce reliable digitized text from verbal or written word). The acquisition of such tools by DOJ would be very useful (especially for the litigating and investigating components) in completing its digitization program, and thus the progress of such tools should be actively monitored.

DOJ would be a follower in automatic language translation, either letting the intelligence community take the lead, or looking for a Web-based service and signing up as a client.

DOJ should be an early adopter of automated content tagging tools once such tools are commercially viable. Tag set standardization for the legal community (prefatory to the use of automatic tagging tools) merits a strong DOJ participation. Getting people to tag documents (in whatever tag set), however, is far more difficult -- akin to asking software developers to document their code or getting intelligence analysts to classify each paragraph they write. But like software, annotation at some point has to take place if case materials are to be truly usable by people at remove from the case itself; good tools will hasten that day.

With regard to data visualization tools, DOJ would be a technology follower, keeping abreast of developments.

DOJ should be an early adapter of data mining tools. As noted, the benefits of having an integrated database of persons assume some sort of data mining capability. Although there are desktop data mining tools, the assumption is that a serious data mining application is likely to sit on its own heavyweight server. Here, the recommended strategy is to experiment robustly with alternative models, pay attention to their specific requirements for data, and, if any appear promising, acquire them as one would a major program.

DOJ should be a technology follower in knowledge management software. These tools can be useful for larger communities; within them it has to be installed widely if it is to be at all useful (and, if it is installed, should cover the broader law enforcement community and not just DOJ's portion); it also has to be carefully designed and implemented. It should stay abreast of technological developments but hold off on implementing its own systems until they are proven useful elsewhere and until the potential benefits to DOJ can be documented.

### *Collaboration Tools*

Collaboration tools are used to enhance interactions among people and permit the creation of virtual teams from people who work for different components or in disparate locations. Enabling

tools include video teleconferencing, whiteboarding, groupware, and the ability to commonly reference material. Implicit in many collaboration tools is that material can be organized in a logical and intuitive manner. The ideal here is for every virtual team member to log into a collective effort and be presented, not only with access to other team members, but also a structured case collection that can be visualized and subject to formatted queries.

*State of the Art and Current Trends*

Many DOJ activities, notably case management, require collaboration, both within groups of individuals within one location or office, and between geographically distributed groups. The state of the art falls under three categories: supporting infrastructure, collaborative application tools, and content repository.

*Infrastructure*: Collaboration requires a network infrastructure that provides many-place many-time access to secure information and communication (any-time any-place access is better, but not always realistic in some situations.) The following discussion assumes team members are collaborating on a "case" (but has a broader relevance) that stretches, project-like, with a beginning, middle and end spanning months or years, and with variable team membership (both from case to case and within a case over time) composed of individuals who may, themselves, be associated with multiple cases. These individuals may be DOJ employees or consultants, affiliates of other government agencies (federal, state, local) or international organizations (e.g., Interpol, other countries' DOJ or INS equivalents). What matters is the ability to create new groups of communication partners with access to at least some parts of the secure network infrastructure on a case-by-case basis, and to add (or delete) individuals quickly and easily.

The network infrastructure must be accessible to case team members from their offices and their homes as well as on the road (in many locations); it should be possible to send/receive still images at least in most situations. The state of the "infrastructure" art is maturing rapidly, with a number of international companies (e.g., InfoNet with its "DialXPress" service) offering thousands of "gateways" (local telephone numbers) into a protected network based either on separate, leased lines, or facilities to tunnel through the Internet with encrypted messages.

*Collaborative applications and tools*: These comprise an extensible repertoire of end-user software embedded in the network infrastructure and/or its clients. These applications and tools should provide support for work group collaboration among case team members. For convenience, such software can be grouped into three subsets[2] with somewhat fuzzy boundaries; they reflect increasingly specific and active roles for collaborative applications and tools.

Special collaboration tools facilitate timely and effective interaction among case team members. Examples include items mentioned above under "case management": address books; interface to secure fax, phone, and printers; special fields in documents to allow explicit threading; automated filing and retrieval; deadline markers; and so on. Cooperation support tools

[2] [following Malone, Olson and others in the computer-supported cooperative work research community]

include specialized facilities to support particular types of multi-person cooperative interchanges, such as:

- Real-time in-person or distributed conferencing, smart whiteboard-like applications, shareable and manipulable group artifacts (e.g., models, flow charts, if-then scenarios),

- Asynchronous distributed technologies that provide at least similar capabilities (e.g., asynchronous conferencing with posting alerts), and

- Decision support tools

Cooperation support tools are emerging from the domain of "peer-to-peer" (P2P) networking. For instance, the Groove Networks system (www.groove.com), which provides a common workplace for distributed participants, provisions for shared document folders, email, chat, shared program "tools" *et al*, security and encryption, the capability to configure multiple workspaces and restrict access to invited participants. This system is P2P in that the content of these workspaces is distributed to participants' computers, and not centralized in any one location. This architecture also provides considerable resilience and robustness, with no single point of failure. In such tools, the software, itself, takes on an active role in managing cooperative activities. Examples include intelligent agents playing rule-based roles in planning, exploring, fact-finding, decision-making, and technologies that provide routine or event-triggered roles in moving the work flow (e.g., enterprise resource planning (ERP)-like systems, some document management systems).

DARPA is addressing the problem of complex, distributed information systems built from heterogeneous components. One example is BBN's Assured Assembly Infrastructure (AAI) Toolkit (see aai.bbn.com) whose aspirations includes permitting the dynamic composition of systems based on real-time feedback of system state, on expressed requirements for system services, and on expressed dependencies between system components. Dynamic composition of systems will benefit long-lived distributed systems by providing adaptability in terms of satisfying evolving requirements under evolving operating conditions.

Related DAPRA work includes the Habitats system, involving user "agent" programs that negotiate with the system and other agents within it to provide access to services and facilities that users require. These programs also rely on "object-oriented" software technologies, in which software modules contain both data and the operations to be performed on those data.

*Content repositories*: Multiple databases will undoubtedly be involved in collaboration. Users need common interfaces and search/browse tools to give them the perception of dealing with one large but well differentiated repository of information with relevance across multiple cases. Quite likely these databases would serve other non-case purposes as well (e.g., report generation, organizational learning, knowledge management, and data mining). Examples of types of contents may include directory information, quantitative or other structured data (e.g., arrest records, motor vehicle records, visa request rejections, and so

on), text reports (background information, memoranda), and images (photos, fingerprints). For content repositories to be useful they must be initially accurate and be maintained/updated on a known and appropriate schedule. It should be possible to search them readily, accessing case-related information and storing it in appropriately useful chunks (perhaps in some sort of case-defined temporary store). Finally, there should be easy-to-invoke links between different types of data potentially residing in different databases (e.g., it would be desirable to be able easily to link quantitative data and a related background report about illegal alien activity at defined borders).

*How Can Technology be Used?*

Many of the individual components of a collaboration suite, such a video teleconferencing and whiteboarding, are fairly mature. Some DOJ components (e.g., EOUSA) are actively investing in such technologies for their own purposes. Other aspects of collaboration, such as the ability to annotate interactions, or to have background materials come up without being summoned are still in the laboratory.

By and large, however, collaboration tools have not been widely deployed, in large part because they do not feel "right." They have yet to capture the social and organizational dynamics of the way people work – with their panoply of social cues, side-comments, and accidental encounters -- in a natural way (robust networking helps but only partway). There remains considerable (and often justified) skepticism that the results of using collaboration tools are worth the bother of learning how to use them effectively. Part of the problem is one of expectations. It would be nice to create a virtual environment in which new entrants to, say, a case or investigation, feel as comfortable as those who have been on it for a long time do. But simply throwing the case materials at someone and hoping this brings them up to speed is hardly adequate; there is a considerable body of tacit knowledge built into a case which is hard to capture easily. Another part of the problem is one of standards; bridging the gaps between still-proprietary systems is difficult.

Nevertheless, given the benefits of information sharing, and the multi-jurisdictional nature of many of DOJ's toughest challenges (e.g., counter-terrorism, counter-narcotics) the benefits of being able to do virtual teaming are very high. The DOJ strategy, therefore, should be to launch some collaboration pilots. Once one or two pilots pass the test of real usefulness, the experiment should be extended to other interested entities within DOJ. If and when these tools become mature and ingrained in how people operate, their wide-scale rollout within DOJ litigation and investigation components and beyond them to other law enforcement entities could represent a significant process improvement breakthrough.

DOJ should be an early adopter in content repositories. Many DOJ components work with the same groups—criminals, aliens, etc. so managing relevant content and providing secure access could enable substantial operational improvements and business process transformation.

## Appendix B
## The Prospects for Technology Insertion White Paper

### *Remote Access*

To help spur overall communications competition based on wireless technology, the U.S. and other governments have begun efforts to reallocate spectrum. The DOJ, along with other U.S. Government agencies, has been forced to revamp its wireless communications infrastructure under the mandate that it cut its need for spectrum by 75% within the next five to ten years.

*State of the Art and Current Trends*

Remote access to data and voice communications networks – whether via wireless or wire-line service – has changed tremendously in the last five years. Technology now makes it possible for DOJ employees to access DOJ voice and data networks from their homes, desktops, colleagues' offices, and the field. This opportunity will only grow over the next five to ten years. Network access entails a broad swath of technologies from radio frequency communications based on licensed and unlicensed spectrum, to copper wires and coaxial cabling of existing service providers, and fiber-optic facilities deployed by incumbents and startups alike. These technologies support both voice networks and a broad array of data networks based on transport protocols such as Ethernet, Frame Relay, ATM, and IP – all available in both public and private forms.

The Telecommunications Act of 1996 and other forms of deregulation has spurred the deployment of new access technologies, and new network operators to offer them. This market is in the midst of a major restructuring, which has yielded a complex telecommunications landscape with glut (largely in the backbone) and shortage (largely in the last mile), vendors with unpredictable business futures, and a cornucopia of choices. Nevertheless, the cell phone is on its way to becoming a ubiquitous fixture in urban areas. That plus the fact that computers and Internet are features of most American households has blurred the line between home and work. Households, in turn, are beginning to switch from dial-up to broadband access; at least 10 million use either high-speed cable or DSL to get to the Internet. In business, wireless access technologies combine with notebook computers to enable workers to fetch e-mail, intranets, and corporate databases from desktop, conference room, or off-site alike. Airports and coffee shops are beginning to experiment with providing Internet access. Broad access coupled with VPN (virtual private network) technology are making obsolete the very notion of a desktop as the only possible workplace – particularly for those whose gather, analyze and use information. Meanwhile computers are becoming general-purpose communications devices thanks to instant messaging service, voice-over-IP capabilities, and stream media. Pagers and cell phones are undergoing this transition in reverse; they become capable of exchanging text, web pages, pictures, and even video.

No single, unifying access technology is likely to emerge as universal as twisted pair copper wiring was for telephony. If nothing else, differences in geography and history will see to that. Similarly, no single access standard is likely to become ubiquitous. Nevertheless, at least three standards – HTTP (for Web access), TCP/IP (for the Internet), and Ethernet (for local-area connections) – are so entrenched that betting against them in any context is likely to be foolish.[3] IP,

[3] Other aspects of access standards and technologies are difficult to forecast with any confidence. Consider wireless data

especially, is likely to dominate as the underlying protocol of choice for universal data transfer. The standard, itself, is on the verge of shifting from the IPv4 implementation to a newer IPv6 implementation. Although it is unclear when the best time to switch from one to the other will be, it probably will not be within the next few years.

Services such as voice, e-mail, and instant messaging are expected to converge based on a common IP transport layer. Technologies, standards and services such as VoIP, H.323 videoconferencing, SIP (Simple Internet Protocol), and instant messaging may well become the basis for a substantial worldwide market to carry long-distance voice services over data networks. If trends continue, business data and voice communications are expected to merge into a single service offering. Video may eventually join this convergence.

Public policy will place increasing amounts of spectrum in the hands of commercial network operators. Communications is becoming a commodity, dominated by economies of scale. Access technologies, and networks suitable for use by DOJ will largely remain in private hands in the next five years. There will be competition among private network operators; however, that competition may be limited to where the reach of large access networks overlaps such as between competing cellular franchises or between cable TV operators and incumbent DSL providers.

*How Can Technology be Used?*

DOJ's path to enhanced remote access can be discussed in terms of three steps:

First, all DOJ employees would be able to log into their workspaces from any DOJ office. For example, an investigator working with a prosecutor on a criminal case would be able to access investigative information resources from the DOJ network at the prosecutor's office to help the prosecutor in preparing the case. At a minimum this requires that all DOJ component networks be sufficiently and simultaneously interconnected and well secured – a departure from the current security model that relies on electronically disconnecting networks from the rest of the world. Thus, the upgrading of OA tools would be coupled by security infrastructures that employ alternative methodologies to enhance security.

Second, such capability would be extended to other U.S. Government worksites (e.g., courts) through common remote access technologies (e.g., a secure 802.11b/802.11a infrastructure).

Third, such capability would be extended to any location in the field. The goal is to enable all DOJ employees away from the office (or even away from a table) to log into their workspace, retrieve and send important messages, and, better yet, participate as a full-fledged member of a virtual or physical team.

---

access. Although Europe has a single standard (whose deployment awaits sufficient capital), the U.S. cellular market is based on several standards, each with its own strategy for evolving to broadband data access. While all of this is debated among the carriers and governments, the 802.11b (and 11a) standards are being used to implement 10Mb/s+ access networks in locations like Starbuck's and airports. There are hints that cellular carriers are considering deploying similar technology [ref].

---

## Appendix B
## The Prospects for Technology Insertion White Paper

The mandate to reduce spectrum use, coupled with the burgeoning development of wireless options for data access offers DOJ an excellent opportunity to rethink its wireless strategy. DOJ must replace its current voice-only wireless infrastructure with something that accommodates data – but is nevertheless compatible with DOJ's stringent security requirements and the geographical distribution of its workforce . Similarly, DOJ must examine where it can best utilize commercial wireless voice and data services to meet its needs. This may, for instance, entail investments in token-based authentication and VPN software for notebook computers and handheld devices that assure authentication, authorization, and privacy and integrity of data regardless of the public network used to access DOJ networks.

DOJ should also recognize that these wireless networks are a competitor to the traditional networks for voice services, as well as data services. While cellular phones, like any other technology, is unlikely to be a universal strategy for DOJ, it may be a suitable targeted alternative to PSTN-based services to assure that DOJ is getting the best prices for services such as local and long-distance voice and voice messaging.[4]

Telecommunications trends point to a future DOJ network design utilizing multiple commercial service providers for access (and backbone) networks.[5] No single carrier will be able to provide universal service for DOJ's needs, and resilience and recovery concerns dictate the use of multiple carriers. Furthermore, even the largest of these carriers may face financial difficulties in the future. Thus, DOJ must develop network architectures that are based on heterogeneous access technologies, and that minimize the substitution of one carrier for another.

Access technology is closely coupled to security concerns. Wireless techniques, notably 802.11b and its putative successor 802.11a, have unacceptably bad security, whether used in a DOJ facility, in an employee's home, or in public (e.g., at an airport). Fixed point-to-point wireless (e.g., free space optics, MMDS, LMDS, and VSAT systems) also has a role in DOJ in providing access to DOJ backbone networks at remote offices. DOJ's use of these technologies must either await better security or the development of virtual private network (VPN) tools that encompass all DOJ LAN nodes using wireless access. These same security tools (e.g., token-based authentication, link- or end-to-end encryption, virtual private networks, etc.) can also be used over public networks to provide access to DOJ networks. Examples include employees using their Internet Service Providers to access DOJ networks from home or hotels, and using public networks to implement communications links between DOJ facilities.

---

[4] Cellular billing plans have virtually eliminated the distinction between local and long-distance prices. Cellular service is by definition mobile and eliminates much of the cost and delay associated with carrier or PBX managed wire-line services (e.g., Centrex).

[5] GovNet may emerge a component of DOJ's access and backbone networks. It is currently envisioned as an "air-gapped" network assuring secured, reliable government communications. It is likely that a GovNet would only be applied to "essential" DOJ operations, and not to all of DOJ's network needs. Furthermore, it seems unlikely that an extensive GovNet would be facilities based. It would likely be completely or partially built using encrypted links over public networks providing access and backbone transport.

## Appendix B
## The Prospects for Technology Insertion White Paper

There are currently two primary devices used for remote access: laptops and palmtops. A growing percentage of worksites will have wireless connectivity to the Internet and, as they do, DOJ equipment should be prepared to take advantage of that fact (e.g., via PCMCIA cards in laptops). For those sites without 802.11b or similar access, the next best option is direct wireless access through a wide-area provider. Yet, as noted below, the bandwidth that would more than satisfy a handheld, may not satisfy a laptop with its greater capacity to display and store information.

The quest for a wireless solution for handhelds raises four issues: adequate bandwidth, adequate coverage, security, and emergency services. As noted, current services, on average, can deliver 10,000 bits per second. This is adequate for exchanging E-mail and black-and-white images (e.g., on the RIM Blackberry) but inadequate for full-fledged data access, the easy use of high-end palmtops (e.g., Compaq's iPaq), or the transfer of even gray-scale images. Within five years, it is likely (but by no means certain) that access speeds (at least in metropolitan areas) will reach 64,000 to 384,000 bits per second. At 64,000 bits per second, a high-end handheld screen (240 x 320 bits) can be filled with a compressed image in one to three seconds (depending on color depth, the degree of detail, and overhead). 64,000 bps is therefore quite adequate, and 384,000 would be excellent. Down the road, it will also be important that these handheld units be able to *transmit* at adequate transmission rates. Many handhelds support cameras. There is no technical reason that a suitably modified handheld cannot acquire slap fingerprints as well (since a full-fledged fingerprint file is roughly a megabyte, transmitting one would take roughly two minutes over a 64,000 bps connection). As all these services come to be offered, DOJ could prototype their use with field agents of a component that do not have stringent security requirements.

In the meantime, DOJ (perhaps in conjunction with other U.S. Government agencies) would look hard for a secure solution for wireless data transfer. A key requirement is that third parties that capture a handheld device not be able to log into the Department's databases or network services without some further authentication mechanism (e.g., a PIN number or biometric).

Three issues are yet to be resolved before DOJ can move off its current voice-only self-managed wireless system (not to be confused with point-to-point wireless systems such as walkie-talkies): voice service, coverage (especially in the southwestern border areas), and emergency capabilities. Getting voice, of course, is the *sine qua non* of any decision to abandon the wireless system; yet, with proper client-side modifications, any system that can transmit data can also transmit voice-over-IP (compressed voice streams can easily fit within 10,000 bps service). Coverage can be met in one of two ways: by special arrangements with a service provider (e.g., via contract or incentive-rate purchased commitments), or by space-based systems.

Emergencies, for their part, come in two types: unexpected service interruptions or unexpected usage patterns (e.g., the congestion of cell phone service in Manhattan after the Twin Towers were hit). Space-based systems have the characteristics that their individual cells are very large; thus even a local emergency that congests local cell service may register only a blip within the larger space-based cells. Nevertheless, both terrestrial and space-based communications offerings are in flux and it is by no means certain which ones, or even if any, are viable business propositions.

## Appendix B
## The Prospects for Technology Insertion White Paper

The DOJ strategy for replacing its current generation of handhelds should put a premium on retaining today's service for now and wait to see how the market shakes out. In the likely event that high-bandwidth data services become available, then the active and intelligent exploitation of such services is the preferred path. Again, depending on market conditions (e.g., the population of low-earth orbit space-based communications), a backup and low-density strategy of using low-earth orbiting space-based communications has a good deal to recommend it.

Finally, the overwhelming role of commercial communications infrastructures within DOJ's overall communications mix, combined with the shortfalls revealed in the wake of the Twin Towers bombing together focus attention to the rules administered by NCS that govern emergency access to such networks. DOJ will help prepare future initiatives to define the responsibilities of carriers to provide government emergency communications services in future emergencies. Realization of these capabilities would then be factored into planning the architecture of DOJ access and backbone networks.

### *Wide-area Networking*

Irrespective of whatever else DOJ invests in, it needs a viable, low-cost, wide-area networking solution to connect its offices and headquarters. The current Justice Consolidated Network (FBI aside) runs roughly 500 megabits per second into an ATM backbone. When, not if, the rest of DOJ adopts patterns of network demand that the FBI will (once Trilogy is complete), it can expect a tenfold demand increase – and that is not even counting the expected year-to-year growth in the installation of bandwidth-hungry applications (e.g., to support collaboration, or wireless connectivity). Wide-area networking solutions that are affordable at 500 megabits per second do not scale to affordability with one or two orders of magnitude more demand.

It is also important that DOJ's WAN infrastructure maximize flexibility so that the system as a whole is robust against failure (e.g., losing one component does not lead to a global breakdown). The WAN's architecture should also pose no barriers to information sharing and collaboration across components.

#### *State of the Art and Current Trends*

The forces that drive access network technology also affect wide-area networking. De-regulation has created competition for long-distance voice services, and data services. The late 1990s saw new fiber-based backbone data networks and sharp declines for both data and voice services. The restructuring of the telecommunications industry highlighted an apparent excess of long-haul bandwidth and put companies, both new and old, in financial difficulties.

Wide-area networking includes not only long haul circuits, but also metropolitan area networks (MANs), which remain an important component in DOJ's backbone network. Their

existence provides a major source of competition for connecting sites in the same city, and a potential way to aggregate traffic for a DOJ long-haul backbone.

