Table of Contents

Appendix A - DOJ Component Information

Appendix B - JMD Office of IRM Senior Officials

Appendix C - DOJ Component Chief Information Officers

I.   Introduction

This document briefly describes the Information Resources Management (IRM) program of the U.S. Department of Justice (DOJ). It outlines the current organizational structure and the mission requirements that affect the Justice IRM program, describes the technical infrastructure that provides the backbone for automated systems and telecommunications activities, and highlights significant endeavors in support of the Department's mission goals and strategic plan.

II. Overview of the Mission, Functions and Organization of the Department of Justice

The mission of the DOJ is to enforce federal law and defend the interests of the United States according to the law, to provide federal leadership in preventing and controlling crime, to seek just punishment for those guilty of unlawful behavior, to administer the nation's immigration laws fairly and effectively, and to ensure fair and impartial administration of justice for all Americans.

To carry out this mission, the DOJ has established seven strategic goal areas, discussed in detail in the Department's Strategic and Performance Plans, which can be accessed via the DOJ website (http://www.usdoj.gov):

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

The DOJ is led by the Attorney General (AG) of the United States. The AG directs and oversees the work of a large number of separate component entities within the Department. These components include the Department's five major law enforcement bureaus: the Federal Bureau of Investigation (FBI), the Drug Enforcement Administration (DEA), the United States Marshals Service (USMS), the Immigration and Naturalization Service (INS), and the Bureau of Prisons

(BOP). There are also six divisions that conduct litigation (Civil, Criminal, Antitrust, Civil Rights, Environment and Natural Resources, and Tax), plus the Justice Management Division (JMD), the United States Attorneys, and additional organizations (known as Offices and Boards) essential to the Department's fulfillment of its mission. **Appendix A** provides several information sources on the mission, organization, budget, projects, and accomplishments of most of DOJ's major entities. The larger components, principally the bureaus and divisions, have separate IRM staffs and budgets, while smaller components draw upon the resources of others (e.g., the Justice Management Division).

Although the Department is headquartered in Washington, DC, most of its work takes place outside of Washington. As a result, a majority of its more than 130,000 employees are dispersed in roughly 2,000 installations of the Department around the country (ranging from single-person border stations to large division offices in major cities), or in one of its nearly 100 overseas offices.

The Department's budget is a little over $23 billion. Much of its growth in recent years has been due to increased funding for criminal investigations, prisons, immigration control, and state and local assistance.

III. The DOJ IRM Program

Goals

The mission of the Department's IRM program is to provide high quality information technology (IT) services that meet customer needs, generate positive return on investment, and support improved performance. Specific goals include:

Architecture	Provide the best IT solutions and a robust infrastructure to support evolving business needs.
Security	Foster customer access and trust through secure data, systems, and infrastructure which assure confidentiality, integrity, and availability.
Investment Management	Maximize the value of IT investments to improve delivery of programs and services to the public and to pursue innovation and high quality in the development and use of IT products and services.
Workforce	Ensure a workforce that has the necessary IT skills and tools to accomplish their jobs effectively and efficiently.

Organization

The Information Resources Management (IRM) program resides within the Justice Management Division (JMD). JMD is the administrative arm of the Department and has policy, oversight, and service delivery responsibilities in such diverse functional areas as budget, finance, procurement, and personnel, in addition to IRM.

The Assistant Attorney General for Administration (AAG/A) heads JMD and serves as the Department's Chief Information Officer (CIO). As the CIO, the AAG/A provides leadership and policy direction for DOJ IRM activities.

The Deputy Assistant Attorney General for IRM (DAAG/IRM) heads the Office of IRM and is the Deputy CIO for the Department. As the Deputy CIO, the DAAG/IRM coordinates and guides IRM initiatives Departmentwide. The DAAG/IRM is supported by six JMD/IRM staffs.

- Computer Services Staff (CSS). CSS operates the Justice Data Centers that provide critical data processing services to Department components (with the exception of the FBI).

- Information Management and Security Staff (IMSS). IMSS develops and implements policies and procedures for IT investment management and information systems security programs. IMSS also manages the Department's IT architecture.

- Systems Engineering and Development Staff (SEDS). SEDS is tasked with project management and development activities, including the Joint Automated Booking System (JABS) project, the IDENT/IAFIS project, the Justice Consolidated Office Network (JCON) Project Management Office (PMO), the Enterprise and Directory Services project, and Web development.

- Systems Technology Staff (STS). STS provides a broad range of office automation and applications support services (including web development) for the JMD, the DOJ Senior Management Offices (SMOs), the litigating divisions, and other departmental components. STS also manages the operation of JCON for JMD and the Senior Management Offices and Justice On-line Information Network (JOIN), which provides Internet access and departmental e-mail access.

- Telecommunications Services Staff (TSS). TSS is the DOJ network services provider and has leadership responsibility for consolidating the Department's data networks. TSS also provides voice and data communication services for the DOJ components.

- Wireless Management Office (WMO) Staff. The WMO was established to coordinate planning, share resources, and foster interoperability among the departmental components for wireless communications. To accomplish this, the WMO will establish a Justice

Wireless Network (JWN) composed of a complementary mix of land mobile radio and commercial services.

A listing for JMD/IRM management is provided in **Appendix B**.

Although JMD/IRM provides many computer and telecommunications services on a departmentwide basis, the components have been delegated considerable independence and discretion in the planning, acquisition, and deployment of information systems on their own. Each of the major law enforcement bureaus, as well as the United States Attorneys, manage additional large-scale IRM efforts of their own. The litigating divisions and smaller components also have separate IRM programs. Each IRM organization in the Department is responsible for the information and IT assets needed to carry out its respective mission. Components exercise this responsibility by developing plans, budgets, and procurement strategies to acquire IT. Additionally, most components manage the development and operations of their own systems and the delivery of IT products and services.

Departmental IRM Coordination

Under the leadership of the Deputy CIO, the Justice CIO Council provides a forum for sharing information and for discussing and resolving IRM issues that affect multiple components. The Council deals with departmentwide information management policies and priorities, helps coordinate systems development and acquisition matters, and identifies areas where assistance is needed. The Council comprises the CIOs of the various DOJ components plus several non-IRM officials as appropriate. The component CIOs are listed in **Appendix C**.

The Department's Information Technology Investment Board (ITIB) advises the Attorney General on IT priorities and IT management issues that impact the Department's strategic initiatives and operational programs. The ITIB is chaired by the Department's Deputy Attorney General and is composed of the heads or principal deputies of the major law enforcement and litigating components. High cost, high risk, and high impact IT investments are monitored through a departmental management process under the direction of the CIO and in cooperation with the component CIOs.

Resources

About seven percent of the Department's total operating budget is spent on IT. DOJ's obligations for IT will be about $1.6 billion in fiscal year (FY) 2001. The INS, FBI, and JMD together account for almost two-thirds of the Department's total IT spending.

The Federal Government requires the reporting of IT outlays according to mission areas and infrastructure/office automation. This requirement is designed to provide basic information to link internal planning, budgeting, and management of IT resources to the mission and core functions of the Department. DOJ's data is available on the Department's World Wide Web site. (See

Budget Exhibit 53, Report on Information Technology.) Most of the mission areas and projects that are identified on the Web site correspond to specific organizational components, and the correspondence is either stated explicitly or readily inferred. The exhibit shows appropriated amounts for FY 2000 and FY 2001, and the President's requested amounts for FY 2002.

Future Direction

The effective use of IT is increasingly vital to the Department's ability to perform its mission. Technology enables the Department to maintain its fight against increasingly sophisticated criminal enterprises; to store, manipulate, and retrieve vast amounts of information related to complex litigation; to better control our nation's borders; to provide swifter, more convenient, and more reliable services to the public; and to "work faster and smarter." General trends include the following:

        C   The development of interoperable systems that facilitate the timely and secure sharing of investigative information among federal, state, and local law enforcement agencies, and between law enforcement and prosecutors;

        C   The increased application of biometrics, video teleconferencing, and Internet technology;

        C   The use of more effective and sophisticated computer and telecommunications security; and

        C   The implementation of DOJ processes that enable better planning for and managing of IT investments.

IV. Technical Infrastructure

Central Processing Capabilities

JMD operates a state-of-the-art data center that offers a wide range of mid-size and large-scale central processing services to DOJ. This resource provides around-the-clock, non-classified information processing capabilities to all departmental components, except for the FBI, which has its own host computing capabilities.