DOJ's networks are IP based. These IP networks must be implemented with one or more link technologies providing transport between DOJ locations. In addition to leased lines, there are extensive national and metropolitan networks that offer ATM and Frame Relay services, available from multiple operators, which can be used to construct DOJ's IP networks. These ATM and Frame Relay networks are typically public networks that switch the traffic from multiple customers over common links and switches in their backbones. VSAT technology is also a candidate, but requires a careful thought about how to tradeoff the limited bandwidth and long latencies of a VSAT against the advantages of a non-terrestrial path between routers.

Although ATM and Frame Relay have extensive legacy networks likely to stay lit for years to come, they are facing increasing competition from fiber optic technologies (e.g., IP over SONET, IP over physical fiber, Ethernet over MANs) in linking IP routers. The slow improvement rate of line cards for ATM and Frame Relay switches contrasts with much faster improvements in line cards that support SONET or fiber directly. The advent of dense wave division multiplexing may accelerate improvements in the costs of transporting bits. True, both ATM and Frame Relay (over an ATM backbone) support prioritization of traffic, and can be somewhat simpler to use. Yet, PVCs can be used to allocate increments of bandwidth between routers in IP networks with only minimal consideration of the underlying physical connections. UBR, VBR and CBR choices offer different ways to prioritize the traffic placed on different PVCs sharing the same physical facilities. In an IP over fiber network, a more complex performance analysis is required because the transport mechanism does nothing to manage the bandwidth of the physical circuit. Mechanisms, such as MPLS, are being introduced to help manage and provision bandwidth in these "pure" IP networks, as well as prioritize traffic based on QoS criteria.

ATM, Frame Relay, SONET, Ethernet, and fiber are all technologies suited for building a private IP network. VPN technology, which permits traffic to be encrypted and tunneled through the Internet, can permit the Internet itself to be an alternative backbone facility for DOJ.

*How Can Technology be Used?*

DOJs networks are IP and will remain so. In the next five years, IPv4 is likely to remain the dominant version of IP. If IPv6 emerges in that time frame, it will probably do so with wireless networks used for mobile access. If it does, DOJ will need an IT strategy for achieving interoperability of its mobile, wireless data networks and its backbones.

Ultimately, WAN strategies are issues of bits-per-dollar, once security and redundancy requirements are satisfied. In a world in which relative prices shift drastically from one year to the next, flexibility is essential in garnering the lowest price. Conversely, locking into one technology to the exclusion of others is generally unwise. While national ATM and Frame Relay (over ATM) are likely to continue in operation in the next several years, they are not likely to offer the most cost effective solution, given technology trends.

## Appendix B
## The Prospects for Technology Insertion White Paper

The current contenders for WAN service are Frame Relay (over ATM), ATM, and IP networks – the last of which might be based on a carrier's shared IP network including the Internet itself. There is little question that economics, and the relative availability of networking equipment, are increasingly favoring native IP transport. The actual prices charged for such services will vary by location and circumstance and there are real limits to how often one should change technologies based on momentary price advantages. At any one point in time DOJ's WAN infrastructure may use a mix of Ethernet, native IP and ATM. Nevertheless, the trends are clear. Early indications are that a public IP solution is already five to ten times less expensive per bandwidth than an ATM solution. All DOJ IP networks should be designed in a way that anticipates the use of multiple technologies and that minimizes the impact of substituting one carrier for another.

The lowest-cost solution, putting DOJ entirely on the Internet, however, exposes DOJ operations to the vagaries of the Internet. The obvious threat is from viruses/worms and hackers. This threat, however, comes from any exposure to the Internet, such as comes from the DOJ gateway in Rockville. The less obvious threat, and one that ATM systems are not nearly as prone to, is from a denial-of-service attack. One type is a failure in the Internet's routing and addressing infrastructures; another type is attempts to flood the connections used by specific users (e.g., the February 2000 distributed denial-of-service attack aimed at various E-commerce web sites). It should be noted that a denial-of-service attack that saturates links between routers could affect ATM systems indirectly, if ATM (UBR) is being used to implement a saturated link.

IP solutions, as such, come in two flavors: private and public. A *private* IP solution for DOJ would be designed so that internal connections would be safeguarded even if connections to the rest of the world were imperiled; in effect, there were be an ISP-maintained firewall between DOJ and the universe. There are two ways to do this: in hardware (e.g., air-gapping) or through software. Given the near-impossibility of a hardware solution, exactly how "private" such a service would be can only be judged by evaluating the ISP and carriers used to build the DOJ IP network.[6] A *public* IP solution means connecting DOJ up to the Internet one node at a time. This requires replacing DOJ's one firewall (to ward off hackers and viruses/worms) with hundreds or thousands of firewalls. Unless and until the various threats to the Internet have somehow mitigated themselves, this is a viable solution for DOJ only if: (1) adequate backup were present, and (2) multiple firewalls could be configured and administered as though they were one.

Recovery and reconstitution of the DOJ WAN also need attention. Point specific faults (e.g., equipment failures, fiber cuts, etc.) are common and their effects should be anticipated and mitigated in an IP network design. These are more likely than region-specific failures (e.g., from major terrorist incidents, weather-related problems), which are more likely than nationwide-failures (e.g., from a wholesale Internet attack, or nuclear events). Thus, a backup plan or system in which unexpected local demands (e.g., as people reroute their communications away from damaged facilities) can be accommodated as part of a nationwide communications fabric are preferred. Space-based capabilities (e.g., in extant VSAT networks to geosynchronous satellites) have some

[6] For example, if a public ATM (UBR) service were used to implement the paths in DOJ's IP network, it could be susceptible to an Internet link saturation attack if it shared a physical facility with the Internet.

very attractive features and merits aggressive pursuit. That noted, because of limited transmission capacity, many large emergencies will require limiting capacity utilization to the most critical applications.

DOJ's strategy is therefore to plan on an IP-based WAN and investigate the relative economies and security implications of private versus public solutions to security issues (a private solution would have to include sufficient peering points). The plan includes the active pursuit of space-based backup.

### *Precision Security*

Notwithstanding the many dimensions of security (e.g., ensuring hackers do not control system functions), precision security is the art of ensuring that read and write privileges to information are strictly limited to those people specifically authorized to do so. Precision security is an important component of information sharing and collaboration; without ironclad assurances that the circulation of information is limited, many DOJ components will not share with others – and deservedly so.

*State of the Art and Current Trends*

DOJ requires secure information systems having four main elements:

- *Authentication*: the ability to ensure that transmissions and messages, and their originators, are authentic, and that a recipient is eligible to receive specific categories of information;

- *Data integrity*: to ensure that data are unchanged from their source and have not been accidentally or maliciously altered;

- *Nonrepudiation*: to ensure that strong and substantial evidence is available to the sender of data that the data have been delivered (with the cooperation of the recipient), and, to the recipient, of the sender's identity, sufficient to prevent either from successfully denying having sent or received the data. This includes the ability of a third party to verify the integrity and origin of the data;

- *Confidentiality*: to ensure that information can be read only by authorized entities.[7]

The phrase "precision security" stresses the need for a system in which individuals take on one or more *roles* within the organization that bring with them certain access *privileges*, but in a dynamic environment in which roles and responsibilities change, requiring information access privileges to be revised promptly.

[7] These definitions and other portions of the discussion in this section are taken from Neu, Anderson, and Bikson (1999) *Sending Your Government a Message: E-Mail Communication Between Citizens and Government*. RAND MR-1095-MF, Chapter 5.

## Appendix B
## The Prospects for Technology Insertion White Paper

The standard way to provide precision security is to adopt a public key infrastructure (PKI) system. Such a system would be defined within a single organization but permit specific other individuals (e.g., within other government organizations, or cooperating foreign government agencies, or private sector organizations involved in a legal case or other DOJ matter) to participate on a limited, specific basis.

PKI systems, although once quite exotic, are now available as commercial off-the-shelf systems (COTS) by providers such as RSA Security Inc. (http://www.rsasecurity.com), Verisign Inc. (http://www.verisign.com), and CertCo Inc. (http://www.certco.com).

PKI systems provide each user with one or more key pairs: a public key known to the user's correspondents, and a private key known only to the user. These keys can be used as encryption keys (to ensure the confidentiality of messages) or as signing keys (to confirm the identity of the sender). Such systems provide certificate authorities (CAs), which are trusted organizations (e.g., an agency given this responsibility within the DOJ) that "certifies" that a particular public key is associated with a specific user. Such a CA would demand proof of identity before issuing a digital certificate binding a public key to a user. The CA must also provide such services as replacing certificates that have been lost or compromised, publishing directories of public keys, and assisting users.

Within a PKI, it is common to distinguish between identity certificates (described above), and authority certificates that grant an individual user specific information access or other well-defined authorities.

A substantial survey of PKI systems is outside the scope of this appendix. However, there are many reference texts available with descriptions of PKI systems. Among them are a report by the Computer Science and Telecommunications Board of the National Research Council (1996)[8], and a more technical treatment in Schneier (1996)[9]

There exists a Federal PKI Steering Committee located within the General Services Administration. The mission of this committee (see www.cio.gov/fpkisc) is:

> ... to provide clear, strong leadership within the U.S. Federal Government during the development and implementation phases of the Federal PKI. The Federal PKI Steering Committee will provide guidance and assist in the development of an interoperable public key infrastructure that utilizes commercial-off-the-shelf, standards-based products and services for a myriad of applications with a goal toward ensuring standards-based approval. However, it is recognized that certain unique applications may require that modifications be made to commercial products. The Steering Committee will: Identify Federal Government PKI requirements,

[8] Computer Science and Telecommunications Board, National Research Council (1996) *Cryptography's Role in Securing the Information Society*. National Academy Press.
[9] Schneier, Bruce (1996) *Applied Cryptography*, second edition. New York: John Wiley & Sons.

recommend policies, procedures and standards development activities that support a Federal PKI, provide oversight of PKI activities in Federal PKI pilot projects, provide oversight and guidance on the establishment of key recovery techniques, specify technologies needed for a Federal PKI, establish and maintain liaison with appropriate communities of interest, establish interoperability and security requirements of products and protocols related to the Federal PKI, and make recommendations regarding establishment, demonstration, and operation of a Federal PKI.

Perhaps the most significant adopter of PKI systems for information security within the U.S. government is the DoD. The Defense Information Systems Agency (DISA) is coordinating these developments.

Due to the importance of information security throughout DOJ operations and agencies, we expect that DOJ would be an *early adopter* of PKI technology, obtaining support and guidance from the Federal PKI Steering Committee to assure that its systems were compatible with other U.S. government PKI initiatives. The "adopter" role is appropriate because PKI security is available in various relevant forms from a variety of commercial providers. It would seem most likely that the DOJ would desire to retain certificate authority procedures in-house, although the administrative burden of issuing, verifying, and revoking certificates as needed – as well as providing user training, education, and help facilities – can be substantial.

*How Can Technology be Used*

The fundamental requirement for precision security is the ability to recognize specific individuals and accord them their proper access privileges. Given the difficulties of passwords (e.g., they may be easily guessed or accidentally revealed), true security requires either a biometric or a token-based device. This, in turn, requires that access to SBU data be accessed only through machines capable of reading tokens or obtaining biometric information. The existence of PCMCIA cards or "memory sticks" for palmtops suggests that such devices do exist. Alternatively, the same digital fingerprint capturing devices employed as part of JABS may be available to double as authentication devices to SBU systems. Access privileges authenticated in that way can then be applied to specific collaboration environments and case files. In support of such devices, DOJ in particular, and the law-enforcement community in general would develop an infrastructure of public keys (PKI).

Software aside, administration has always been the major challenge in the practical implementation of public key systems. If the system is too small, then it will have to handle too many exceptions; if it is too large, then a complex arrangement of key servers trusting other key servers will be necessary. Although issuing keys is straightforward (access lists can be created one-at-a-time, as administrators require), revoking them requires a detailed review to find which systems have to be alerted. Until that far-off day when a global and trusted public key infrastructure exists, DOJ would concentrate on the requirements of the nation's law-enforcement community: federal law-enforcement agencies plus selected counterparts, from foreign, state, local, and tribal

governments (with the participation of the intelligence community to be determined). This would be a total population unlikely to exceed 200,000 -- well within the capabilities of a single (albeit well backed up) server. At its steady-state, such a system might have to issue as well as revoke roughly a hundred keys a day; again, no larger than a single office could deal with.

U. S. Department of Justice
Information Technology Strategic Plan

# Appendix C

# Infrastructure Strategy

# White Paper

**Appendix C**
**Infrastructure Strategy White Paper**

# Background

Infrastructure can be defined as the collection of information technology (IT) elements that provides the technical features and capabilities necessary to implement business functions. It encompasses the layering of technology capabilities from applications through telecommunications as shown in Figure 1. Specifically:

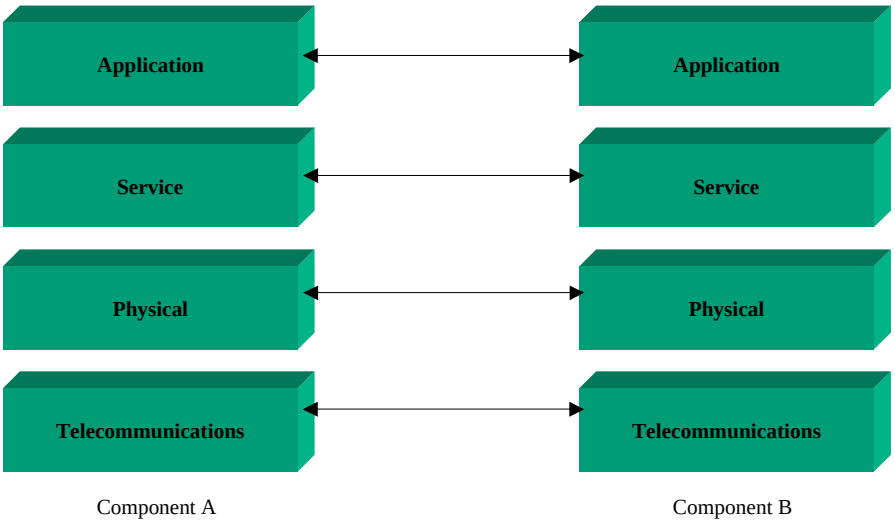



**Figure 1**

- The application infrastructure consists of the programs that implement and automate business functions. These may be either custom developed to provide a unique business capability or commercial-off-the-shelf to serve in a more general role.

- The service infrastructure consists of intermediate and often general-purpose services upon which applications may be built. This infrastructure layer includes components like programming languages, electronic mail transport systems and user authentication services. The service infrastructure is build from physical infrastructure elements.

- The physical infrastructure consists of the commercial products used as building blocks for the services infrastructure. They include computers, software packages, cables and other tangible products that are assembled to build the more complex service infrastructure.

**Appendix C**
**Infrastructure Strategy White Paper**

- The telecommunications infrastructure provides connectivity between upper infrastructure layers. It consists of the wide and local area networks as well as wireless data, land mobile radio and plain old telephone service (POTS).

The Department uses numerous large and small IT systems to support its missions and objectives. These IT systems provide the computing infrastructure with which the business processes of the Department are automated. The infrastructure components are usually owned and operated by the various Justice organizations that use them, with a few exceptions. For example, wide area telecommunications data infrastructure is often leased.

JMD operates two central data centers that consolidate computing functions. The JMD data centers provide a centrally operated and managed computing resource exhibiting high availability through the use of mainframe computers maintained by a 7 by 24 staff (i.e., 24 hours day, 7 days a week). As IT evolves, the mainframes are giving way to farms of UNIX and Windows servers. Located in Rockville MD and Dallas TX the two data centers provide geographic diversity with the goals of providing mutual backup capabilities (high availability) and computing resource consolidation (cost containment). In actuality, the two centers lack the redundant telecommunications needed to support a seamless fail over from one to the other in the event of a critical failure of either. Additionally, the two centers provide only a limited subset of common computing services resulting in a limited and highly manual fail over process. There are computing resources located at component locations across the nation as well. Although, redundancy exists in some systems to support fail over, there are no Departmental standards for availability or survivability of the IT infrastructure. Each component must provide contingency planning as part of the certification and acceptance process but the plans many times do not always provide for reasonable IT continuation during the loss of critical IT infrastructure.

The Department has implemented office productivity desktop services through the Justice Consolidated Office Network (JCON). It consists of standard desktop software and centralized electronic mail, file storage and help desk services. JCON consolidates and standardized desktop capabilities to a significant degree. Still, JCON installations can be tailored to meet individual component needs, thus diluting the intent and leverage of a standard desktop. For example, both Microsoft Office and Corel Perfect Office are available to desktop users. Although there are somewhat compatible data formats in common to the two packages, many times information exchanges between users are cumbersome – document formats do not convert well from one product to another. JCON operates on the individual component's local area network (LANs) under a wide range of performance parameters, security conditions, and trust relationships. Also, JCON usage is not mandatory for the components. In particular the largest components have pursued their own unique solutions to providing desktop applications resulting in unacceptable interoperability among desktop users.

One of the biggest problems with the current IT infrastructure is the Department lacks an overall policy on how engineering decisions should be made to permit interoperability across the enterprise. Currently, the Enterprise Architecture exists as highly independent and fragmented component architectures. Each component has developed IT systems and solutions with only

secondary regard for the enterprise. Interoperability is typically engineered on a per system, per mission basis without Department wide standards or interoperability guidance. This fact often makes unplanned interoperability a major undertaking for each new requirement and can force crisis development and deployment efforts to establish new interoperability when urgent events arise.

The Department performs many diverse business functions ranging from financial management, law enforcement and litigation, among others. Each of these functional areas has supporting applications operating in a legacy infrastructure environment consisting of "stovepipe" systems and data supporting unique business functions. Some server consolidation has occurred; mainframe computers host applications from several mission areas. However, to date, the Department lacks an overall plan for developing applications and systems with respect to the complete enterprise, resulting in disparate islands of IT infrastructure within each component. Each component, being focused only on their specific missions, has developed systems and applications without a view of the Department enterprise resulting in a plethora of overlapping and non-interoperable applications and databases.

The services infrastructure suffers from the same silo approach that impacts application interoperability. Systems like electronic mail have limited usefulness because the implementers approached it as a communication tool to be used within the component rather than throughout the Department. This has resulted in the use of several different email systems that provide only the most basic interoperability and restricts, to the component's domain, many advanced features (e.g. calendaring and public folders) desired by the users at an enterprise level. Other services have been implemented using similar narrowly focused approaches, resulting in systems that often work very well within a component, but do not interoperate well at the Departmental level.

The physical infrastructure is varied and diverse. Each component has selected products to implement its infrastructure with little Departmental guidance. The various component data centers operate a wide range of hardware and software. The use of features unique to a specific vendor limits the portability of applications and services.

Efforts to consolidate the telecommunications infrastructure have had mixed success. Although the Justice Consolidated Network bundles and resells bandwidth based on standard protocols, it has failed to gain critical mass, where the projected cost savings have been realized. There are still large numbers of dedicated leased point-to-point circuits in use throughout the Department.

## Vision

The Department requires seamless interoperability between IT systems. This goal can be met with a unified IT infrastructure. A unified infrastructure specifies horizontal and vertical interoperability guidance for each of the infrastructure layers shown in Figure 1. This goal must be met within the context of affordability. The following features outline a vision and direction for the Department's computing infrastructure that will satisfy current and future business needs.

**Appendix C**
**Infrastructure Strategy White Paper**

Information Exchange – With a unified infrastructure, interoperability will provide users access to the right information at the right time. To meet the Department's data sharing goals, authoritative databases must be available to appropriate users needing the information they contain from anywhere within the enterprise. Fundamental to meeting the goal of data sharing is information protection and security. Users must be authenticated and exhibit the need to know before being granted access to critical Department data. Technologies are evolving, particularly in the area of knowledge management, to allow subject matter experts to extend their reach throughout the enterprise. Data mining and other analysis tools provide users the ability to access and examine views of information of their own choosing. No longer will it be acceptable to require a programmer develop a unique application to provide a unique view of information, as this flexibility can be given directly to the user. Systems will be able to exchange information throughout the enterprise. Data definitions will be universal within the Department.

Flexibility and Adaptability – The unified infrastructure will respond to changes in requirements without requiring extensive changes to the infrastructure. Systems must exchange information on demand using universal data formats and exchange mechanisms. It is no longer acceptable to have multiple systems deployed that perform the same job. Standardization of applications across the Department will allow the use of systems that can serve a number of the components. Systems must be extensible to meet the unique requirements of specific components while allowing the maximum reuse of software, common to all components. Networking will become ubiquitous. It will no longer be necessary to engineer a communication path to support a new data exchange requirement or application.

Ubiquitous Computing - The unified infrastructure will allow Department users to access their systems from anywhere in the enterprise. The reach of enterprise computing will expand with the introduction of wireless data technologies and hand held computing platforms. Additionally, the deployment of secure integrated networks will provide the user access to the systems and applications they require to complete their jobs anywhere in the enterprise. This provides significant advantages for disaster recovery and contingency planning. With few exceptions, all Departmental workstations should support the execution of a common set of core Department applications developed around a common application reference architecture.

High Availability – The unified infrastructure can help meet the critical goals of high availability. As computing becomes more important to performing the Department's functions, it is critical that systems be available when needed. Redundancy in the infrastructure allows high availability by providing redundant communications and services upon which applications are built. Standardization of platforms and ubiquitous networking provides portability of applications.

Predictable Development – As the Department's applications become more complex and widespread, the acquisition and development processes become critical to meeting the Department's goals. This plan envisions planning via the Enterprise Architecture process. This planning will precede a unified acquisition and development process to support the introduction of infrastructure into the Department. This process shall use metrics and public reviews to

inform the user community and program sponsors of the status of acquisition and development efforts. User involvement will occur at all stages of the acquisition and development process.

## Strategy

The Department requires a unification of the infrastructure through the systematic modernization of the application, service, physical and telecommunications infrastructure layers. The Department must build infrastructure using an enterprise infrastructure architecture. Specifically this architecture must address.

- Interoperability – Applications, services and telecommunications should be based on an enterprise architecture implemented with technology and configuration standards to facilitated interoperability among component systems at all levels of the infrastructure. Interoperability should be general purpose and "matter of fact." Changes in missions should require no or minimal changes to the infrastructure.

- High Availability – High availability systems are those that have sufficient redundancy to resume mission operations after the failure of one critical component, after an acceptable fail over interval. High availability functions can be achieved through component redundancy and geographical diversity within a framework or process for fail over. Each business function along with its supporting mission critical application must be evaluated to determine availability requirements. These requirements will then be used to determine the degree of redundancy required and a suitable fail over process and strategy. Ubiquitous networks will allow the centralization of mission critical systems into a few high availability data centers, which can serve as mutual backups. The data centers will possess telecommunications diversity, redundant power and environmental systems, appropriate physical security and a trained staff of operators and technicians.

- Component Portability and Reuse – Software will be developed so that it can be reused to support like functions at different components. Software objects must be supported as libraries for reuse within multiple applications. Applications must be developed around a reference architecture to allow common or core capabilities to be developed once and shared by all systems needing the same functionality. The reference architecture must be extensible to allow adding component or mission specific software components to augment the capabilities of standard applications and libraries. All applications should share a common set of user interface (UI) characteristics and behavior.

- Enterprise Development - The Department must develop a business process for IT system acquisition and development. Formal processes for major and significant systems, incorporating public reviews, will provide management and users insight into the progress and effectiveness of the pending solutions pertaining to acquisition and development efforts. The overall process must address all areas of the system life cycle to

include requirements definition, development or acquisition, operations, maintenance, testing, training, certification and acceptance, and end-of-life-disposal.

## Recommendations

The following recommends are made:

1. Assemble a team to produce an enterprise infrastructure architecture. This team should be led by the JMD/IRM/IMSS Enterprise Architecture Group with participation from the components. This group will collaborate as a team in a sustained effort until the architecture is published.

2. Evaluate the current component infrastructure architectures for points of unification. Consider unifying email services, directory services, office automation and other easily identifiable compatibilities to determine the feasibility of implementing near term fixes to common problems.

3. Commence the development of a public key infrastructure (PKI) solution to address the security needs of the unified infrastructure. The unified infrastructure can create significant security vulnerabilities if not designed within the context of a comprehensive, integrated security architecture implemented with appropriate technologies. Federal agencies are beginning to deploy PKI. It appears that PKI can help meet the needs of the Department with respect to securing the IT infrastructure. Since a number of the components are beginning PKI deployment, this recommendation brings those projects together with the goal scaling these integrated initiatives to meet the PKI requirements of the Department.

4. Develop an Application Reference Architecture (EAG). This architectural component describes the mandatory interfaces, standards, and services to be used in the development of applications programs. Additionally it describes an application framework for software delivery and extensibility. Recommend the EAG commence identifying application segment architectures based on Departmental business areas.

5. Develop a list of approved technology products to address standardization of the physical infrastructure layer.

U. S. Department of Justice
Information Technology Strategic Plan

# Appendix D

# Department of Justice Telecommunications Strategy

# White Paper

**Appendix D**
**Telecommunications Strategy White Paper***

Telecommunications at the DOJ comprises data networks, conventional voice networks, and wireless networks that include cell phones, radios, and data devices such as Personal Digital Assistants. This material focuses primarily on the strategy for the DOJ's data networks.

# Background

Almost all of the DOJ's data networks are based on the TCP/IP protocol family. These IP networks are implemented using a variety of technologies that include leased lines, Asynchronous Transfer Mode (ATM), and Frame Relay circuits. There are a few exceptions to this rule, e.g., video conferencing services, and these exceptions are evolving to IP networks. Generally, these specialty service networks have been developed and operated by DOJ components.

The DOJ IP network is a "network of networks" Viewed from an IP-perspective, the DOJ network comprises a number of independent, national networks developed and operated by each of the major DOJ components. These individual networks are generally hierarchically organized, reflecting the organization structure of a DOJ component, as illustrated in Figure 1. The heavier lines in this figure are wide-area network connections (discussed later in this section). Each office building has a local area network. Each DOJ component network has a headquarters site that acts as the communications hub for that DOJ component. Interconnections between DOJ components are typically done between headquarters sites (usually in metropolitan Washington, DC), via the Justice Management Division (JMD) network. Connections with other outside entities, including other Federal agencies and the JMD-provided services (such as Internet access and an e-mail gateway), are typically performed through a DOJ component's headquarters site as well.

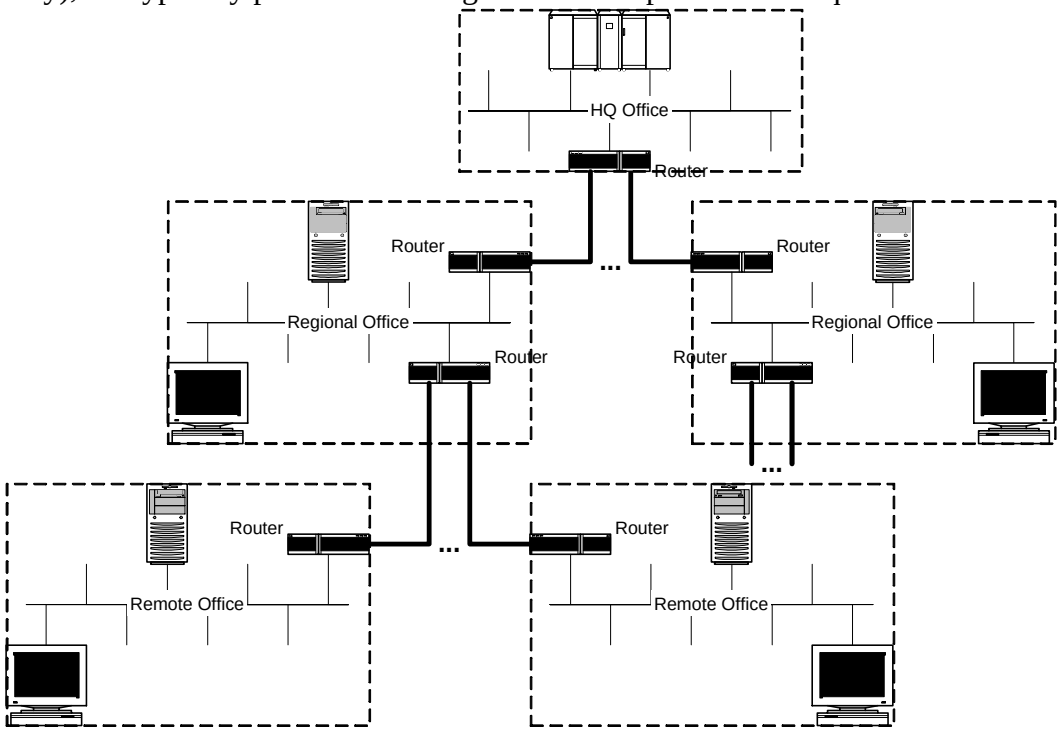



**Figure 1**

**Typical Organization of a DOJ Component Network**

* This White Paper is based on unpublished material prepared by the Rand Corporation for the Department of Justice.

## Appendix D
## Telecommunications Strategy White Paper

The MAN or JMD network is not a national network, but primarily serves the Washington, DC area. It provides transit for traffic exchanged between DOJ component networks (horizontal sharing); common services such as an e-mail translation service, a gateway to the Internet, and external web servers; and provides access to shared data centers. These network relationships are illustrated in Figure 2.

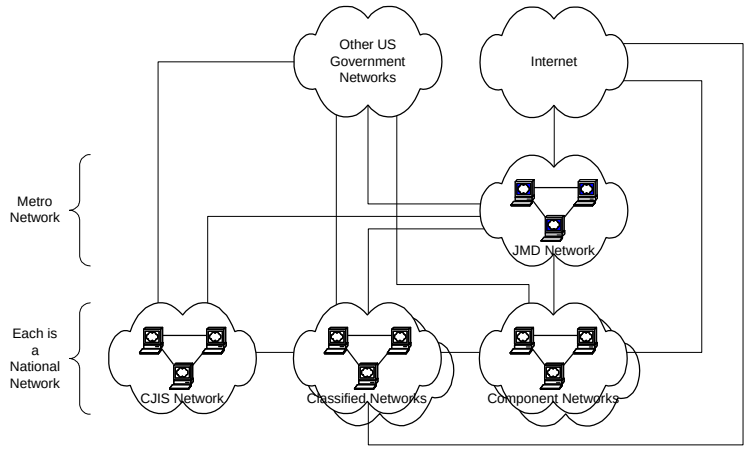



**Figure 2**

**DOJ Networks and Their Relationships**

Figure 2 represents the details of individual DOJ component networks as a communications "cloud". Each of the component networks (as well as some of the classified networks and CJIS) is national in scope and has an implementation similar to the network shown in Figure 1. Figure 2 suppresses many important details. For example, it does not show firewalls, gateways or specific hosts. It is intended to label the types of existing networks and shows a simplified view of the connectivity among them.

The DOJ component networks include unclassified networks, generally carrying Sensitive, But Unclassified (SBU) traffic; classified networks (such as those serving the FBI and DEA); and the network enabling vertical sharing of information with local and state law enforcement agencies – the Criminal Justice Information System (CJIS) network.

There is a DOJ-wide policy stating that the JMD is to provide the only Internet access for the DOJ as a whole, in order to assure a common policy governs security functions such as screening for viruses, and intrusion detection. In addition to dial-in access, the JMD is now piloting Virtual Private Network (VPN) functions that provide secure access to the DOJ's networks from home, hotels, and other remote locations with access to the public telephone network. In practice, there are additional direct connections to the Internet, other than that provided by the JMD (e.g., the connection maintained by the BOP). Many DOJ components maintain dial-up access to the Internet from individual machines, dedicated to this purpose. Some provide dial-in access from the Internet. The JMD also provides a dial-in access service to most DOJ networks. Each of

these additional points of interconnection with the Internet or other external network is managed by a different DOJ component with a potentially different policy about security. Multiple policies weaken DOJ's overall security posture against external threats.

The DOJ's IP networks are built from a variety of public network technologies and services. The DOJ has been pursuing a strategy calling for *all* DOJ networks, including classified networks and CJIS, to be built using the Justice Consolidated Network (JCN). 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. About two-thirds of all of the DOJ's unclassified network locations are serviced by the JCN.

In late 2001, a decision was made to exempt the FBI's Trilogy project from using the JCN. The waiver allowed another supplier, MCI, to be used to expedite the FBI's network and Office Automation (OA) upgrade project. The FBI's network is a completely classified network. It has a strategy that calls for the development of a trusted guard that will connect it to the JMD network for the exclusive purpose of delivering unclassified e-mail.

The JCN was conceived to promote information sharing while minimizing total DOJ costs for data network services. The cost savings have been marginal. This was a consideration in the decision to rebuild the FBI's network using a second supplier. The information sharing objective has not been realized either. The DOJ operates multiple national networks, each serving a DOJ component. Sharing of an application between DOJ components (e.g., an application run by one component, and accessed by another) requires a customized connection between hosts residing in each component's network. Sharing of data between DOJ components is typically done by regularly extracting a copy of some subset of data "owned" by one DOJ component and providing that extract to another DOJ component under the terms of a Memorandum of Understanding (MOU) governing its use. Extracts are typically communicated as a file transfer between DOJ component networks or through some other media such as tape.

## Vision

The DOJ Information Technology Strategy is based on a vision of a DOJ-wide, national network that enables data and application sharing. Such a network will continue to be based on the TCP/IP protocol family, since this is the dominant industry standard for all applications, operating systems platforms, and network equipment. A single, national IP network, rather than the current arrangement of multiple national IP networks is the best solution to achieve this critical Department objective.

A single, national IP network provides the foundation for implementing DOJ-wide policies that reduce barriers to information and application sharing among components while advancing overall security. This network should be a Department utility that serves *all* DOJ components. A

single, Department network provides any-to-any communications between DOJ components. This is the critical first step in a DOJ-wide information-sharing infrastructure. The network should be accompanied by a security infrastructure that is discussed in another section of this report. The vision for a Department data network is illustrated in Figure 3.

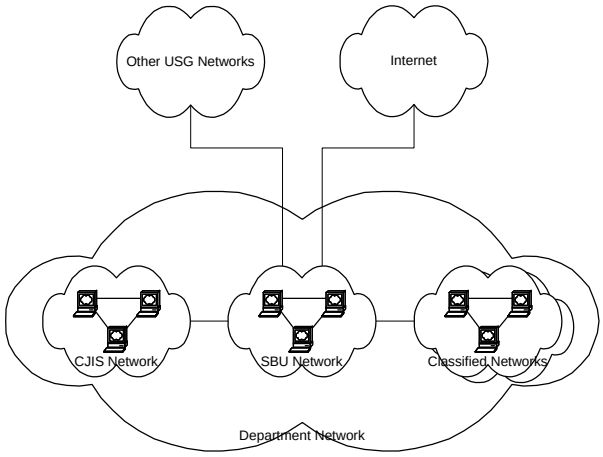



**Figure 3**

**Vision**

Every unclassified DOJ component network currently makes an independent decision on how to implement the transport of SBU traffic. Some DOJ components encrypt all traffic over public links; others do not encrypt SBU traffic over any links. A single, Department network for SBU traffic assures that there is a uniform policy for how SBU traffic will be carried. A Department policy, if based on encryption of traffic over public links, would improve security for the entire DOJ.

A Department network provides for clear accountability. One organization is accountable for end-to-end communications. This is a critical enabler for sharing of applications and data collections among DOJ components. Today, the goal of sharing an application or data can be defeated by conflicting priorities and commitments made by multiple DOJ component organizations that must make changes to their separate networks to enable sharing.

A critical element of any security strategy requires that interconnection of the DOJ's network to non-DOJ networks be carefully managed. The Department SBU network would define the perimeter for a DOJ-wide defense against external threats. DOJ must connect to the Internet, other US Government networks, State, Local, and Tribal data networks, and private networks in the public sector. The nature of these interconnections includes direct access, dial-up access, and virtual private networks. A uniform policy governing firewalls, virus scanning, and intrusion detection can be implemented at these points of interconnection. A Department network can minimize the number of interconnections to external networks. It can eliminate duplicative

efforts to monitor such interconnections. It can reconcile conflicting policies governing how multiple interconnections are operated (e.g., what viruses scans are performed).
Data networks are fundamental to the DOJ's daily operations and the execution of its mission. Interruptions of data connectivity must be managed in terms of frequency, duration of outage, and effort required to recover from the interruption. A Department data network can eliminate duplicate network contingency planning efforts in DOJ components, and promote effective and efficient network contingency planning DOJ-wide.

Every data network must be managed. A wide-area network supplier who already provides high-quality network management for its network should be selected to provide and manage the DOJ network. Such suppliers also provide managed network services for network equipment on customer premises. Currently, many DOJ components staff a network management center for their national network, and these, in turn, are further duplicated by the JCN network management center. A supplier-managed, Department network can eliminate the duplicate network management functions that are performed today by DOJ components and the JCN. Service level agreements should be employed to assure that the supplier's network management services meet *all* DOJ needs. Properly managed, a Department network would let DOJ components streamline their help-desk operations to focus on their information systems.

It is also important for DOJ employees to be able to access their networks, applications, and data stores when away from their desktops. Future demands for remote access will go beyond dial-up. They will also require access from offsite work locations, travel locations (e.g., hotels and airports), meeting sites, courtrooms, residences, and, indeed, wherever an employee happens to be when he or she needs to get work done. Wireless Ethernet (802.11b) hotspots are but the latest such opportunity for remote access.[1] Wireless access may range from broadband (e.g., from suitably-equipped homes, work sites, and hotels) to more restricted wireless connections. Indeed, remote access links ought to be able to support high-bandwidth big-screen clients as readily as low-bandwidth small-screen (e.g., PDA) clients. They also ought to be broadly compatible with commercial services regardless of their manifestation (e.g., second-and-a-half generation wireless). Finally, remote access methods should complement normal network methods should the latter be unavailable in crisis or emergencies. Both wire line and wireless access to DOJ's SBU network should be viewed as a Virtual Private Network, tunneled through the Internet, connecting a PDA or computer to the Department SBU network, and providing SBU-level encryption for traffic in the tunnel.

## Strategy

Understanding and satisfying comprehensive data communications requirements for all of the DOJ's components is no small task. The input of each DOJ component is critical. This statement of telecom strategy does not pretend to be a comprehensive set of requirements for a Department network. However, the following strategy reflects requirements that would be part of any complete set of requirements for a Department network.

## Appendix D
## Telecommunications Strategy White Paper

*Create a Department network that provides one transport fabric*. A Department network should not require provisioning of either real or virtual circuits to implement sharing of applications or data by DOJ components, if their offices are already provisioned with access to the Department's national network. At present, DOJ components' networks do not meet this requirement. A Department network must be based on one, DOJ-wide, national backbone network (potentially assembled from multiple supplier's networks to assure competition and redundancy). The existing DOJ component national backbones should be combined into one national backbone. Such a national backbone should have sufficient performance and redundancy to meet both the operational and contingency plans for the DOJ, as a whole. Performance and continuity of operations should be examined and implemented at the Department level. The backbone must satisfy a consistent DOJ policy for providing performance and continuity of operations that meet the needs of *all* of the DOJ's components. Decisions about the capacity and redundancy used to connect an individual office to the backbone can be tailored to the specific needs of an office connected to the backbone.[1]

*Create a Department network that provides one service fabric*. A Department network should provide adequate performance for *best effort* data services.[2] It should also be able to support video services, and IP-enabled voice services with a single network, anticipating that DOJ components will develop the business cases justifying such services. Such services have more demanding performance requirements than best effort data services.

*Create a Department network that provides a DOJ-wide approach to protection against external threats.* As a matter of policy, all on net, DOJ data (including video and voice) traffic should be considered to be at least SBU. The transport fabric should encrypt all data carried over public facilities (i.e., a supplier's network providing the wide-area data services used to implement a Department network) using commercially available, NIST and NSA certified encryption products. There should be a Department policy governing the exchange, filtering, and monitoring of traffic with non-DOJ networks interconnected with the SBU network. This enables clear accountability at the Department-level for defense against external threats. Type I encryption should be added to support mission specific needs. Classified networks and networks used to connect to external partners (e.g., CJIS) should ultimately transition to VPNs within the overall DOJ network. The classified networks would have an additional layer of encryption and be tunneled through the SBU network. There should be a Department-level policy governing the interconnection of the Department SBU network with classified networks and the CJIS network that establishes clear, Department-level accountability for the implementation of the policy.

[1] Access and backbone redundancy should consider VSAT technology as an element of the Department network. In addition to path diversity that reduces common failure modes (e.g., damage from an earthquake), VSAT technology may be the most cost-effective way to reach some remote offices (e.g., those associated with the border patrol and immigration).

[2] *Best effort* data services are those provided by the IP protocol. The transport network makes no guarantee that a packet will be delivered. Applications must choose to use an end-to-end protocol such as TCP to guarantee delivery of a packet.

All forms of remote access to the DOJ's SBU network raise security issues. The Department network should access the Internet from a controlled number of points (for redundancy of the service) subject to a common policy for exchanging, monitoring and filtering of traffic. VPN access (tunneled through the Internet) to DOJ's IP networks should follow suit. A VPN (tunneled through the Internet) should extend dial-in access to include common forms of broadband access and wireless access. A wireless VPN gateway should be a DOJ-wide service. It should be centered on support for commercial off-the-shelf wireless data devices, e.g., the RIM Blackberry. DOJ should also specify a DOJ standard PDA and mobile computer configuration that implements a secured VPN.

# Recommendations

The DOJ should phase out the JCN and the Metropolitan Area Network (MAN), and apply lessons learned to the implementation of a Department data network.

- PVCs are not cost effective. The JCN has demonstrated that it is not possible to rapidly deploy either (permanent) virtual or real circuits to accommodate a new configuration of an application and its clients. PVCs do not scale with new applications that are required by DOJ components. For example, a full mesh of PVCs is required to provide the performance and connectivity the EOUSA requires between its PBXs to implement an converged IP backbone for its voice and data services.
- Currently, many DOJ components staff a Network Management Center (NOC) for their national networks, and these functions are duplicated by the JCN network management center. Each of these DOJ-managed NOCs must be coordinated with the network supplier's (Sprint) NOC. This has proved to be continual source of frustration and confusion in managing network outages and configuration changes. The DOJ does not need to operate a NOC at either the component or department level. Managed network services are widely available from multiple suppliers. The DOJ should rely on its suppliers and Service Level Agreements (SLAs) to assure a well-run network.
- Unpredictable billing makes budgeting for data communications difficult for the DOJ and its components. The present system needs to be replaced by a funding mechanism that makes budget planning predictable at all levels of the DOJ.

The DOJ should fully outsource the implementation and operation of a Department network. Transport services are a commodity. The DOJ's costs associated with designing, operating and managing network elements duplicate costs already incurred by the supplier. The DOJ and its components should not duplicate network services (such as NOCs, managed network elements, etc.) already available from multiple suppliers. The outsourced network should include edge or premises devices that are located at DOJ facilities. In addition, the DOJ should procure, but outsource the operation of, the Type I encryption devices it uses to implement classified networks as VPNs running over the outsourced SBU network. The Local Area Networks (LANs) within a building should be the point of demarcation between DOJ component run facilities and the outsourced Department data network. (Note: the DOJ should consider outsourcing the

operation of in-building LANs as well.) Figure 4 illustrates the minimum set of concepts that should be outsourced.