The FBI presently operates two data centers for processing both classified and non-classified information. These data centers provide for the large-scale automated information needs of FBI agents and administrative personnel located throughout the United States and at locations abroad.

Telecommunications

Improving the Department*s telecommunications capabilities is a high priority, since rapid and reliable communications are vital to effective law enforcement. Some of the more prominent telecommunications initiatives are the Washington Area Switch Program successor (WASP II), the Justice Metropolitan Area Network (MAN), and the Justice Consolidated Network (JCN). The Department is also pursuing a new wireless networking environment, and greater networking capabilities across the national criminal justice community. Each is described briefly in the following.

The Washington Area Switch Program (WASP II) provides a state-of-the-art telecommunications system that has replaced a majority of the Department's older Washington area telephone systems. WASP II provides a digital switching system, enabling the integration of voice and data communications, while vastly improving the quality, delivery, and management of communications.

The Washington Metropolitan Area Network (MAN) offers a high-speed fiber optic network with a common communications backbone, which connects departmental components throughout the Washington metropolitan area. The MAN enhances network performance, enables access to applications requiring higher bandwidth capacity (imaging, videoconferencing, distributed databases, etc.), and improves security.

The Justice Consolidated Network (JCN) provides the Department with a high-capacity wide-area network. Through JCN, the DOJ will consolidate the departmental telecommunications networks onto one major data transport system to reduce costs. An additional benefit is that the JCN offers support to the components' emerging high-capacity data transmission requirements without the disruption of ordering new services and removing outdated services.

The Justice Wireless Network is a Congressional mandate to provide Department law enforcement, investigative, and detention officers with modern interoperable mobile communications services. The new network will replace the six existing land mobile radio systems operated by the Federal Bureau of Investigation, Drug Enforcement Administration, Immigration and Naturalization Service, Bureau of Prisons, U.S. Marshals and the Office of the Inspector General. The objectives of the Justice Wireless Network include implementing a narrow-band communications system; maximizing the use of radio spectrum; improving wireless communications among Department components, as well as with state, local and other federal law enforcement agencies; and reducing the cost of wireless communications services.

The Global Criminal Justice Information Network (GLOBAL) aims to develop and implement a standards-based electronic information exchange capability, providing DOJ components with timely, accurate, complete, and accessible information in a secure and trusted environment. The value of a Global Justice Information Network capability is that it benefits *all* operational justice officials.

This level of information sharing can be accomplished most efficiently by using state-of-the art technologies to create a new network capability rather than a new network. Where possible, the goal is to enhance, expand, and link the current networks and systems under open, Web-based standards that enable broader sharing of relevant information. As new systems are designed within each justice discipline using Internet and Internet-like technologies, they can be linked to the existing enhanced networks, bringing increased benefits to the new users and, at the same time, adding value to the universal infrastructure.

Because the goal is a new network *capability* rather than an entirely new network, the GLOBAL is not a separate effort creating redundancy or conflict regarding national justice planning, policy, and standards setting. Rather, it is an effort to advise the Attorney General on current justice systems integration planning and design efforts, as well as on new and developing technologies that affect justice information sharing.

The FBI Digital Collection system for the Foreign Intelligence Surveillance Act (FISA) will provide the foundation for an up-to-date, flexible digital collection infrastructure. Deployment of this system will significantly enhance system interoperability through electronic information transfer in a common mode format. The digital collection system for FISA will be configured to support a wide variety of new collection requirements such as fax and modem intercepts. This system will consolidate existing collection capabilities into a single system with multi-line collection, monitoring, recording, and playback capabilities.

The CJIS WAN is the national communications infrastructure, as well as the Criminal Justice Information Services (CJIS) Division's main Transmission Control Protocol/Internet Protocol (TCP/IP) based network. It provides secure electronic connectivity to customers who require access to the CJIS Division's law enforcement services, including the Integrated Automated Fingerprint Identification System (IAFIS) and the National Crime Information Center (NCIC) 2000. The CJIS WAN also provides access to the Laboratory Division's Combined DNA Index System and DRUGFIRE. The CJIS WAN provides the bandwidth, encryption, access control, sub-network interface services, and the communications protocols necessary to enable secure use of these systems.