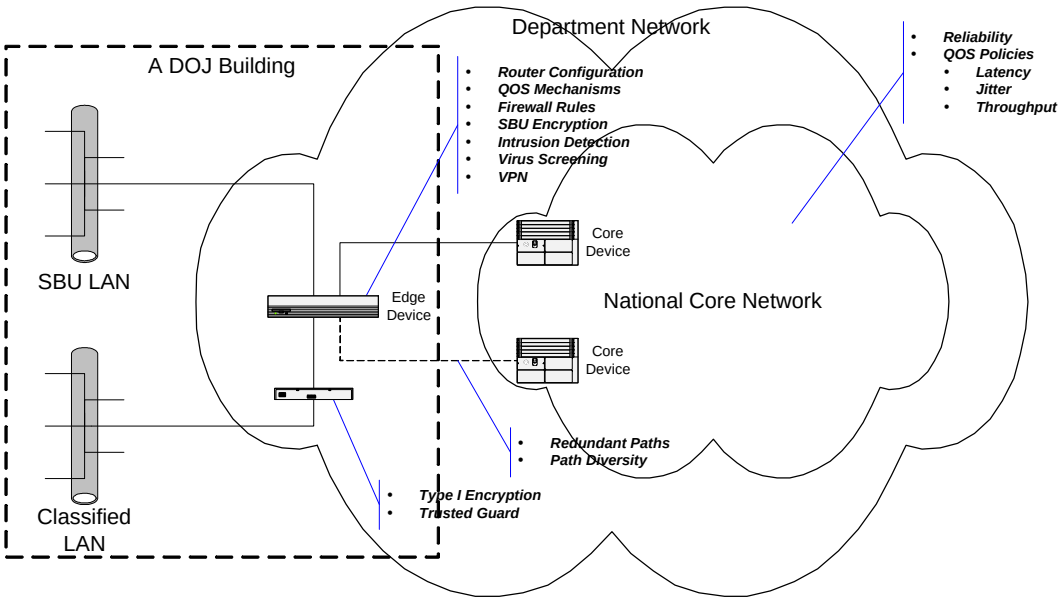



**Figure 4**

**Concepts to Outsource**

The national core network shown in Figure 4 should be designed to be highly reliable, meeting the overall needs of a Department-level continuity of operations plan. Access to this core network from individual buildings can be adapted to meet the specific needs of the DOJ components that are tenants of a building. A component with a continuity of operations plan that can tolerate or shift operations to another location in the event of a failure of an access path may chose to have a single physical connection to the national core network. A component with a continuity of operations plan that requires network access as long as a building is functioning may chose to deploy redundant, diverse paths connecting it to the core network, as suggested by the second dashed line between the edge and core devices shown in Figure 4.

DOJ component-level responsibility should be shifted to the Department-level (in consultation with DOJ-components) for several key deliverables. These deliverables include:

- Requirements for *one* Department network
- Development and execution of a transition plan for DOJ component networks to a Department network
- Development and execution of an acquisition plan for a Department data network

The Department, in consultation with its components, should assemble and hold accountable a single organization responsible for contract management related to the operation of a Department network with special emphasis on the skills needed to:

- Write and evaluate Request for Proposals (RFPs)
- Write, monitor, and enforce SLAs

- Perform configuration management
- Perform traffic monitoring, analysis and forecasting
- Perform reliability monitoring, analysis and forecasting

In order to implement the data network portion of the Information Technology Strategy, the DOJ should revisit and revise the model it uses to fund data networks. The DOJ must first develop a plan for funding the transition of multiple data networks to a Department data network.

The DOJ should also develop a plan for sustained funding of a Department network. This plan must be consistent with the goals of clear accountability for end-to-end communications, and assure that the network provides the characteristics of a Department utility that enables information sharing. This means agreeing on a Department network that meets or exceeds *every* DOJ component's requirements for security, performance, and continuity of operations, and developing a plan for satisfying those requirements.

The DOJ should create a Program Management Office (PMO) for the Department network. The PMO would be the single point of accountability for the network. The PMO should be staffed at the DOJ-level. It should be based on an "all star" team of technologists and contract administrators drawn from multiple DOJ components and contractors. The PMO should employ industry "best practices" for enterprise network development.

A Department network should be developed by first creating a national, SBU network to support the EOUSA and one other DOJ component. The EOUSA has some of the most sophisticated requirements for data networks (data, video and voice services), and has the most aggressive schedule for revising its network to meet its evolving requirements. The EOUSA's requirements cannot be met cost-effectively by the JCN.

The SBU network should support at least two DOJ components from the start. This would assure that the DOJ develops the processes, management teams, and suppliers that can meet requirements from more than one DOJ component. Candidate partners for the EOUSA include the USMS and the INS. The USMS must reach most of the same geographic locations as the EOUSA. The USMS needs to significantly improve its network infrastructure to enable changes in the Prisoner Tracking System and the deployment of the Joint Automated Booking System. Both the EOUSA and the USMS would be able to focus on the principles, processes, and requirements for building and operating a Department network because of the immediacy of their networking needs.

The INS has the most extensive and difficult to implement network of the DOJ components (because of its geographic diversity). The INS would assure that initial requirements for the SBU network dealt with a large diameter network. Redirecting the INS network to a shared SBU network may be the basis for an attractive funding plan for the transition to a Department data network. The involvement of the INS would be complicated by the need to simultaneously address many other critical information technology issues in the INS.

**Appendix D**
**Telecommunications Strategy White Paper**

The DOJ should immediately reduce spending on the JCN. It can do so by reducing the JCN NOC and DOJ components' NOCs that duplicate services already provided by Sprint. The DOJ should invest its efforts to monitor and enforce Sprint's compliance with its Service Level Agreement during the transition period to a Department network. As the EOUSA leaves the JCN, the DOJ should reduce the JCN circuits provided by Sprint to be better match to the reduced needs of the DOJ components temporarily served by JCN.

After the initial Department network is established to support the EOUSA's and one other DOJ component's operations, the DOJ should expand the implementation of the SBU network to include all other, non-classified DOJ networks. This will require developing and funding a transition plan that moves each remaining DOJ components' operations to the new network, and completely phases out the JCN and the MAN.

Once a DOJ-wide SBU network is constructed and operational, DOJ should then expand it to carry mission-specific, classified network traffic. The approach should use the SBU network as a national backbone for classified VPNs implemented by Type I encryption as traffic leaves and enters classified DOJ office spaces. Since the entirety of the FBI's network (Trilogy) is classified, the FBI would be the last DOJ component to move its primary network to a Department network. This has the advantage of assuring that the major upgrade undertaken by Trilogy has been completed and stabilized before a transition takes place.

As a last step, the Department network should be expanded to provide the underlying transport for the CJIS network. As with classified network traffic, an implementation of the CJIS network should be a VPN. CJIS delivers connectivity for non-DOJ law enforcement agencies and should be logically separated from the SBU network that serves the DOJ's internal needs. Unlike the SBU or classified networks, the CJIS network has a governing board that comprises representatives of state, local and tribal law enforcement organizations. This board would need to have its requirements met as CJIS is transitioned to a Department network.

DOJ should anticipate and quickly respond to the need for wireless and remote access to the DOJ's network. DOJ should invest in short-term security mechanisms, and adequate network and encryption capacity to assure that wireless and other forms of remote access to DOJ's IP networks can be encrypted at a level suitable for SBU traffic, and without performance impact.

Appendix E

# Public Key Infrastructure at the Department of Justice

White Paper

**Appendix E**
**Public Key Infrastructure White Paper***

# Introduction

As part of its strategic plan, the Department of Justice (Department) is seeking opportunities to improve many facets of its operations. The Department is faced with many different obligations in meeting its responsibilities. Since the terrorist attacks of September 11, 2001, the Department has been asked to take a larger role in the war against terrorism. At the same time, the Federal Government has urged its departments and agencies to conduct their business functions electronically to the extent possible while insuring information security. The Government Paperwork Elimination Act (GPEA), in particular, encourages the use of electronic documentation and electronic signatures. In accepting these additional responsibilities and improving its business processes, the Department has identified significant shortcomings in its abilities to meet these demands.

Traditionally, each component within the Department has been responsible for managing its own information technology (IT) infrastructure. This has led to disparate systems that cannot communicate with each other. Therefore, the Department has identified the need for a unified IT architecture with the ability to do the following:

- Securely access applications owned by other Department components
- Conduct much of the Department's routine business electronically, within the Department, with other Federal agencies, and with the public (e-government)
- Provide State and local law enforcement personnel access to Department applications in the execution of their roles and responsibilities

The Department has identified a minimum set of required security services that must be provided by the unified architecture to meet the growing reliance on information services. The following minimum security services must be available across the Department's IT infrastructure:

- Confidential (i.e., encrypted) information exchange
- Information integrity
- Strong authentication
- Digital signature and non-repudiation
- Advanced key management including key escrow, long-term key archive, and efficient key revocation
- "Litigation-strength" security
- Operation across different environments, allowing the secure interchange of information at multiple information sensitivity levels with external trading partners, other Federal agencies, Department components, and the public.

Cryptographic functions such as encryption and secure hashes can help protect the information. However, many of the challenges of meeting the Department's goals are associated with verifying the identity and authorization of individuals attempting to access the Department's information. Application administrators need a mechanism to verify an individual's authorizations before granting them access to system resources. Individuals must authenticate

* This White Paper is based on unpublished material prepared by SRA for the Department of Justice.

themselves to each application. If each application uses a separate password for authentication, then the individual must remember each password. When faced with the necessity of remembering many different passwords, individuals will typically use easy to remember passwords, use the same password for all systems, or write down the passwords. All of these pose significant security threats to the Department's information.

Public key technology can assist the Department in providing a secure, unified, information technology infrastructure that will meet these goals. Public key encryption may be used to implement digital signatures, secure hashes, and encryption services. This technology is based on using two discreet keys, a public key and a private key, to perform the cryptographic functions. The private keys are safeguarded by the individual who will sign or decrypt the messages. The public key is made available to other users to verify the signature, or encrypt messages for that particular individual.

## Requirements for a Department-wide Public Key Infrastructure

A Public Key Infrastructure (PKI) provides the supporting mechanisms necessary to use public key cryptography. The primary components of a PKI are the certificate authority (CA) and registration authority (RA). The CA issues certificates to individuals that link their private and public keys together. It provides the trust mechanism so that individuals and applications can have assurance that a particular public key is associated with a particular individual. Certificates also can define specific authorizations or capabilities that a user may possess. Individuals are enrolled in the system by a RA.

Since there is a significant overhead cost associated with establishing and securing the key elements of a PKI, this technology has been adopted slowly by the Government and industry. However, it offers the greatest promise of meeting the Department's long-term IT security goals of providing a unified, secure IT infrastructure throughout the Department. As e-government progresses and more Government agencies and departments implement their own PKI solutions, the Department will need to interact electronically with citizens, businesses, and other Government entities. For example, the Federal judiciary has begun implementing an electronic case file (ECF) system that eliminates paper documents at the court. Although the ECF system is not currently using a PKI, it is envisioned that a PKI solution will be necessary as the ECF is migrated from the civil sector to the criminal sector. As the courts move to a paperless environment, the Department's attorneys will also need to move in that direction.

A Department-wide PKI will enable the following:

- Confidential (i.e., encrypted) information exchange between authorized individuals
- The implementation of strong (two-factor or more) authentication mechanisms
- Digital signature and non-repudiation capabilities
- Trusted authentication across organizational barriers within the Department, with other Federal departments, with State and local law enforcement organizations, and with the public. A single authentication method for users across multiple applications, reducing

the number of password-related help desk calls resulting in direct cost savings to the Department

By providing a mechanism for strong authentication and the verification of digital signatures, a PKI can enable the Department to migrate many of its manual processes to electronic mechanisms. A PKI can provide the needed trust to enable e-government and e-commerce to materialize, with their potential cost savings and improved workflows. The interface with other law enforcement departments and agencies will provide the ability to better coordinate resources and conduct investigations.

The following section highlights some potential benefits of developing a Department-wide PKI. Annex 1 lists some of the currently identified PKI initiatives within the Department. Annex 2 identifies some potential applications that can be developed using the Department-wide PKI. While any of the applications listed in Annex 2 may be implemented without a PKI, they would each need to establish and manage separate authentication schemes. Individuals who use more than one application would need to employ a different authentication mechanism for each application. The Department-wide PKI would provide a common authentication scheme that all applications could use, allowing individuals to use a common authentication mechanism for access to all applications for which they need access.

## Department-wide PKI Benefits

The Department has already begun several PKI initiatives. All PKI efforts within the Department have been initiated to meet a specific operational requirement. They reduce paperwork associated with fulfilling legal mandates, automate workflow process, or provide improved authentication. The majority of these initiatives have focused on requirements within an individual component with only limited cross-organizational PKI efforts. A list of currently identified PKI initiatives within the Department is provided in Annex 1.

A Department-wide PKI will provide the following direct benefits to the Department:

- The ability to establish timely and secure electronic communications
- Cost savings associated with automated work processes and reduced help desk calls
- Additional cost savings with a centrally-managed PKI solution over multiple component-level solutions

The Department has a growing reliance on electronic information. There is also increasing pressure for better coordination within the Government in the war on terrorism and crime in general. These factors will require all of the components within the Department to exchange information with other components and agencies securely.

A Department PKI would provide many benefits to the Department. One of the administrative activities the Department-wide PKI could support is the automated processing of travel vouchers, forms, and leave requests. Electronic processing would reduce errors and increase the efficiency in processing these routine reports. An early Department PKI cost/benefit analysis estimated an

annual savings of nearly $29.5M by automating the work flow process. Potential future applications that could benefit from the Department-wide PKI are listed in Annex 2.

Additional cost savings may be possible with fewer help desk requests to reset forgotten passwords. If users are able to use a single authentication mechanism for all accesses, then users will be less likely to forget or write down their passwords.

The Department may develop a centrally managed PKI solution, or allow each component to develop its own solution and provide a bridging capability between the components, the Federal PKI Bridge, and other entities. The development and maintenance of several CAs and building a bridge between them may be more costly than building a single, larger CA. Additional savings would be made in only developing a single certificate policy (CP) and certificate practice statement (CPS), instead of duplicating this development at each of the components. Developmental costs would be focused on one system rather than several. Administration costs would also be lower to support a single CA, rather than several.

The bridge approach would provide more autonomy to each of the components and would not provide a unified infrastructure. Each component would need to go through the expense of implementing and maintaining separate CAs. Access control modifications to component applications also would need to accept certificates from other component CAs. All of the Department's shared services would need to accept certificates issued by any of the components' CAs. This would be a difficult undertaking.

The need for interoperability along with the potential cost savings[1] indicates the need for a centrally-managed Department CA. The limited number of skilled personnel available for Federal and contractor support also indicates that the Department's efforts be consolidated.

A central Department CA would provide a unified infrastructure that would be consistent across all components. This would allow application access modifications to be accomplished in a standardized manner. It would also allow the Department to consolidate the costs of implementing and maintaining the PKI. Each component would still retain control over their information and could also take on the RA activities and responsibilities.

Some components may have unique security requirements that dictate that they have their own PKI and provide their own certificates. However, these components will need to securely communicate with other components and others outside of their PKI. The Department-wide PKI would support the administrative and functional activities of the agency by providing a framework to allow the components to securely communicate across organizational boundaries. Without a central Department-wide PKI, each component will need to cross-certify CAs with each organization it needs to communicate. The Department must consider any perceived security benefits along with the increased cost of implementing multiple CAs and a bridge CA.

[1] A formal cost analysis was not completed as part of developing this white paper.

**Appendix E**
**Public Key Infrastructure White Paper**

# The Department PKI Program Management Office

To implement a Department-wide PKI, a program management office (PMO) will need to be established. The PMO will lead the effort to establish a common PKI throughout the Department. It will also serve as the interface with other Government PKI initiatives.

The PMO responsibilities can be divided into several functions: Architecture, Audit, Infrastructure and Shared Services, Operations, and Policies and Standards.

# Architecture

The PMO will be responsible for developing the overall PKI architecture. The architecture will define how each of the components will be integrated into the PKI and how external agencies, law enforcement, and the public will be incorporated. Also, since the PKI will be a critical service for the Department, contingency plans must also be considered when designing the architecture.

The Department-wide PKI would also provide a conduit to State and local law enforcement agencies. Figure 1 shows the conceptual architecture. The conduit would provide a path of trust so that certificates from the Federal, State, and local law enforcement agencies could be accepted by each other. This capability would be useful as multiple agencies try to coordinate investigative activities that cross jurisdictional boundaries. Through the use of the Federal Bridge CA, individuals would be capable of securely communicating with individuals from other branches of Government. This is especially important as the Government focuses its resources on specific functions. The country's fight against terrorism, for example, requires that individuals from many different Federal, State, and local departments and agencies collaborate securely.

Some key questions that will need to be considered are:

- Who will be responsible for registering individuals?
- What backup and recovery plans will be implemented?
- How many redundant certificate servers will be used?
- How will the components access the certificate servers?
- How will law enforcement access the certificate servers?
- Will hardware tokens or biometrics be required?
- Who will be required to use them?
- Can different tokens or biometrics be used in different portions of the PKI?
- What electronic services will be made available to the public?
- Will the public services make use of the Department-wide PKI? If so, How?

**Appendix E**
**Public Key Infrastructure White Paper**

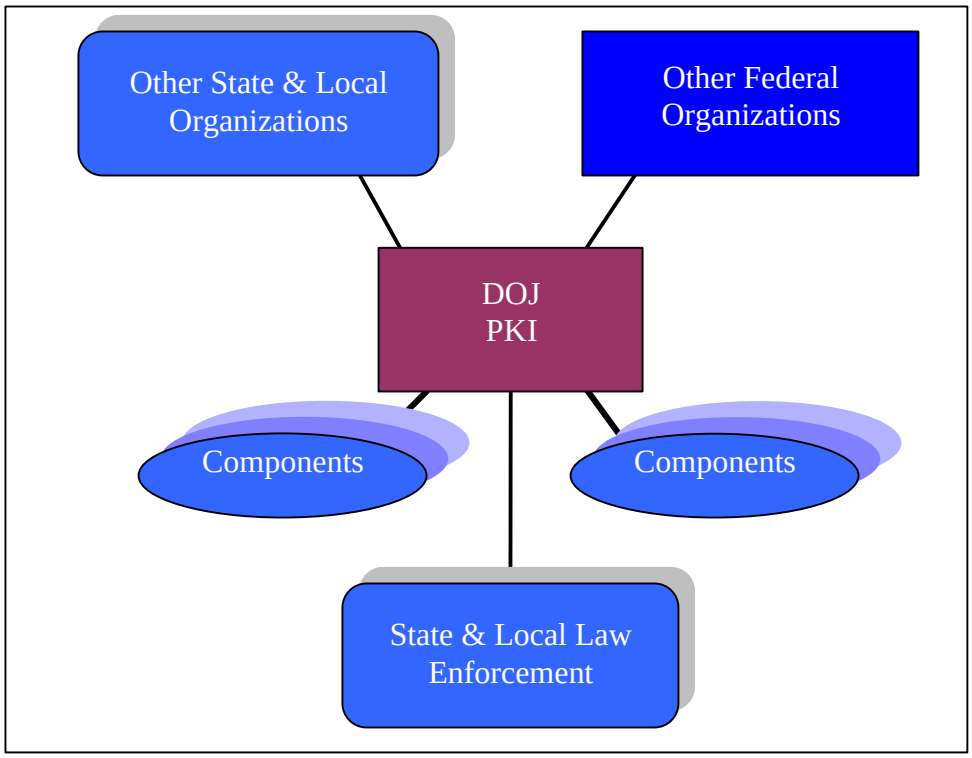



**Figure 1. Department-wide PKI Concept**

# Audit

Since the PKI provides critical security services to the Department, it is important that it be maintained securely. The audit function will verify that necessary security precautions are implemented to protect the CA, RA, and other critical PKI functions. Audit activities would include the following activities:

- Reviewing audit logs
- Performing a formal annual audit of the CAs and RAs
- Evaluating the effectiveness of security controls
- Conducting the initial and subsequent certifications and accreditations of the PKI systems

# Infrastructure and Shared Services

The Department's infrastructure must also be updated to accommodate the PKI services. Server, network, and backup capabilities must be able to handle the demands that will be placed on them. Also, the Department's shared services will need to be integrated into the PKI. The PMO will need to ensure that the total infrastructure is PKI-ready and that the shared services are PKI-enabled. Activities would include the following:

- Enabling PKI in shared applications
- Identifying necessary enhancements to the Department infrastructure

- Establishing a Department directory service
- Defining the physical security requirements for PKI elements

The Department currently provides some shared services to multiple components. Some of these are listed in Table 1. By sharing these services, the Department is able to reduce the total cost of establishing and maintaining these services. The PMO would be responsible for providing the necessary PKI services for these shared services to continue to reduce the total cost of establishing and maintaining these services. This would provide a mechanism for implementing strong authentication mechanisms throughout the agency.

| |
|---|
| JCON – Justice Consolidated Office Network – desktop and e-mail (Exchange) services |
| JOIN – Justice Online Internet Network – Internet, intranet, and browser services |
| JUST – Justice Message Service – store and forward message service. Primary application is to provide Federal law enforcement personnel access to the FBI's National Crime Information Center. |
| Justice Automated Messaging Systems – provides a secure messaging system service. Smaller components would rely on the Department's PKI for support. |

**Table 1. Department Shared Services**

The greatest benefit of establishing a Department-wide PKI will be the ability to communicate securely across organizational boundaries without requiring a complex verification and validation process. The Department-wide PKI will facilitate the secure communication between individuals in separate components, throughout the law enforcement community, and with other Government departments and agencies.

# Operations

The PMO will be responsible for establishing the operational procedures for the CA, RA, and other components of the PKI. Maintaining the confidentiality, integrity, availability, and accountability of the certificates is a critical function of the PKI operations. Some activities include:

- Issuing and maintaining public and private keys
- Issuing and maintaining certificates
- Registering individuals
- Issuing tokens
- Revoking certificates
- Verifying certificates
- Maintaining PKI servers
- Escrowing encryption keys

# Policies and Standards

The PMO will also establish the policies and standards for interoperation with the PKI. The policies and standards will define the various levels of access that may be granted and the requirements for individuals and organizations to be enrolled at given levels. These policies and standards will need to address Department personnel, law enforcement personnel, and any other individuals who may need to gain access to Department resources. The Department also needs to consider the legal ramifications of implementing a PKI and using PKI-protected information in a court of law. Some of the policies that will need to be developed include the following:

- Trust levels
- Legal constraints
- Key retention
- Physical security
- Registration requirements
- Cross-certification policies
- Hardware token policies

The Department is participating in the Federal PKI Steering Committee which provides Government-wide guidance and coordination of Federal activities to implement a Federal PKI. One of the major tasks of this committee is the establishment and management of a Federal Bridge Certification Authority. This Bridge CA will support secure communications and commerce between Federal agencies, other branches of the Federal Government, State, and local governments. It allows other Federal CAs to accept certificates from other organizations by providing trust levels for the participating CAs based on their policies.

In order to allow the Department PKI to serve as a conduit to the Federal Bridge and other CAs, the Department would take the following actions:

- Continue its involvement with the Federal Bridge program
- Define an architecture for sharing certificates
- Provide standard Department-wide directory services
- Develop a Department CA policy and procedures
- Implement a Department CA
- Connect to the Federal Bridge

# Next Steps

To be successful, the Department needs to modify its business practices and establish the importance of implementing a Department-wide PKI. A Department PKI PMO would be responsible for establishing the Department-wide PKI and leading all Department PKI activities. This office also would be responsible for developing and implementing the security functions of the Department-wide PKI, such as establishing the Department-wide policies and procedures and

developing the conduit to other organizations' CAs. Some of the PMO activities would include the following:

- Developing funding and cost estimates
- Updating the Department Security policy to reflect PKI and Digital signatures
- Developing a Trust Model
- Providing Department-wide directory services
- Developing a unified information infrastructure
- Developing a Concept of Operations (CONOP) for the PKI
- Developing Certificate Policy (CP)
- Developing Certificate Practice Statement (CPS)
    - Defining the RA process, including the need for tokens or biometrics
    - Developing key management procedures
    - Defining individual responsibilities
    - Developing backup and contingency plans
- Defining deployment goals
- Developing deployment roadmap
- Making infrastructure modifications – upgrade systems, install new equipment for the PKI, smartcards, readers, physical environment, etc.
- Developing PKI pilots
- Implementing PKI-enabled services
    - Implementing the pilot
    - Training users
    - Rolling-out the PKI-enabled system

# PKI Pilots

An essential part of implementing a successful PKI is implementing a pilot program and then migrating the technology throughout the Department. The Department-wide PKI pilot programs need to focus on applications between different components and across the Government. The programs would focus on those technologies that will provide the greatest benefit to Department users. Four of these are: secure e-mail, virtual private networks, user authentication, and web-based applications.

**Secure e-mail.** PKI-enabled e-mail would allow the greatest flexibility in providing secure electronic communications. An initial pilot would focus on intra-Department secured e-mail between different components. This capability would then be applied throughout the Department on a phased basis. After successfully piloting an intra-Department solution, the Department might then focus on interagency pilots to promote secure communications with other Government and law-enforcement organizations.

**PKI-enabled Virtual Private Network (VPN).** PKI-enabled VPN access to Department resources would allow the Department to consolidate and control its telecommunications expenses. Remote users currently dial into the systems that they need to access. A VPN would

allow the Department to consolidate telecommunications resources and provide greater security for remote users. This scenario could potentially provide a cost savings as well. A pilot would begin with a single component and then be migrated throughout the Department.

**Strong User Authentication.** The Department-wide PKI would be used as part of a strong authentication scheme. Users would be required to use at least two factors to authenticate themselves to the system. The Department-wide PKI would focus on the shared services and enable them to use the hardware token or biometric information as one factor in the authentication process.

**Web-based Application Security (Single Sign-on).** One of the Department's security goals is to provide a single sign-on capability for Department applications. Currently, the easiest manner to accomplish this is through a web interface. Web applications can be PKI-enabled to recognize the Department-wide PKI. Users would then only need to authenticate to the PKI which would validate the user for each web application. The PMO would need to identify web-based applications that would benefit from being PKI-enabled. Legacy applications would need to have a web front-end in order to include them in the single sign-on environment.

In addition to establishing the Department PKI, the Department PMO would lead the law enforcement PKI community of interest (COI) panel. This panel would work with the Federal PKI Steering Committee to establish mechanisms for the interoperability of PKIs used in law enforcement. Some of the activities of this panel include the following:

- Establishing a Community of Interest Panel
  - Reviewing business requirements, legal framework, and cooperative policies
- Defining identity framework within Community of Interest (COI)
  - Defining how to identify levels of confidentiality, availability, integrity, and authorization, such as a layered approach to meet business, legal, and policy requirements
  - Considering larger interoperable security framework into other sectors
- Developing CA and RA requirements

## Summary

The Department is being asked to conduct more of its business electronically, both internally and externally with other Government agencies and the public. Due to the current war on terrorism, individual components need to work more closely with each other and with other law enforcement organizations. A Department-wide public key infrastructure could aid the Department in providing timely and secure electronic access to information and in implementing e-government.

## References

*Paperwork Reduction Act of 1995* (44 USC 3501-3520).

**Appendix E**
**Public Key Infrastructure White Paper**

*Government Paperwork Elimination Act* (Title XVII of P.L. 105-277). 1998.

*Memorandum for the Heads of Executive Departments and Agencies. Subject: Electronic Government*. Dec 17, 1999

*Department of Justice Information Technology Architecture Public Key Infrastructure Cost Benefit Analysis*. October 1999.

*The Evolving Federal Public Key Infrastructure*, Federal Public Key Infrastructure Steering Committee. June 2000.

*Federal Agency Use of Public Key Technology for Digital Signatures and Authentication* (NIST Special Pub 800-25, October 2000).

*An On-going Assessment of Government Information Assurance, e-Business Policy, and Implementation in a Changing 'Trust' Environment – A Potentially Disruptive Technological Approach.* Federated Electronic Government Coalition, May 3, 2002.

**Appendix E**
**Public Key Infrastructure White Paper**

# Annex 1: Current Department PKI Initiatives

The Justice Management Division (JMD) has initiated two PKI efforts. The first prototype is the Secure Encrypted Title III (SET3) PKI initiative involving the Federal Bureau of Investigation (FBI) and the Drug Enforcement Administration (DEA). The purpose of this program is to increase the effectiveness and efficiency of personnel supporting Special Agent operations by enhancing the confidentiality, authenticity, integrity, availability, and reliability of the Title III Pre-Authorization Approval Sub Process (PAASP). Participants who request, and respond to requests, regarding Title III Electronic Surveillance records are able to sign and encrypt e-mail documents.

The second initiative was a civil PKI prototype that is no longer in use. The prototype involved encryption and digital signature support for the civil law environment. The preliminary participants were the Department's Tax Division and the Internal Revenue Service (IRS). Both e-mail messages and desktop files were encrypted and signed.

In addition to the JMD-initiated efforts, individual Department agencies have developed PKI initiatives to meet specific requirements. Some of these initiatives are presented in this section.

The FBI has identified two PKI initiatives. The first is to develop an FBI-wide internal PKI system that would be used for creating and managing Virtual Case Files (VCF). They have also implemented a PKI-enabled application to allow Federal Firearms Licensees (FFL) to request a search of prospective firearms purchasers through an FBI web site.

The DEA's Office of Diversion Control is using two separate pilots as a proof of concept for meeting the regulatory requirements associated with controlled substance prescription and distribution. The first pilot is being conducted with the Department of Veterans Affairs and focuses on the benefits that a PKI-enabled system might provide in prescribing and dispensing controlled drugs from a pharmacy. The second pilot involves manufacturers and distributors and is attempting to reduce the paperwork burden associated with manufacturing, transporting, and distributing controlled substances.

The DEA also uses a PKI to allow secure remote dial-in access to Firebird, the DEA's office automation network.

The Immigration and Naturalization Service (INS) has implemented a PKI to provide limited e-mail security and file encryption. It also issues certificates to INS web servers to enable them for Secure Sockets Layer (SSL) connections. INS also uses a PKI to support laptop encryption.

# Annex 2: Potential Applications Using the Department-wide PKI

By providing a mechanism for strong authentication and the verification of digital signatures, a PKI will enable the Department to migrate many of its manual processes to electronic mechanisms. A PKI can provide the needed trust to enable e-government and e-commerce to materialize, with their potential cost savings and improved workflows. The interface into other law enforcement departments and agencies will provide the ability to better coordinate resources and conduct investigations. This section highlights some potential applications that might be developed using the Department-wide PKI.

While any of these applications may be implemented without a PKI, they would each need to establish and manage separate authentication schemes. Individuals who use more than one application would need to employ a different authentication mechanism for each application. The Department-wide PKI would provide a common authentication scheme that all applications could use, allowing individuals to use a common authentication mechanism for access to all applications for which they need access.

## Employee Access

Mobile and wireless computing devices can be PKI-enabled. This would provide the future capability of granting secured access to e-mail and other electronic information through devices such as a Personal Digital Assistant (PDA). Information on the laptop or other mobile computing device may be encrypted or otherwise protected with the PKI to prevent unauthorized access if the device should be lost or stolen. Traveling employees must also be able to securely communicate while conducting investigations, preparing court papers, or performing other tasks away from the office. The Department-wide PKI would permit the Department to provide VPN access to Department resources from virtually any location. This could potentially provide a cost savings as telecommunication links are consolidated.

With a common infrastructure, employees could be assigned to different components and offices within the Department without having to modify all of their information. As needs arise, individuals with the appropriate skills may be placed on task forces or other assignments without regard to which component they work for primarily.

## Federal Government Communications

Employees gain access to their pay and benefits information through the National Finance Center (NFC). By integrating the Department-wide PKI with the Federal PKI, employees will be able to use the same Department token to access their personnel information. The authenticity and non-repudiation factors might be extremely important as employees reallocate their Thrift Savings Plan funds and the markets fluctuate.

## Law Enforcement Community of Interest

The Department must also communicate with other Federal, State, and local authorities. By establishing PKI standards for the law enforcement community, certificates may be cross-certified and allow secure information sharing at all levels of law enforcement. The FBI has already established a program to allow Federal Firearms Licensees access to FBI data to conduct checks for potential firearms purchases. The FBI, INS, DEA, and other components could

provide services to the law enforcement community. This same technology might expedite the process of searching for outstanding warrants when individuals are arrested. This also would enable multiple agencies to securely communicate with an ad hoc command center when responding to high-profile crime scenes such as the World Trade Center.

## Contractor Communications

PKI provides the ability to conduct business electronically. Although this aspect of PKI is less mature than other uses, the Department might eventually take advantage of its PKI program to manage its contractors. Contracts and Task Orders could be issued electronically with digital signatures. Contract deliverables also could be encrypted, signed, and delivered electronically. The NFC has already implemented a PKI for conducting e-commerce.

## Public Communications

The General Services Administration's Access Certificates for Electronic Services (ACES) program facilitates secure access to Government information and services by the public. This program would allow the Department to provide secure services to individuals who have a valid ACES Certificate.

The Department also publishes public information on Internet web servers. The Department may digitally sign the contents of the web pages and then periodically validate that they have not been modified inappropriately. If an attacker were able to modify any of pages, then the verification process would detect the change and could take additional actions.

Appendix F

# Segment Architecture of the Law Enforcement Booking Process

# Appendix F
# Segment Architecture Analysis of the Law Enforcement Booking Process*

## Preface

This document provides the Department of Justice (Department) with an example of a segment architecture analysis to illustrate how Enterprise Architecture (EA) Planning can be used to provide a blueprint for defining an organization's Baseline (As Is) and Target (To Be) architectures. EA Planning assists in defining the business processes needed to support an organization's mission; defining the data required to support those business processes; and identifying how to provide that data to those in the organization who need it. Usually EA Planning, as its name implies, encompasses an entire organization. It is essential to first have this enterprise-wide view before developing a detailed analysis of a single segment. Efforts are underway within the Department to develop the overarching framework, however, for purposes of illustration only, one segment of the Department's enterprise was chosen for this study.

The focus of this example is the Department's law enforcement booking process. The booking process was chosen as an illustration because of differences in the way that the Department's law enforcement components manage booking data. The Department developed an automated system called the Joint Automated Booking System (JABS) to facilitate the sharing of arrest and Federal offender data among the law enforcement components. Currently, the Drug Enforcement Administration (DEA) is the only Department component that interfaces with JABS, although, the United States Marshals Service (USMS), the Federal Bureau of Investigation (FBI), and the Bureau of Prisons (BOP) are working toward an interface capability. In addition, the Immigration and Naturalization Service (INS) is pursuing a modification to their booking process to include JABS.

This segment architecture example compares how the DEA and the INS manage booking data in support of the Department's mission and strategic goals. These two law enforcement components were chosen because each provides an example of a different approach to the data flow. The DEA developed an electronic process and the INS currently uses a manual process to transfer data to the Federal Bureau of Investigation's (FBI) Integrated Automated Fingerprint Identification System (IAFIS).
For purposes of this document, the baseline view of the Department's booking process is based on JABS, Version 1.3, which is the current operational version. The Target Architecture describes a combination of elements from JABS, Version 2, and INS' future interface from its Automated Biometric Identification System (IDENT) to IAFIS. The IDENT interface with IAFIS (IDENT/IAFIS, Version 1.2), would automate the INS interface with JABS.

* This White Paper is based on unpublished material prepared by SAIC for the Department of Justice.

**Appendix F**
**Segment Architecture Analysis of the Law Enforcement Booking Process**

## Part I. Architectural Model

### 1.0 INTRODUCTION

#### 1.1 Purpose

This segment architecture analysis of the Department of Justice (Department) booking process defines a target architecture to optimize the relationships between the Department's booking process and the underlying information technology (IT) that supports that business process. It is a high-level blueprint that shows how the business activities and data should be supported by IT (applications and infrastructure). The Department's vision is for its Joint Automated Booking System (JABS) to become the conduit for access to Federal law enforcement booking data (see Figure 1).

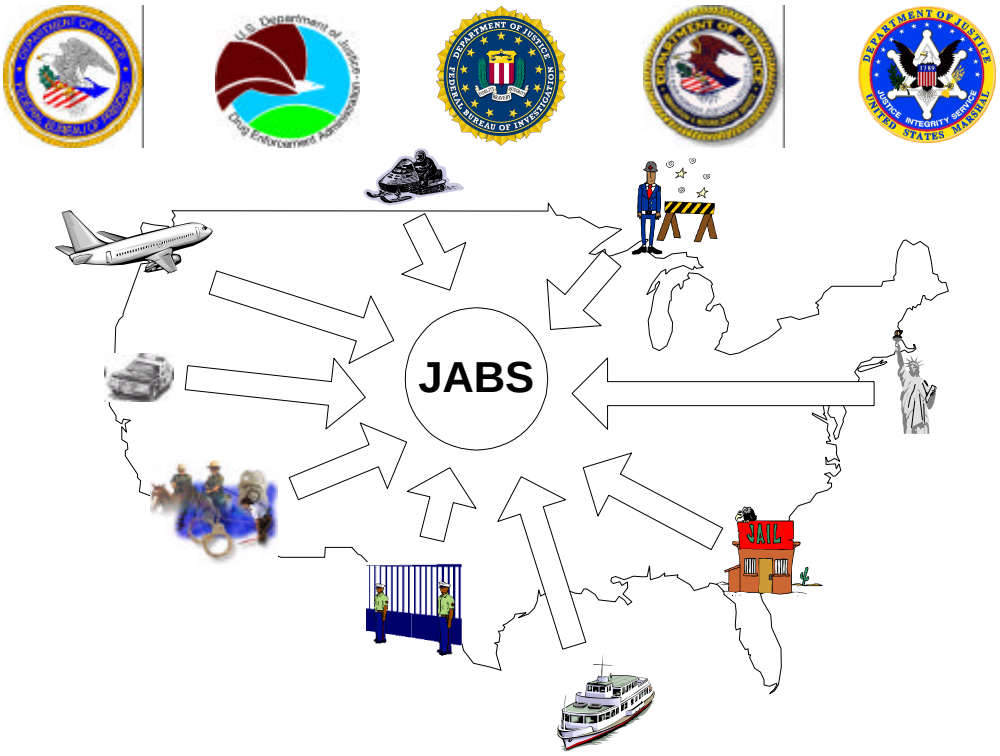



**Figure 1: JABS: A Conduit for Law Enforcement Data**

#### 1.2 Scope

The Department has developed JABS, a system for electronic information sharing to automate the booking processes of the entire organization. This segment architecture analysis examines how two of the Department's law enforcement components, the Drug Enforcement Administration (DEA) and the Immigration and Naturalization Service (INS), use their own

---

This document contains information that serves the purpose of demonstrating an example of a segment architecture and does not reflect the current JABS program in its entirety.

internal booking processes to manage data in support of the Department's mission and goals. The analysis also examines how these two components share booking information and interface with two other important systems in the Department's booking process: JABS and the Federal Bureau of Investigation's (FBI) Integrated Automated Fingerprint Identification System (IAFIS).

## 2.0 ARCHITECTURAL METHODOLOGY

This segment architecture analysis consists of three primary elements. The first is the Baseline Characterization of the Department's booking process, which describes the booking process and examines how well it supports the Department's business. The second component is the Target Architecture, which describes the four architecture views—business, data, application, and technology—that make up the booking process. The third component provides a gap analysis and a transition plan. The gap analysis identifies the gaps between the two architectures (the baseline and the target), while the transition plan outlines the migration from the baseline (As Is) to the target (To Be) architecture. This methodology is based on guidance from the Federal Enterprise Architecture Framework (FEAF) for Enterprise Architecture (EA) Planning, and includes inputs from the Department's Business and Data Architectures. Figure 2 depicts how these elements relate during the process of developing and maintaining the segment architecture for JABS.

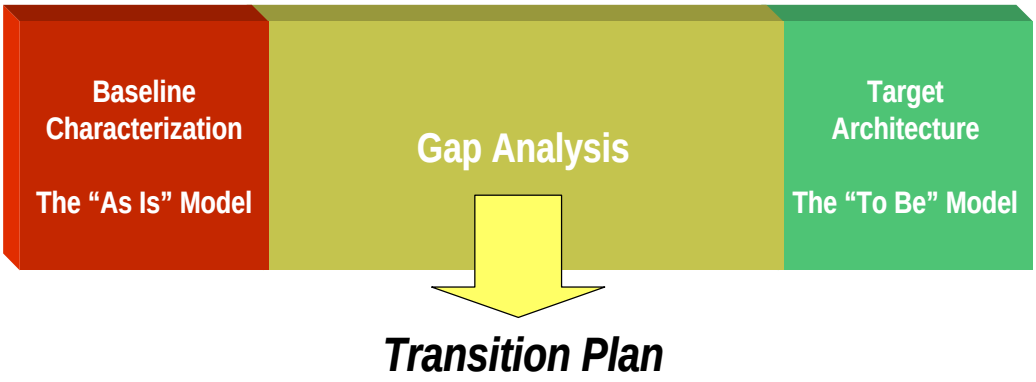



Figure 2: Components of a Segment Architecture

This approach is consistent with the guidance in the Clinger-Cohen Act. This Act directs the Chief Information Officer (CIO) to ensure that information technology (IT) is acquired and information resources are managed according to the business priorities of the organization. The first step in developing a segment architecture is to define the Enterprise Statement. The Enterprise Statement defines the scope of the Department's booking process.

| ***Enterprise Statement**: Rapid identification of suspects, sharing of common booking information among all law enforcement components, and tracking Federal offenders.* |
|---|

**Appendix F**
**Segment Architecture Analysis of the Law Enforcement Booking Process**

## 3.0 CHARACTERIZATION OF THE "AS IS" JABS BASELINE MODEL

### 3.1 The Business Architecture

The Business Architecture defines a high-level view of the Department's booking process within the context of the Enterprise Statement. In addition, it examines the activities and attributes (e.g., user classes) that make up that process and the relationships between them.

#### 3.1.1 Overview of the Department of Justice Booking Process

The Department's booking process is actually a compilation of systems and processes. The process consists of the Department-wide system for capturing booking data, JABS; the systems and processes established by each of the Department's law enforcement components; and the FBI's IAFIS, which provides ten-print fingerprint identification and criminal history services to other law enforcement components. The law enforcement components collect much of the same arrest information through their booking processes, such as ten-print fingerprints and other biometric information, to facilitate making a positive identification of a suspect. Each of the components has the capability to query IAFIS to assist in identifying suspects by obtaining a positive fingerprint match. The roles and responsibilities of the different players are illustrated in Figure 3.