The FBI network (FBINET) provides secure data communications to all FBI offices. The FBI currently relies on the data communications infrastructure that was designed in Fiscal Year (FY) 1991 to support the FBI's Systems Network Architecture (SNA)/token ring network. The FBI's data communications infrastructure directly supports the FBI's investigative and administrative core mission. The information technology environment used by FBI's Legal Attaches (Legats) has received minimal upgrades over the past ten years. The FBI has a plan to increase bandwidth to existing and proposed Legats, replace legacy telecommunications equipment currently being used to access the Department of State's (DOS) worldwide network, and provide for other infrastructure-related requirements.

The Secure Automated Message Network (SAMNET) is the FBI's secure messaging system used to transmit and receive messages from the intelligence community and other agencies. SAMNET is also used by field and legal attache offices to exchange documents up to the Top Secret/Sensitive Compartmented Information (TS/SCI) level. Currently, messages are received via SAMNET and sent to printers for manual assembly and delivery. SAMNET hardware and software is being upgraded to (1) enhance message preparation, transmission, and dissemination; and (2) meet the Department of Defense requirement that all civilian agencies have full operational capabilities to interface with the Defense Messaging System by FY 2003.

Office Automation Platforms

Office automation (OA) support is tailored to meet the needs of the various components of the Department. The Department's bureaus operate and manage office automation systems designed to meet their respective requirements. Several components, including the FBI, INS, DEA, and USMS, are undertaking efforts to replace, expand, or upgrade their individual office automation systems.

The Justice Consolidated Office Network (JCON) II Program is an infrastructure initiative that provides a reliable, robust and common platform upon which the Department's litigating and management components operate their office automation applications. There are approximately 24,000 users in 11 Department components, including participants from the Antitrust (ATR), Civil (CIV), Civil Rights (CRT), Criminal (CRM), Environment and Natural Resources (ENR), and Tax (TAX) Divisions; the Executive Office for the United States Attorneys (EOUSA); the Executive Office for Immigration Review (EOIR); the United States Trustees (UST); the Community Relations Service (CRS); the Justice Management Division (JMD), and the Department's Senior Management Offices.

To date, the JCON II Architecture has been implemented in seven components, including: CIV, CRS, CRT, ENR, TAX, UST, and JMD. One component, EOIR, has completed a partial roll-out of the JCON II Architecture. EOUSA is currently in the implementation phase of the JCON Systems Development Life-Cycle. The benefits of the JCON II system include: enhanced component interoperability, improved data integrity and security, and increased component productivity.

In order to keep pace with rapid technology change and to avoid the obsolescence of the JCON II Architecture, the JCON Program Management Office (PMO) has embarked upon the JCON IIA project, a modernization effort aimed at ensuring the current JCON II Standard Architecture continues to remain a viable platform for the foreseeable future. This project represents the logical evolution of the JCON II Standard Architecture rather than a complete system replacement. That is, the JCON IIA project will leverage, as much as is practical, the investment made in the current architecture. In addition, this updated architecture will interoperate with the current system until all JCON II components can transition to the JCON IIA platform. ATR and CRM are the first two components scheduled to implement the new JCON IIA Architecture.

The BOP Network (BOPNet) is a local and wide area network that provides an infrastructure for the electronic transmission of information among all BOP locations. The BOPNet wide area network is monitored by a network control center in Washington, DC. BOPNet provides a flexible computing environment and allows access to local secure servers that maintain sensitive databases on the institution's inmate population.

The DEA's FIREBIRD project upgrades DEA*s IT infrastructure by implementing a flexible hardware and software architecture to include a communications plant, network servers, workstations, office automation support applications, and specialized system services. FIREBIRD enables agents, investigators, and analysts to manage case material from their desktop workstations more efficiently, to gain immediate access to critical information, and to exchange information within the DEA.

The INS network INSINC supports the communications requirements of INS. The INS Technology Infrastructure Project (TIP) standardizes the Wide Area Network (WAN) and Local Area Network (LAN) architecture throughout INS. Operational capabilities provide for the capture and sharing of data across all levels for INS offices, including District Offices, sub-offices, and satellite sites, as well as Border Patrol sections, stations, checkpoints, and satellite offices. The standard hardware suite includes workstations, servers, local area networks, the wide area network, scanners, and other peripherals.