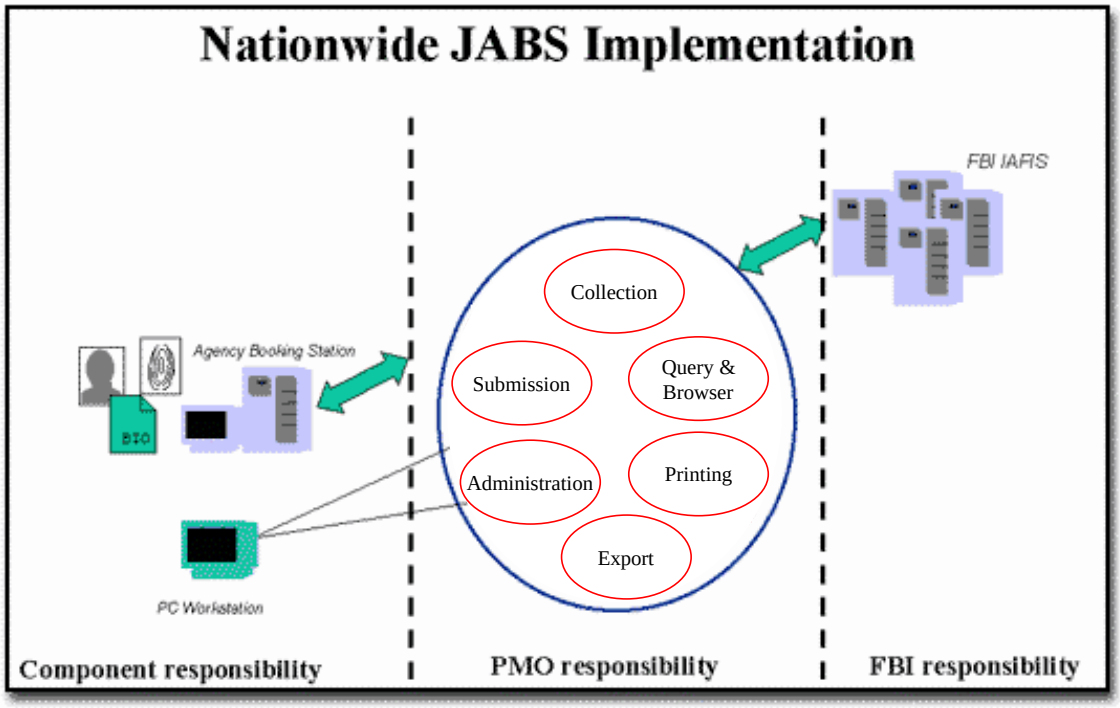



**Figure 3: Nationwide JABS Implementation**

In 1993, the Department determined that there was a need to share booking data among the Department's law enforcement components. To meet this requirement, JABS was developed to transmit fingerprint and other relevant arrest and suspect data between IAFIS and the law enforcement components. In 1999, the Department completed development of the JABS System

## Appendix F
## Segment Architecture Analysis of the Law Enforcement Booking Process

Boundary Document and established the high-level requirements for the JABS nationwide development and implementation. The objectives of the JABS program are outlined below:

| | |
|---|---|
| *Automate the Booking Process* | Facilitate the rapid identification of individuals under arrest or detention and minimize duplication of data entry by multiple law enforcement components through the automation of the booking process. |
| *Share and Exchange Booking Information* | Enable each law enforcement component to share and exchange booking information. |
| *Track Federal Offenders* | Allow immediate identification of known Federal offenders in time-critical situations and track the offender's location of incarceration and store a history of changes to location. |

As a result of a JABS pilot program conducted in South Florida in 1999, it was decided that the following functional *principles* should drive the design and implementation of the nationwide deployment of JABS.

Each component will develop its own automated booking capability.

JABS will provide the critical data exchange capability among law enforcement components.

As a central transitional data repository of booking information, JABS will allow authorized users to query the database to find needed information about an offender.

JABS will be the conduit to successfully transmit digital fingerprints to IAFIS for identification and return this information to the source component.

When fully deployed, JABS will provide the following law enforcement functionality:

**Submission to FBI's IAFIS** — Each designated law enforcement component will have the capability to electronically submit the booking packages that were created in its internal automated booking system to the FBI's IAFIS through JABS. As part of this service, JABS will validate and repackage (reformat to comply with IAFIS directives) the data prior to submission to IAFIS. The submission will be tracked in JABS and the data will be archived for future retrievals and queries.

**Access and Retrieval** — Each designated law enforcement component will have specialized access to booking records that it submits. In addition, the capability to retrieve information that another component originated for further analysis and processing.

**Query and Search Tool** — Standard query and search capabilities will be available to all authorized users. When performing investigative casework, users can search on common data fields to retrieve possible suspect matches and additional prior booking information. Data fields subject to query include file numbers, personal information, physical characteristics, vehicles, and known criminal associates.

**Reporting Capability** — A tool that generates standard reports; such as component statistics, will be available to all authorized users.

---

This document contains information that serves the purpose of demonstrating an example of a segment architecture and does not reflect the current JABS program in its entirety.

**Additional Capabilities** — Various technical and administrative services; including security, auditing, database management, e-mail, and interface tools; will be available.

As more components use JABS, many benefits are envisioned for the future. JABS could provide an offender/case-tracking number to be used by all Federal criminal justice agencies. This could ensure court dispositions and U.S. Attorney declination decisions are electronically transmitted to the criminal history records at the FBI's Criminal Justice Services Division.

### 3.1.2 Law Enforcement Components Booking Processes

The Department's booking process is intended to manage booking data via six business activities as follows:

Creating a new booking record

Updating an existing booking record

Querying existing booking records

Managing the component level booking station

Managing JABS

Providing Department-wide technical support for JABS

The DEA and the INS components are responsible for supporting the "*Enforcement Operations*"[1] business area of the Department. While their missions and goals vary, they perform similar business activities. Each component conducts the business function called "*Arrest Suspects.*"[1] This function requires a booking process to gather specific information about detained or arrested individuals. Also, each component's booking process collects biometric and biographic information that is important for suspect identification.

#### 3.1.2.1 DEA

The DEA collects booking data through an automated booking process called the Firebird Booking Service (FBS). When a suspect is arrested, ten-prints and other arrest related data elements are collected on a Form FD-249 (Arrest and Fingerprint Card) in an FBS local workstation that directly transmits the booking package electronically to a JABS server. JABS stores the booking data in a central database where it is available to be queried by the DEA. JABS repackages the booking data into a format determined by the FBI and sends it to IAFIS for a positive identification of the suspect. IAFIS returns a response to the DEA, usually within 2 hours of the original submission to JABS.

#### 3.1.2.2 INS

INS currently employs a mix of manual systems and automated systems to perform the booking process. It uses its Enforcement Case Tracking System Booking Module (ENFORCE) to process the majority of its apprehensions. ENFORCE is an automated system that is used extensively in the field by border patrol agents to submit electronic data forms. A related system was

[1] U.S. DOJ, Information Resources Management, *U.S. Department of Justice Enterprise Business Architecture*, December 17, 2001.

developed called the Automated Biometric Identification System (IDENT) as an automated, two-print identification system. These two systems, ENFORCE and IDENT, exchange information through an electronic interface. The purpose of the ENFORCE/IDENT interface is to allow the ENFORCE users to correlate the information stored via electronic forms with the biometric data stored in IDENT. The INS imports a subset of the FBI's "wants and warrants" fingerprint files into IDENT and uses this information to identify known criminals, usually within 2 minutes. The initial booking process is automated, but the submission of the ten-prints to the FBI is manual.

As soon as the INS agents determine that it is necessary to hold a suspect for more than 6 hours, they *book* the suspect. A set of ten-prints and other biographic data elements are collected and placed on a Form FD-249 fingerprint card. The booking information is added to a case file and mailed to the FBI, or in a few instances, transmitted via secure facsimile, for the eventual inclusion in the FBI's IAFIS. This data is not presently transmitted through JABS. The FBI examines the fingerprints and compares them with prints stored in IAFIS. Normally, the INS receives a response from the FBI within 6 to 8 weeks. The INS does not store the ten-prints in an INS database, however, it does store two index fingerprints in its Automated Biometric Identification System (IDENT) database.

### 3.1.3 User Classes and Business Activities

Of the 128,000 employees in the Department, approximately 36 percent are classified as specializing in enforcement and investigations. Another 11 percent are detention officers. These Department employees, who represent nearly half of the total, comprise the core users of the Department's various booking processes. In addition to the core users, attorneys supporting the litigation and hearings represent another category of users who require booking data for prosecution, management, and analytical purposes. This represents an additional 10 percent of the Department's workforce. In total, over half of the Department's employees are engaged in business activities that require standardized information from the booking process.

The components have a similarly wide variety of employees who use the booking data. Approximately 4,500 of the DEA's 9,500 employees—as well as an additional 2,500 state and local employees deputized and working under DEA supervision—are responsible for conducting bookings. Within the INS, 7,000 of nearly 40,000 employees are responsible for conducting investigations and 13,000 are responsible for conducting the actual bookings. Additionally, within both components, there are many more employees, other than those who conduct the bookings, who rely upon the booking information to perform their duties.

Figure 4 lists the JABS common "user classes." A user class is a group of individuals who perform similar activities with a similar purpose. These individuals enter and use arrest information from the booking process. Figure 4 also illustrates the business requirements supported by each user class while performing the "Arrest Suspects" business function.

**Appendix F**
**Segment Architecture Analysis of the Law Enforcement Booking Process**

| User Class | Capabilities Required |
|---|---|
| Booking Agent | Create Data<br>Update Data<br>Query Data |
| Investigator/Analyst | Query Data |
| U.S. Attorney | Create Data<br>Query Data |
| Pretrial Court Office | Create Data<br>Query Data |
| Probation Court Office | Create Data<br>Query Data |
| Corrections Officer | Create Data<br>Update Data<br>Query Data |
| Statistician | Query Data |

**Figure 4: Department of Justice Booking Process User Classes**

### 3.1.4 Business Functions and Work Locations

The DEA has 350 locations where bookings are conducted. Approximately 100 are electronically linked to IAFIS through JABS. The remaining booking locations are expected to receive the JABS booking stations by the end of FY03. In addition, the DEA has 25 Mobile Enforcement Teams (MET) with the capability of conducting remote bookings in the field and linking via a wireless connection to the FBS.

The INS has approximately 900 locations where bookings are performed. In addition, the INS is currently testing the technical and operational feasibility of using a "Remote IDENT" to provide the border patrol agents with the capability of using a laptop computer in a remote location with a dialup phone line to process apprehensions and book suspects.

The DEA and the INS have many booking locations within the same geographic area. Because crimes tend to be local or regional in nature, it is not uncommon for the DEA and the INS to be investigating the same crimes or to be booking the same suspects concurrently. However, because there are no automated links between their individual booking processes, there is no efficient way for these organizations to share booking information or avoid duplicate data entry.

**Appendix F**
**Segment Architecture Analysis of the Law Enforcement Booking Process**

## 3.2 The Data Architecture

The Data View depicts the logical relationships of specific data elements required by the individual business activities that comprise the business process—in this case the booking process. This view analyzes, and attempts to describe, the relationship between the information required (i.e., the data) and the business activities essential to the booking process.

The Department's data view is concerned with the data that supports the missions and strategic goals of all of its law enforcement components' booking processes. While the DEA and the INS have a need for data specific to their respective missions, there is also a common pool of data that all booking agents require. These data elements can be grouped together in the 12 unique categories of data listed below.

- Photos of scars, marks and tattoos
- Vehicle information
- Medical and mental history
- Administrative booking data
- Information on associates
- Information on family members
- Mugshots
- Identifying numbers and documents
- Description of the arrest
- Physical description of the suspect
- Ten-print fingerprints
- Information contained in the FBI response (e.g., arrest history, incarceration data, "rap sheet")

### 3.2.1 Data Flow of the Components

#### 3.2.1.1 Data Flow for the DEA Booking Process

The DEA collects booking and arrest data through its FBS. Once a booking package has been automatically constructed in FBS, the package is sent electronically to JABS, which repackages the information and submits it electronically to IAFIS. IAFIS responds with an e-mail message to JABS, which in turn, transmits the response with the data to the DEA. Figure 5 depicts the information flow between the FBS and IAFIS.

**Appendix F**
**Segment Architecture Analysis of the Law Enforcement Booking Process**

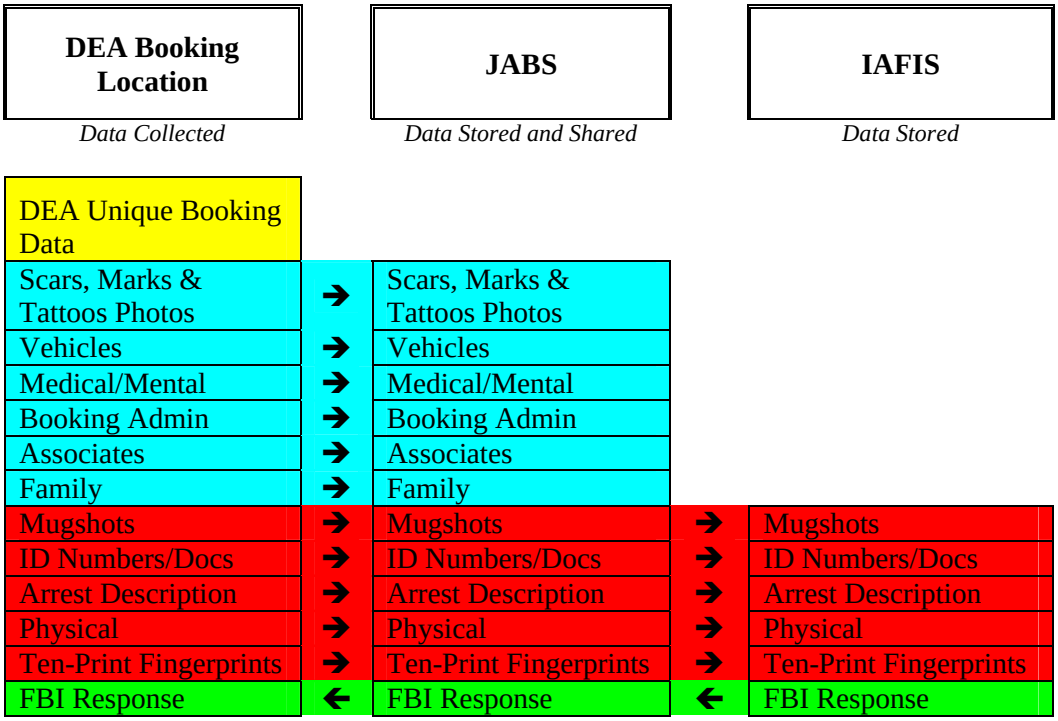



**Figure 5: Data Flow for the DEA Booking Process**

Through JABS, the DEA can electronically create a booking package or an inquiry; transmit it to IAFIS for identification; and quickly receive an IAFIS response. By interfacing electronically to JABS, the DEA receives a response from the FBI on average within 2 hours. Prior to the development of an electronic interface, the elapsed time for the DEA to receive the IAFIS response ranged between 6 weeks to 3 months.

In addition, data submitted to JABS is stored in a central data repository where it is available for query or reports by other organizations. This supports the JABS program objective for the facilitation of data sharing among its components.

### 3.2.1.2 Data Flow for the INS Booking Process

The INS uses a case tracking and booking system, ENFORCE, to capture biographical information related to INS enforcement activities and capture retrievable biometrics through the INS's IDENT. IDENT is a quick screening database that contains index fingerprint records (two-print) both for criminals and non-criminals. ENFORCE accepts electronic forms completed at the various Border Patrol locations. Together, these two systems create the ENFORCE/IDENT Booking Module, which provides data to the INS enforcement data repository and allows the INS Border Patrol to correlate the data supplied by the ENFORCE electronic forms to the biometric information captured by IDENT. For the INS, bookings are conducted on cases that are considered or accepted by the U.S. Attorneys Office for Federal

prosecution. All other case types are not booked through JABS. Currently, the INS does not have the capability of electronically submitting ten-prints to IAFIS[2]. Therefore, the submission of the booking and arrest data to IAFIS and the subsequent FBI response are manual processes. Ten-print cards are sent predominantly by mail, but occasionally by facsimile, to the FBI for identification and comparison with fingerprint data stored in IAFIS. In contrast to the DEA data flow, Figure 6 shows the information flow between INS and IAFIS.

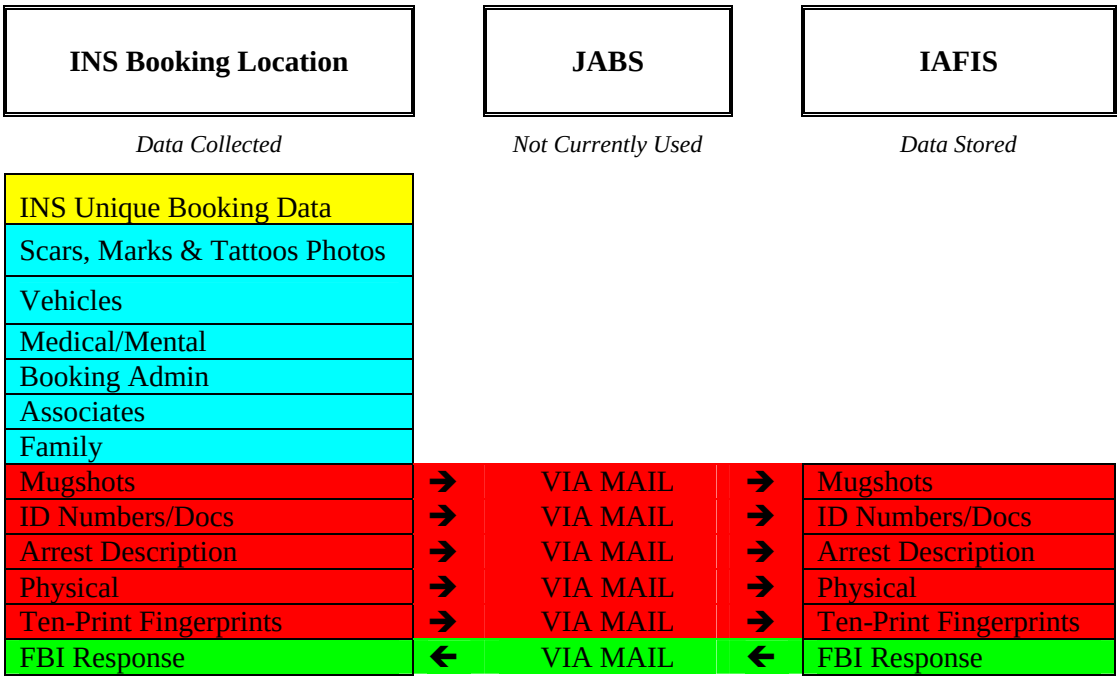



**Figure 6: Data Flow for the INS Booking Process**

Because the INS does not receive a response from the FBI for 6-8 weeks, the INS is not able to use the real-time identification information from the FBI when a subject is first detained. To alleviate problems in this area, IDENT periodically imports "wants and warrants" data from IAFIS. However, because ENFORCE/IDENT does not interface with JABS, the information contained in this database cannot be shared with other components. Conversely, the INS is not able to query the JABS database for relevant data from other organizations.

### 3.3 Applications Structure Characterization

As discussed in the business characterization (see Section 3.1.2), the Department's booking process is intended to manage data through the six phases of the booking process: create, update, query, component management, JABS management, and technical support. The Department's booking process consists of three major applications: Core JABS, which is the system for collecting and integrating data from all of the Department's component booking processes; the

[2] The exception to this is a pilot program located in a Brownfield border patrol station.

DEA's automated booking system (i.e., FBS); and the INS's ENFORCE/IDENT. Figure 7 depicts the JABS activities that are performed by the existing applications.

| | **REQUIREMENTS OF THE BOOKING PROCESS** | | | | | |
|---|---|---|---|---|---|---|
| **APPLICATIONS** | Create | Update | Query | Component Admin | JABS Admin | Technical Support |
| Core JABS | × | × | × | × | × | × |
| DEA Booking Station | × | | × | × | | |
| INS Booking Station | × | | Pilot | Pilot | | |

**Figure 7: Department of Justice Booking Process Applications and Business Activities Supported**

### 3.3.1 Core JABS Applications Structure

JABS is designed to provide for rapid identification of criminals via the FBI's IAFIS. The system provides real-time information sharing for investigations; eliminates the need for data-entry redundancies and manual, paper-intensive processes; and establishes a tracking capability for individuals held in Federal custody. Within this process, JABS sends up to three messages to the booking station submitting the package. The first message simply indicates that JABS has received the submission. The second message indicates that the package was forwarded to IAFIS. The third message provides the response returned from the FBI with an attached FBI identification record, if available. The FBI maintains information records on more than 24 million persons. For each individual for whom criminal justice information is submitted, the FBI's Criminal Justice Information Services Division compiles an identification record, or "rap sheet." A rap sheet reflects information regarding arrests, convictions and other dispositions when known, and incarcerations.

To improve maintainability, the application architecture relies mostly upon commercial off-the-shelf (COTS) products and encourages a minimal use of development software. The purpose of JABS customized software is to integrate the COTS applications.

### 3.3.2 DEA Applications Structure

As shown in Figure 7, the DEA application supports all of the booking process business activities. FBS workstations are directly interfaced to JABS, allowing booking data to be electronically transmitted to IAFIS through the JABS server. Data is stored on the JABS server so that the DEA booking data is available to other JABS-capable entities within the DEA, and can be queried, printed, and exported.

### 3.3.3 INS Applications Structure

As stated earlier, the INS primarily uses its ENFORCE system to capture booking data (e.g., Border Patrol processes over 99 percent of their apprehensions through ENFORCE). ENFORCE is an automated system that is linked to IDENT and is used extensively in the field. Together,

this is known as ENFORCE/IDENT. IDENT is used to identify an individual based on internal INS data and the FBI's "wants and warrants" fingerprint files, which are periodically imported into IDENT.