The Marshals Network (MNET) provides an infrastructure for mission-critical communications and enterprisewide information. MNET gives USMS offices local area networks which are connected by a wide area network (WAN). MNET provides high speed data communications for electronic mail, office automation functions, and mission-critical applications.

The FBI's TRILOGY project will provide a much needed infrastructure upgrade for the Bureau. In 1997, the FBI established the Information Sharing Initiative (ISI) as a comprehensive effort to develop and deploy modern information technology to accomplish the FBI's strategic goals and objectives over a five-year period. In February 2000, the FBI reduced the scope of the ISI to meet the most critical information technology infrastructure requirements, a project that was referred to as the eFBI. In September 2000, under the direction of a new Assistant Director, the FBI proposed the FBI Information Technology Upgrade Plan (FITUP) to meet the critical information technology infrastructure needs of the FBI in a manner that would provide new applications and the critically needed network and desktop computing needs in a faster, less costly manner. This plan, now known as TRILOGY, will be deployed over three years as a comprehensive effort to upgrade the FBI's user applications, transportation networks, and information presentation components.

V. Significant Endeavors by Mission Area

Today, there are hundreds of computer-based information systems in use within the Department. In addition, many more are in the planning or development stage. This section describes some noteworthy initiatives, categorized in the major topic headings of the DOJ Performance Plan and identified from the perspective of those mission headings.

Investigation and Prosecution of Criminal Offenses

DRUGX

The objectives of the DRUGX project are to create a user-friendly, fully integrated, compatible mechanism for sharing drug-related information between DEA and the FBI, and to improve the access to such information for other DOJ law enforcement agencies, including the USMS. DRUGX has been designed for eventual expansion to law enforcement agencies in other federal departments, in particular the U.S. Customs Service, on a reciprocal basis. Presently, this project involves an automated system for data sharing and investigative coordination between DEA and the FBI.

MERLIN

Project MERLIN provides DEA intelligence analysts with increased capabilities for intelligence support to its law enforcement operations. This effort is designed to give certain DEA offices advanced intelligence analyst workstations and the capability to transmit, access, and share classified data over a secure network. Project MERLIN takes advantage of the FIREBIRD infrastructure and supports both domestic and foreign intelligence needs.

MODEL 204 (M204)

The M204 database system is the standard DEA development tool for all investigative and administrative applications. It includes 60 core investigative and administrative applications that provide support for special agents, diversion investigators, and intelligence analysts.

CONCORDE

Project CONCORDE, a new DEA major system initiative, targets the development of a state-of-the-art application architecture that will provide real-time access to a comprehensive set of all mission-critical data now residing in the 21 year old M204 Corporate Database System. CONCORDE will provide users (special agents, intelligence analysts, diversion analysts, and administrative personnel) with the ability to exploit, with a single query, all information stored in M204's 60 different applications.
Casa De Web

The Casa De Web project will provide an enterprise web-based collection management and retrieval capability for all FBI field offices. Casa De Web will provide an interface between the FBI's electronic surveillance (ELSUR) central monitoring plant (CMP) in each field office and users connected to the field office's FBI LAN. Field offices will be interconnected with each other and with FBI Headquarters through the FBI's WAN as a part of the TRILOGY initiative to provide full enterprisewide access to ELSUR collected by any field office. The Casa De Web project and TRILOGY will work together to promote a seamless functional integration so that TRILOGY users with the proper privileges can easily access case-related ELSUR data.

National Integrated Ballistics Information Network (NIBIN)

On December 2, 1999, the FBI, DOJ, and the Department of Treasury entered into a Memorandum of Understanding (MOU) for the joint agency implementation of a single federal ballistics imaging system. This MOU phases out the DRUGFIRE automated computer technology developed by the FBI Laboratory. In its place the FBI will assist Treasury's Bureau of Alcohol, Tobacco and Firearms (ATF) in the development of the new National Integrated Ballistics Information Network (NIBIN). The new NIBIN system is combining the best features of ATF's Integrated Ballistics Identifications System (IBIS) and the FBI's DRUGFIRE system and will employ a common image format. The work accomplished by both agencies will ensure a coordinated vision and implementation plan for the NIBIN system. The FBI will provide the national network for the NIBIN system through the Criminal Justice Information Services (CJIS) Division wide-area network (WAN). ATF will then be responsible for the day-to-day operations of the NIBIN system. The transition to the NIBIN system is expected to be completed in late FY 2002.