Because the INS booking process is not linked to Core JABS through an electronic interface, the INS booking data is not available to other law enforcement components and cannot be queried, printed, or exported by JABS. The INS does not store ten-print records within ENFORCE/IDENT, although it does have a means to extract the two-print index finger impressions from the ten-print file and store this information in its database.

### 3.4 Current Technology Baseline

For purposes of this document, the technology of the Department's booking system is the total of the technology of Core JABS, the DEA's FBS, and the INS's ENFORCE/IDENT.

#### 3.4.1 Core JABS Technology Baseline

Core JABS consists of two server-class machines on a network segment. The Local Area Network (LAN) is connected to the Department's Justice Consolidated Network (JCN) via a firewall. The Unix server is a Hewlett Packard (HP) 9000/800 N4000 series that serves as a host for the JABS database and Web server. The Microsoft (MS) NT server is a PL5500-RXN500 Compaq server that hosts the JABS e-mail application. Both servers have redundant critical subsystems including system disks, power supplies, Central Processing Units (CPU), and cooling fans.

JABS services reside on a protected subnet, which is connected to each of the components' networks and the Department's intranet via a Virtual Private Network (VPN). JABS is installed at the Justice Data Center (Rockville, Maryland). The architecture consists of a server and associated peripherals hosting the Oracle database management system that provides the data repository, security, and audit, and transactional services. JABS printers are managed by the JABS system administrator and must be registered with the administrator.

#### 3.4.2 DEA Technology Baseline

At the DEA, biometric and biographic data captured on the FBS client during the booking process is sent to the JABS Mail Server via a Simple Mail Transfer Protocol (SMTP) transaction. The JABS Mail Server sends the information to IAFIS, which processes the SMTP message when it arrives. Likewise, IAFIS responds to the FBS client with an SMTP message containing the suspect's identification information (i.e., "rap sheet") included as an attachment to the message. The DEA FBS architecture consists of a distributed client segment and a centralized server segment that are connected via a wide area network (WAN).

#### 3.4.3 INS Technology Baseline

The INS booking data is mailed to the FBI, or on rare occasions submitted electronically to IAFIS through a facsimile transfer to an FBI secure fax machine. At the FBI, the fingerprint data is manually compared with records stored in IAFIS. As was noted earlier, this process can take up to 2 months before INS will receive a response.

---

**Appendix F**
**Segment Architecture Analysis of the Law Enforcement Booking Process**

INS does have a database that is centrally located at the INS Headquarters (HQ) in Washington, DC, which currently contains biometric data on individuals it detains. Each ENFORCE/IDENT client connects directly into the central site login server for all transaction requests. However, the type of network access varies by area: LAN, INS WAN, or NetBlazer to INS WAN. Once the initial connection is established, all INS clients have access to the same fingerprint database. The centralized database gives INS clients access to up-to-date biometric information.

### 3.5 Summary of the "As Is" Model

The mission of the Department's booking process is to enable its law enforcement components to share booking data; facilitate the rapid identification of suspects through IAFIS; and track Federal offenders. While JABS has been developed to provide these capabilities, only DEA has a process in place to use the JABS' capabilities. As a result, the mission, as stated, is only partially fulfilled.

The DEA is able to take advantage of the ability of the system to provide rapid identification of suspects through IAFIS. Through JABS, IAFIS provides a response to the DEA within 2 hours of its original submission. Because the INS submission process is not automated, it can take up to 8 weeks to receive a response from IAFIS. This operational inefficiency may hinder on-going investigations or may allow offenders to be prematurely released due to the lack of reliable and timely data.

Since the DEA is the only component with an electronic interface to IAFIS, neither organization is able to share the booking data efficiently. Although they often work closely together; implement similar processes; investigate the same cases; use the same equipment and facilities; and appear before the same Federal magistrates; each law enforcement component often processes cases separately because of this inability to share data. This duplication of effort places a strain on data entry, booking procedures, and resources.

## 4.0 The "To Be" JABS Enterprise Architecture Target Model

### 4.1 The Target Business Model

The focus in the target business segment analysis will be on the activities associated with the booking process and its related functions. After developing the target business and data models, the information will be analyzed to determine a target application structure and the supporting "To Be" technology.

#### 4.1.1 The Department of Justice Business Model

The enterprise level business model for the Department[3] has three business areas: Enforcement Operations, Justice Services, and Corporate Services, which are further decomposed into business functions. Figure 8 demonstrates how the major functions of the Department combine

[3] U.S. DOJ, Information Resources Management, *U.S. Department of Justice Enterprise Business Architecture*, December 17, 2001.

## Appendix F
## Segment Architecture Analysis of the Law Enforcement Booking Process

to achieve the strategic goals of the Department. The depiction is based on a widely accepted model—the Michael Porter Value Chain. The small scope of the business segment being analyzed (i.e., booking) does not allow for a true value chain analysis. However, it can be surmised from Figure 8 how an efficient booking process can contribute immensely to the overall objectives of the rapid identification of suspects; the sharing of common information among all law enforcement components; and the tracking of Federal offenders.

The upper section of the model displays the Department's support functions. These functional areas work together to achieve the Department's overall strategic goals. The lower section represents the "line" or direct business functions of the Department. The *Arrest Suspects* business function, which is highlighted under the Enforcement Operations business area, is the primary function that is supported by the booking process.

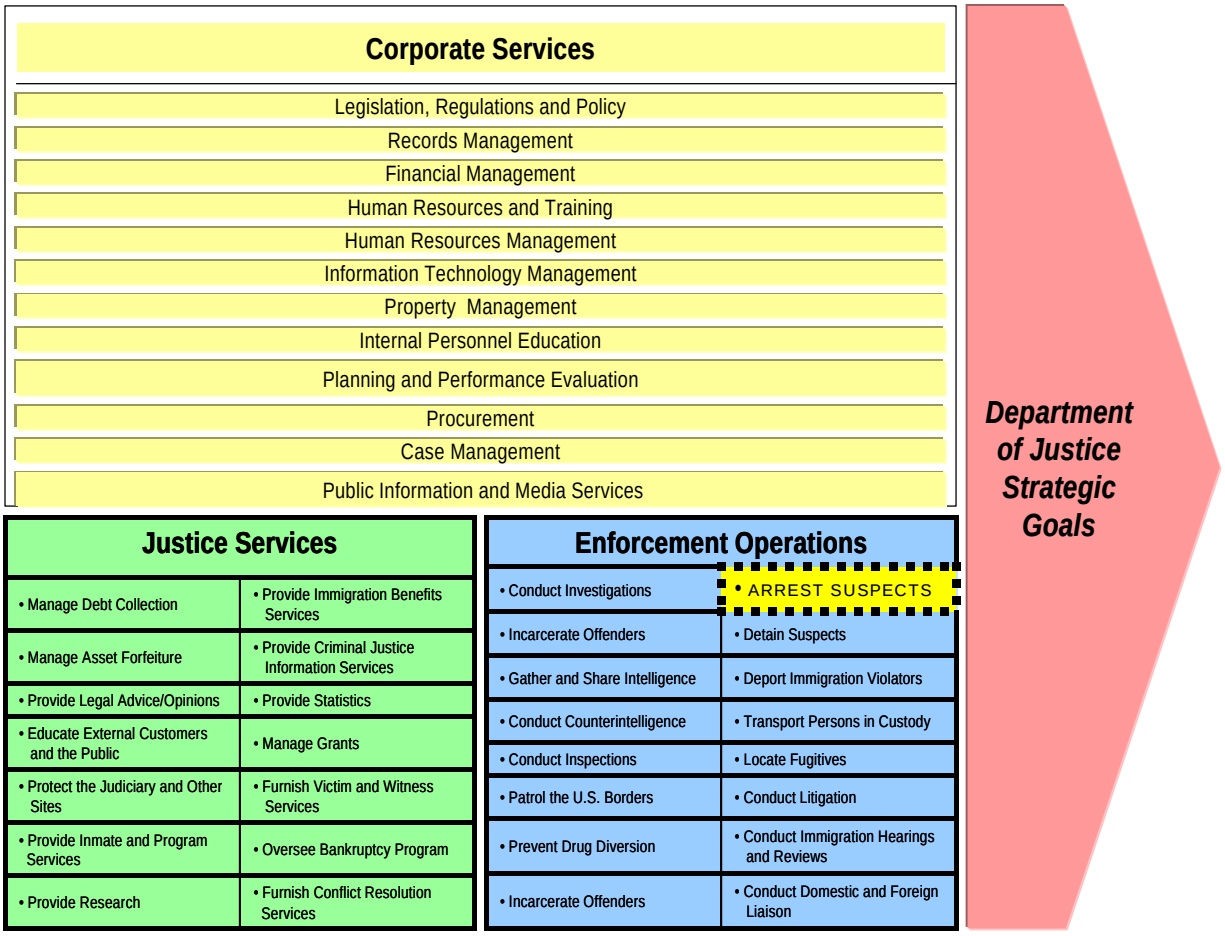



**Figure 8: Department of Justice Value Chain**

### 4.1.2 Overview of the Department of Justice Target Arrest Function

The Department has five law enforcement components that share responsibility for arresting suspects: Bureau of Prisons (BOP), DEA, FBI, INS, and United States Marshals Service

**Appendix F**
**Segment Architecture Analysis of the Law Enforcement Booking Process**

(USMS). A judicial case is initiated for any number of reasons, such as suspicion of wrongdoing, informant tip, intelligence, regulatory compliance audit, or arrest. Once a case is initiated, agents, analysts, investigators, and other personnel may perform additional functions as the case is developed. One such function may be an arrest[4].

The FBI, the DEA, and the INS are three of the components responsible for supporting the arrest function of the Department. While these components have different missions and goals, they perform many of the same business functions, processes, and activities. Each law enforcement component conducts a business function called *Arrest Suspects* and must capture and utilize certain offender information to perform their mission effectively.

### 4.1.3 The Target Booking Process

An important part of the "business" of any Federal law enforcement component is the rapid and positive identification of individuals under Federal arrest or detention. This requirement is driven by the mission of the *Enforcement Operations* business area, as well as, many of the Department's strategic goals. As shown in Figure 9, a process subordinate to the *Arrest Suspects* function is the booking process. This process consists of six activities.

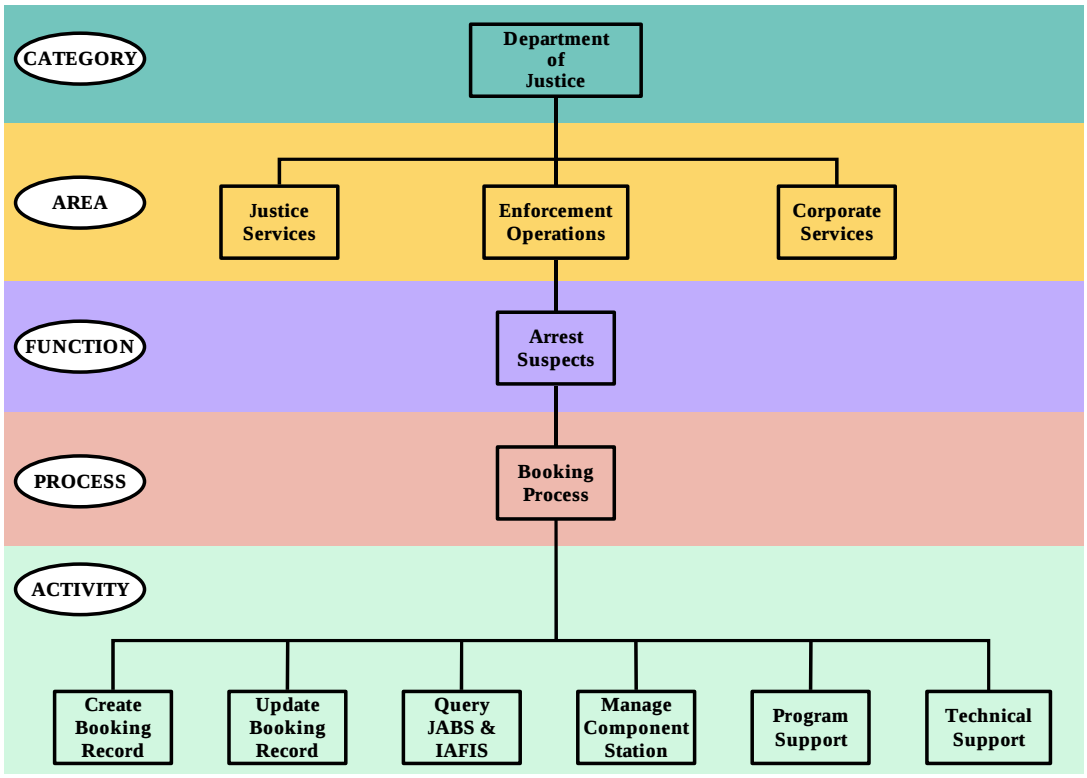



**Figure 9: The Business Structure of the Department of Justice**

[4] Taking an individual(s) into legal custody based upon observed offenses, probable cause, or prior warrants, and taking possession of all materials related to suspected criminal actions.

## Appendix F
## Segment Architecture Analysis of the Law Enforcement Booking Process

During the booking process, the arresting agent creates a record of the offense and biographical data on the offender; produces mug shots and evidentiary photographs; and captures the fingerprints of the offender for identification purposes and transmittal to the FBI.

### 4.1.4 The Target Booking Business Activities

The first step in developing the business architecture was to decompose the booking process into its key or high-level activities. When the decomposition process was complete, all the lowest level activities were identified. They represent unique activities that manipulate the data required to perform the booking process. Figure 10 lists the final or lowest level business activities associated with the target booking process.

| Activity Name | Activity Description |
|---|---|
| **Component Activities** | |
| **Create a New Booking Record** | This activity begins when the determination is made to "detain" a suspect. Booking information (e.g., identification numbers, personal information, fingerprints) is collected and input into the component level booking station. Once the data has been reviewed for accuracy and compliance with JABS standards, the "create" record is submitted to JABS. This activity ends when a verified IAFIS response has been received by the component. |
| **Update an Existing Booking Record** | This activity begins when a component has new or updated information pertaining to an existing booking record. The information is input into the component level booking station. This activity ends once the data has been reviewed for accuracy and compliance with JABS standards and the "update" record is submitted to JABS. |
| **Query JABS and IAFIS for Existing Booking Information** | This activity begins when a component has new or updated information that requires further investigation. The component must first determine the scope of the query (e.g., need additional information, determine detention location, view rap sheet). Subsequently, the "query" record is input into the component level booking station. Once the data has been reviewed for accuracy and compliance with JABS standards, the "query" record is submitted to JABS. When the requested information is returned, the component will review and analyze the information. This activity ends when the component determines the action, or next steps, required as a result of the analysis. |

**Figure 10: Booking Process Business Activities**

**Appendix F**
**Segment Architecture Analysis of the Law Enforcement Booking Process**

| Activity Name | Activity Description |
|---|---|
| **Component Activities** | |
| **Manage the Component Level Booking Station** | This activity begins when a Component receives new or revised Department standards, policies, or procedures related to the booking process. This can include technical interface information. All aspects of program management (e.g., System Development Life Cycle (SDLC) management, budget issues, system status) and technical management (e.g., operational system deployment, component level infrastructure, database administration) are included in this broad category. Operational support and maintenance are additional sub-activities. This activity ends when all operational systems have been disposed of and the project is transitioned or closed-out. |
| **JABS Management Activities** | |
| **Provide Department-wide Program Management for JABS** | This activity begins when the Department receives funding and approval to manage a Department-wide automated booking process. The Department establishes program standards, policies, and procedures related to the booking process. All aspects of program SDLC management, budget issues, system status) are included in this broad category. The Department continually monitors the project to ensure that JABS is meeting its overall performance measures and that it contributes effectively to the accomplishment of the Department's strategic goals. Enhancements to the system are managed using these goals as the basis for priority (e.g., desire to create a Federal Offender Tracking System). This activity ends when all operational systems have been disposed of and the project is transitioned or closed-out. |

| | |
|---|---|
| **Provide Department-wide Technical Support for JABS** | This activity begins when the Department receives funding and approval to manage a Department-wide automated booking process. The Department establishes technical standards related to the booking process. All aspects of technical management (e.g., operational system deployment, component level infrastructure, database administration) are included in this broad category. The Department continually monitors the project to ensure that JABS is meeting its technical performance measures. This activity ends when all operational systems have been disposed of and the project is transitioned or closed-out. |

**Figure 10: Booking Process Business Activities (Cont.)**

### 4.2 The Target Data Model

The purpose of the data architecture is to identify the data required to successfully and efficiently accomplish the target business activities described above. Additionally, the creation and manipulation of the data is analyzed to determine the prevalent data flow.

#### 4.2.1 The Target Booking Process Data Entities

Figure 11 depicts the major data entities used in the Department's booking process. The target data entities were selected for inclusion based on the activities outlined in the business model (see previous section). Data requirements are derived solely from business activities and are not related to who uses the data, where or when the data is used, or any current applications or technology solutions. Each of the data entities has at least one unique attribute that can be used to distinguish the different occurrences of that entity. For example, a *Subject* will have an identifying number or document; or an *Arresting (Booking) Officer* will have a unique badge number or employee number to distinguish different arresting officers within the Department.

| Data Entity | Description | Attributes |
|---|---|---|
| Arrest Event | An act of taking an individual into custody resulting in, or from, the formal charging of an individual for a violation of the law (not an immigration law) | Arrest description |
| Arresting (Booking) Officer | A Department or Component employee (or deputized official) who takes a subject into custody and creates a booking package | Arresting officer's identifying information |
| Associate | An individual who is known to the subject, but is not related, and associated with the arrest event | Associate's identifying information |

**Appendix F**
**Segment Architecture Analysis of the Law Enforcement Booking Process**

| | | |
|---|---|---|
| Biometrics | A biological characteristic of a person that can be used for identification or verification | Ten-print fingerprints |
| Booking Event | An act of collecting information about a subject that results in the creation of a booking package | Booking administration information |
| Detention Location | A room or building where persons are held in custody | Location code |
| FBI Identification Record "Rap Sheet" | A document containing the chronology of a subject's arrest and incarceration history | FBI identification record |
| Judicial Case | A case related to the administration of penal or criminal law | Case number |

**Figure 11: Booking Process Data Entities**

| Data Entity | Description | Attributes |
|---|---|---|
| Subject | A person who is the focus of an arrest or booking event | Mugshots, physical descriptions, Scars, Marks, and Tattoos (SMT) photos, medical/mental history, family members, identifying numbers and documents |
| Technology Resources | A system, technique, or technology asset used to automate business functions, processes, and activities (This includes Enterprise Architecture) | Hardware, software, network, infrastructure, and applications |
| Vehicles | A device or structure for transporting persons or items | Vehicle description and identifying numbers |

**Figure 11: Booking Process Data Entities (Cont.)**

### 4.2.2 Relationship of Activities and Data Entities

The table displayed in Figure 12 depicts the relationship between the target business activities defined in Section 4.1.4 and the target data entities listed in Section 4.2.1. The matrix identifies what actions an activity performs on the data element. For the purposes of this analysis, an activity can create (C), update or modify (U), reference or query (R), or delete (D) the target data entity. These relationships are important for determining the sequencing of the new applications, which will become an important basis for prioritizing available funds. It is necessary to design and build the applications that create the data entity prior to those applications that update or reference those same entities.

## Appendix F
## Segment Architecture Analysis of the Law Enforcement Booking Process

| Business Activity Names | Data Entities: Arrest Event | Arresting (Booking) Officer | Associate | Biometrics | Booking Event | Detention Location | FBI ID Record "Rap Sheet" | Judicial Case | Subject | Technology Resources | Vehicles |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Component Level Activities** | | | | | | | | | | | |
| Create a New Booking Record | **R*** | **R*** | **C** | **C** | **C** | **R*** | **C** | **R*** | **C** | | **C** |
| Update an Existing Booking Record | **R** | **R** | **RUD** | **RUD** | **RUD** | **R** | **RUD** | **R** | **RUD** | | **RUD** |
| Query JABS/IAFIS for Existing Booking Information | **R** | **R** | **R** | **R** | **R** | **R** | **R** | **R** | **R** | | **R** |
| Manage the Component Level Booking Station | | | | | | | | | | **CRUD** | |
| **Department-Level Activities** | | | | | | | | | | | |
| Provide Department-wide Program Management for JABS | | | | | | | | | | **CRUD** | |
| Provide Department-wide Technical Support for JABS | | | | | | | | | | **CRUD** | |

Legend: C - Create, R - Reference, U - Update, D - Delete

***** Some data entities are created by activities that are out of the scope of this analysis

Figure 12: Booking Process C-R-U-D Matrix

This document contains information that serves the purpose of demonstrating an example of a segment architecture and does not reflect the current JABS program in its entirety.

**Appendix F**
**Segment Architecture Analysis of the Law Enforcement Booking Process**

## 4.3 The Target Application Model

The purpose of the application architecture is to define the major and significant applications needed to manage the data entities and support the business functions of the Department. It is not intended to provide detailed system design or a requirements analysis, but rather to provide an analysis of what applications will do to help manage the data. Figure 13 provides a list of the target applications for the Department's booking process. A brief description of the applications is included along with the supported requirements and objectives. The logical relationship of these target applications is provided in Figure 14.

| Application Name | Description of Application | Activities Supported | Objectives Supported | Status |
|---|---|---|---|---|
| Core JABS | A conduit and central control module for Department booking process | Create<br>Submit<br>Update<br>Query<br>JABS Program Mgmt<br>JABS Tech Mgmt | Automate Booking Process<br>Share Booking Data<br>Track Federal Offenders | Existing |
| Offender Tracking Module (JABS) | A searchable database for data about Federal offenders | Update<br>JABS Program Mgmt<br>JABS Tech Mgmt | Track Federal Offenders | New |
| Latent Fingerprint Processing Module (JABS) | Allow fingerprint matching based on latent fingerprints | Update<br>Query | Automate Booking Process<br>Share Booking Data<br>Track Federal Offenders | New |
| Update Transaction Processing Module (JABS) | Allow updates to suspect records without triggering a response from IAFIS | Update | Share Booking Data<br>Track Federal Offenders | New |
| Security Upgrade Module (JABS) | Enhance the security features of JABS | JABS Program Mgmt<br>JABS Tech Mgmt | Automate Booking Process | New |
| IAFIS | Stores biometric and criminal history data | Query | Automate Booking Process<br>Share Booking Data<br>Track Federal Offenders | Existing |
| Component Booking Stations | A central control module for component booking process | Create<br>Update<br>Query<br>Component Sys Mgmt | Automate Booking Process<br>Share Booking Data | New |

**Figure 13: Application Matrix for Booking Process**

## Appendix F
## Segment Architecture Analysis of the Law Enforcement Booking Process

| Application Name | Description of Application | Activities Supported | Objectives Supported | Status |
|---|---|---|---|---|
| DEA/JABS Interface Module | A central control module for DEA booking process | Create<br>Update<br>Query<br>Component Sys Mgmt | Automate Booking Process<br>Share Booking Data | Existing |
| SENTRY/ JABS[5] | A central control module for BOP booking process | Create<br>Update<br>Query<br>Component Sys Mgmt | Automate Booking Process<br>Share Booking Data | New |
| FBI/JABS[5] | A central control module for FBI booking process | Create<br>Update<br>Query<br>Component Sys Mgmt | Automate Booking Process<br>Share Booking Data | New |
| Prisoner Tracking System/ JABS[5] | A central control module for USMS booking process | Create<br>Update<br>Query<br>Component Sys Mgmt | Automate Booking Process<br>Share Booking Data | |

**Figure 13: Application Matrix for Booking Process (Cont.)**

[5] These applications are outside of the scope of this segment analysis, but are part of JABS, Version 2.0.

**Appendix F**
**Segment Architecture Analysis of the Law Enforcement Booking Process**

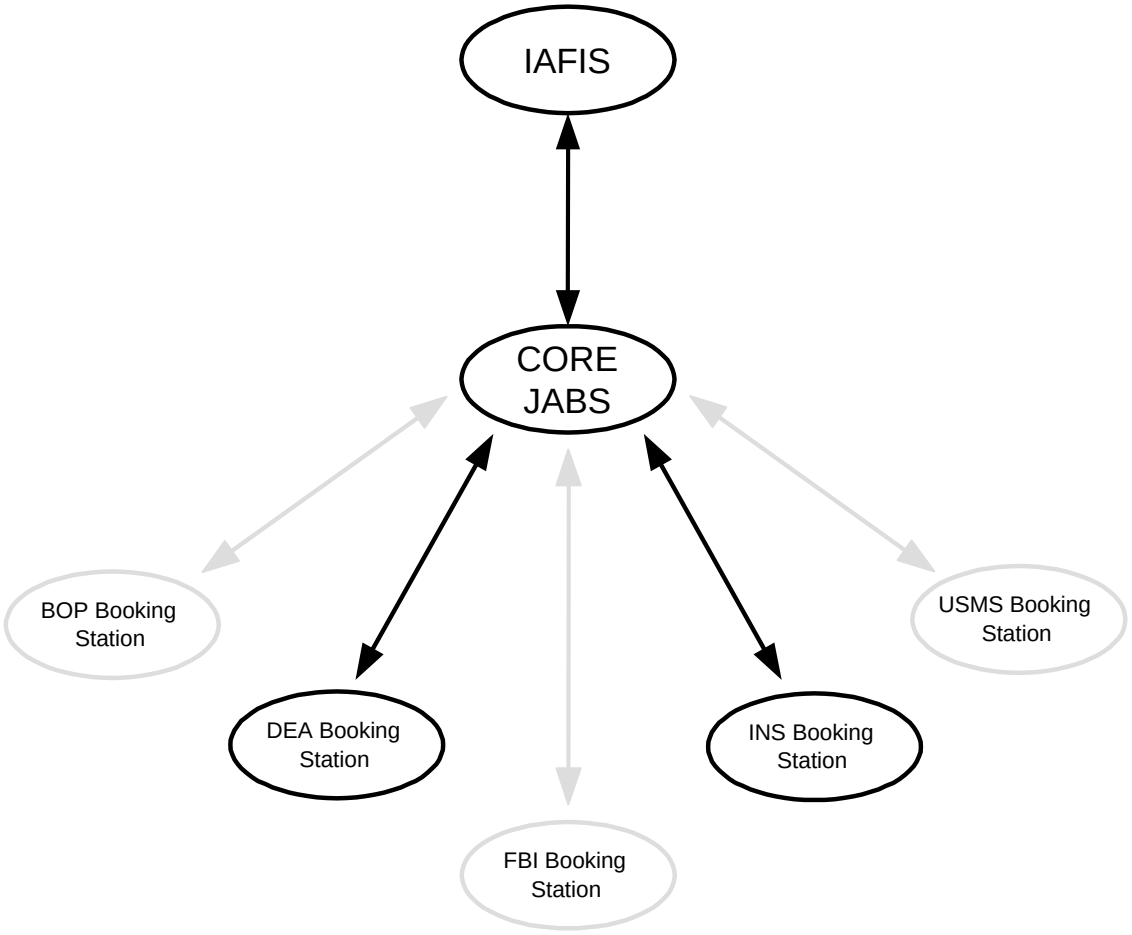



**Figure 14: Logical Relationship of Target Booking Process Applications[6]**

## 4.4 The Technology Model

A tenet of the JABS technology architecture is that each component's booking process is independent. Each component will establish a strategy that meets its own mission and technical requirements. In order to support both the components' missions and the Department-wide mission, the components will need to establish booking stations that include:

Pentium class workstations

Ten-print fingerprint devices

Digital cameras

Scanners

[6] The grayed sections are outside of the scope of this segment analysis, but are part of JABS Version 2.0.

**Appendix F**
**Segment Architecture Analysis of the Law Enforcement Booking Process**

Printers

JABS provides transport and validation services for submitting fingerprints to IAFIS and passing any results back to their submitter. In order to fulfill these requirements, the JABS technology architecture will consist of the following items:

- VPN switch
- IDS analysis reduction tool
- Router
- Ethernet switch
- Firewall
-

JABS will also provide a searchable repository to be used by the components in pursuit of their strategic goals. The technology architecture supporting that requirement will consist of two server class machines on a network segment. In order to meet operational requirements, it will have redundant critical subsystems including:

- System disks
- Power supplies
- CPUs
- Cooling fans for high reliability operations

The diagram displayed in Figure 15 shows how these individual Components interact to form the basic “system” called JABS.

**Appendix F**
**Segment Architecture Analysis of the Law Enforcement Booking Process**

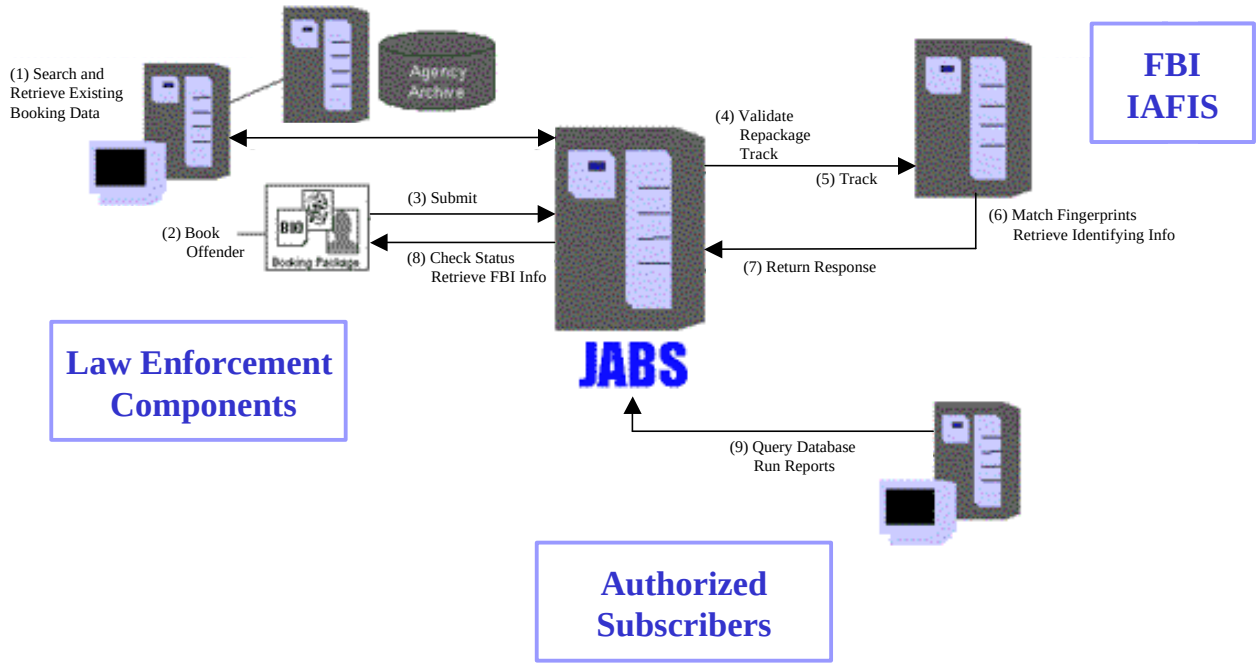



**Figure 15: Automated Booking Workflow**

## 4.5 Summary of the "To Be" Model

The target business, data, applications, and technology architectures above will allow the Department to design and implement a booking process that will enable its law enforcement components to share booking data; facilitate the rapid identification of suspects through IAFIS; and track Federal offenders. When complete, all of the Department's law enforcement components will have an automated booking station, riding a robust infrastructure, to create the booking data repository.

**Appendix F**
**Segment Architecture Analysis of the Law Enforcement Booking Process**

## PART II: Analysis of the Architectural Model

## 5.0 GAP ANALYSIS

### 5.1 Summary of Analysis

The segment analysis identified three goals of the Department's booking process: to enable the Department law enforcement components to share booking data; to facilitate the rapid identification of suspects; and to develop a means to track Federal offenders. The current architecture does not support these goals primarily because the INS submission process has not been automated. The target architecture, however, would accomplish these goals and allow for an effective and efficient automated booking process. The residual effect of fully automating this process would be to allow the law enforcement components to share booking data and, as such, would be the first step toward establishing a Federal offender tracking system.

The following list outlines the major enhancements that would have to be addressed to migrate from the *Current* to the *Target* architecture.

- Fully develop the component booking stations to allow for the automated collection and submission of booking data to IAFIS through JABS
- Modify Core JABS to allow components to update existing booking data records (i.e., modify the Core JABS Booking Record Update process to allow updates to JABS booking records without always triggering a transaction to IAFIS)
- Modify Core JABS to upgrade the security infrastructure with enhanced user authentication and data encryption to the user workstation
- Modify Core JABS to provide the ability to process latent fingerprint transactions
- Modify Core JABS to contain the initial functionality to position JABS as a conduit for a Federal offender tracking system

### 5.2 Constraints and Limitations

The following are potential constraints and limitations to achieving the major enhancements.

- Changing Department and Component priorities
- Hiring a sufficient number of analysts to complete the development work
- Training a large number of employees
- Completing infrastructure upgrades to accommodate additional traffic
- Retaining the autonomy of each component's booking system
- Collecting and submitting relevant criminal history information to the JABS in a timely manner (must avoid significantly increasing the time required by the INS to process aliens)

---

- Recognizing that Components may have competing or contradictory technical requirements
- Having sufficient funds available

### 5.3 Operational Requirements

Any enhancements or modifications of JABS must meet the following list of target operational requirements:

- The system should be available continuously (i.e., 24/7/365)
- Core JABS should process a valid booking transaction within 2 minutes
- IAFIS should, on average over a 30-day period, return a response to JABS within 2 hours
- The system should be scalable to accommodate an increasing number of bookings
- All data records should be stored for 99 years (or as determined by the JABS PMO)
- The system should support the printing of Core JABS data and fingerprint cards from component printers (components will control the capability of configuring their own printers)

### 5.4 Mitigating Actions

- The following list provides possible mitigating actions that can be considered when developing a detailed strategy for transitioning from the “As Is” to the “To Be” architecture.
- Prioritize the applications and sequence the projects to span multiple fiscal years
- Use FBS as a strawman model, to avoid costly and time-consuming research and development
- Use existing JABS Application Program Interface (API) in IDENT/IAFIS workstations
- Integrate JABS training into existing training programs
- Coordinate the deployment of JABS booking stations to coincide with component infrastructure improvements

### 5.5 Additional Benefits

The following are additional benefits derived from the completion of the target architecture:

- All law enforcement components will have the ability to identify individuals with “wants and warrants”, criminal records, and previous INS encounters based on real-time data
- A fully deployed JABS will facilitate the collection and development of arrest metrics
- Reduce the likelihood that criminals will be unwittingly released from custody
- Provide Federal, state, and local law enforcement organizations with an integrated picture of the criminal activity known to components of the Department, including INS encounter histories of persons who have illegally crossed the border

---

**Appendix F**
**Segment Architecture Analysis of the Law Enforcement Booking Process**

## 6.0 TRANSITION PLAN

### 6.1 Sequencing Considerations

The following elements were considered in developing the sequencing of the new applications outlined in the transition plan:

- Business Priorities – Impact on achieving the program goals of JABS
  - Facilitate the sharing of information
  - Reduce the time needed to identify suspects
  - Improve the ability to track Federal offenders
- Data Dependency – The phase of the data lifecycle that is affected (i.e., C-R-U-D)
- National Security – The likelihood that criminals will be identified and detained
- Congressional Directives – The level of political sensitivities or direction (e.g., 1999 Congressional directive to integrate the fingerprint systems of FBI and INS[7])

These sequencing considerations are used to create a priority scheme for the design, development, and deployment of system enhancements as seen in Figure 16.

| | SEQUENCING CONSIDERATIONS | | | |
|---|---|---|---|---|
| **ENHANCEMENTS** | Business Priorities | Data Dependency | National Security | Congressional Directives |
| **Component Level** | | | | |
| Component Booking Stations | **High** | **High** | **High** | **High** |
| **Core JABS** | | | | |
| Offender Tracking | **High** | **High** | **High** | **Medium** |
| Process Latent Fingerprints | **High** | **High** | **High** | **Low** |
| Process Update Transactions | **High** | **High** | **Medium** | **Low** |
| Upgrade Security of System | **High** | **Medium** | **Medium** | **Medium** |

**Figure 16: Sequencing Considerations for JABS Enhancements**

[7] The FY2000 House Appropriations Report expressed the belief that Federal, state, and local law enforcement should have access to INS fingerprint information and that the INS should have the full benefit of FBI criminal history records. The House report directed that INS suspend further deployment of IDENT until DOJ submitted to the Committee a plan for integration of IDENT and IAFIS. The subsequent conference report retained the provision.

**Appendix F**
**Segment Architecture Analysis of the Law Enforcement Booking Process**

## 6.2 Transition Plan

Through analysis of the sequencing priorities as depicted in the previous table, a summary transition plan can be developed which mirrors the priority scheme. Figure 17 outlines the individual milestones that would allow the Department to transition from the current or "As Is" architecture to the target or "To Be" architecture. The project would be bounded by the constraints, limitations, and operational requirements discussed in Sections 5.2 and 5.3. However, this plan serves as an initial blueprint that can be used by those who will be tasked in the future with making funding and development decisions.

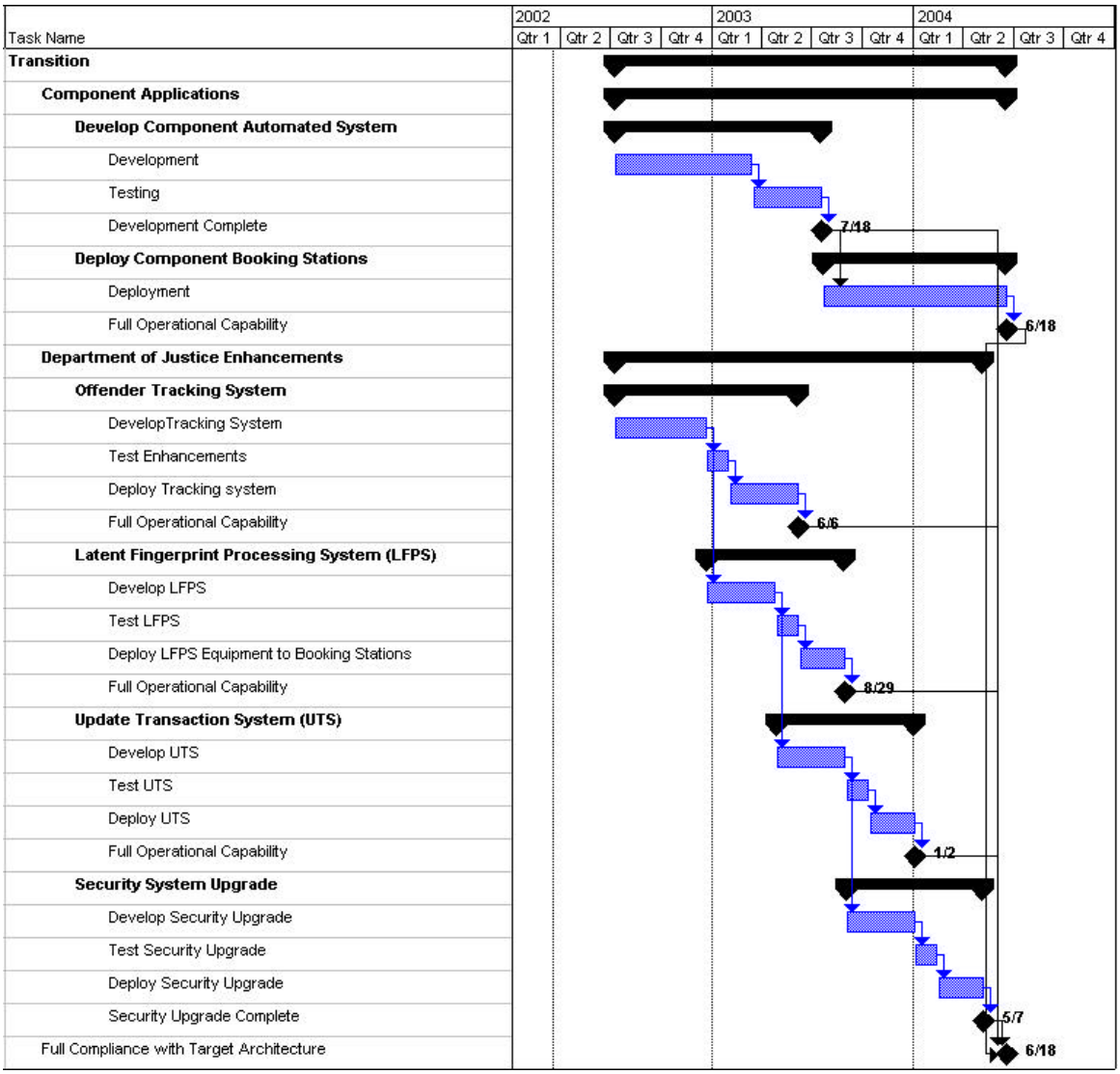



**Figure 17: Summary Transition Plan**

## Appendix F
## Segment Architecture Analysis of the Law Enforcement Booking Process

### GLOSSARY OF GENERAL ENTERPRISE ARCHITECTURE TERMS[8]

| | |
|---|---|
| **APPLICATION ARCHITECTURE** | A component of the design architecture that defines the major applications needed to manage data and support business functions. |
| **BUSINESS ARCHITECTURE** | A component of the current and target architectures which relates to the enterprise mission and goals. It contains the content of the business models and focuses on enterprise business areas and processes responding to business drivers. The business architecture defines enterprise business processes, enterprise information flows, and information needed to perform business functions. |
| **CURRENT ARCHITECTURE** | The current state of an enterprise's architecture. The "As Is" model is the representation of the cumulative "as-built" or baseline of the existing architecture. |
| **DATA ARCHITECTURE** | A component of the design architecture. The data architecture consists of among others, data entities, which have attributes and relationships with other data entities. These entities are related to the business functions. |
| **GAP ANALYSIS** | The process whereby an enterprise identifies, and determines the effort required to correct gaps or deficiencies between its desired (target) architecture and its actual (current) architecture. |
| **SEGMENT ARCHITECTURE** | An abridged enterprise architecture analysis that focuses on only one "segment" or business area of the enterprise. A segment architecture document should provide sufficient information to guide investment decisions and system designs within the segment. |
| **TARGET ARCHITECTURE** | The target state of an enterprise's architecture. The "To Be" model is the representation of a desired future state or "to-be-built" for the enterprise within the context of the strategic direction. |
| **TECHNOLOGY ARCHITECTURE** | The physical depiction of the technology environment for the enterprise showing actual hardware and systems software at the nodes and lines and their systems software, including operating systems and middleware. |

[8] These definitions were derived from a variety of Federal CIO Council documents.

**Appendix F**
**Segment Architecture Analysis of the Law Enforcement Booking Process**

| | |
|---|---|
| **TRANSITION PLAN** | The blueprint or plan that helps an enterprise to bridge the gap between its "As Is" and "To Be" models. The plan should identify the required transition activities, the priorities, and the milestones/timelines. |