Joint Automated Booking System (JABS)

JABS is a secure medium that enables the automation of the federal criminal booking process; allows law enforcement agencies to electronically share criminal data, thereby improving response times for criminal identification; and avoids duplication of booking data entry. Equally important, it provides a secure link for transmitting electronic fingerprint and biometric data to the FBI's Integrated Automated Fingerprint Identification System (IAFIS). JABS defines and maintains a repository of common offender data elements for identification of arrestees by participating law enforcement organizations. JABS eliminates repetitive booking of offenders, standardizes federal booking data elements, enables cross-agency sharing of booking information, enhances cooperation between law enforcement agencies, and reduces the threat to law enforcement officials and the public by facilitating the rapid and positive identification of offenders. Participants in the JABS project include the FBI, the Immigration and Naturalization Service, the Drug Enforcement Administration, the U. S. Marshals Service, the Bureau of Prisons, the Executive Office for United States Attorneys, and the Justice Management Division.

Assistance to State and Local Governments

Integrated Automated Fingerprint Identification System (IAFIS)

IAFIS was developed by the FBI for state-of-the-art fingerprint identification and criminal history data services. It has dramatically improved the fingerprint processing services that the FBI provides to 72,000 federal, state, and local law enforcement and criminal justice agencies. It uses new state-of-the-art technologies in image scanning, capture, and processing, plus large file data management. It became operational in 1999.

Automated Biometric Identification System/Integrated Automated Fingerprint Identification System (IDENT/IAFIS)

The IDENT/IAFIS project was established to integrate the INS Automated Biometric Identification System (IDENT) with the FBI's Integrated Automated Fingerprint Identification System (IAFIS), resulting in a single fingerprint identification system. The integration of the IDENT functionality into IAFIS will greatly benefit both INS and the FBI, as well as federal, state, and local law enforcement. The real-time connection with the FBI's IAFIS will provide INS with the ability to quickly determine if a person it apprehends is the subject of a currently posted Want/Warrant or has a prior criminal record. Similarly, law enforcement agencies will be able to receive all relevant immigration information as part of a criminal history response from a single FBI search request.

Combined DNA Index System (CODIS)

The DNA Identification Act, included in the 1994 Crime Bill, authorized the FBI to establish CODIS for law enforcement purposes. The FBI has developed CODIS to function as a national DNA system containing forensic and convicted offender indices. The forensic index contains DNA profiles derived from crime scene body fluid stains, and the convicted offender index contains DNA profiles of individuals convicted of violent crimes. CODIS enables state and local law enforcement crime laboratories to exchange and compare DNA profiles electronically, thereby linking serial crimes to each other and identifying suspects by matching DNA from crime scenes to criminal offenders. CODIS began as a pilot project in 1990, serving 14 state and local DNA laboratories. Currently, CODIS is installed in 110 laboratories in 44 states and the District of Columbia. The FBI provides CODIS software, together with installation, training, and user support, free of charge to any state and local law enforcement laboratories performing DNA analysis. Each state is responsible for purchasing commercial off-the-shelf hardware/software necessary to operate CODIS.

National Crime Information Center (NCIC) 2000

The FBI's NCIC, established in 1967, is a nationwide criminal justice information system that provides the criminal justice community with immediate access to certain kinds of law enforcement information, such as wanted persons, missing persons, stolen vehicles, and outstanding warrants. NCIC 2000 represents a significant improvement in capabilities. Among the many new functions of NCIC 2000 is the capability to transmit a fingerprint image between a law enforcement officer's patrol car and the NCIC 2000 central computer, where the fingerprint image will be searched against fingerprint images associated with wanted and missing persons. The officer rapidly receives the results of the search back to his/her location.

National Instant Criminal Background Check System (NICS)

NICS enforces the provisions of the Brady Handgun Violence Prevention Act. NICS supports the timely identification of individuals who are prohibited under the Act from possessing or receiving firearms. The system currently operates by telephonic voice inquiry for a file check. It is anticipated that NICS will transition to a Web-based on-line inquiry design.

National Drug Pointer Index System (NDPIX)

The NDPIX System, operated by DEA, provides participating federal, state, and local law enforcement agencies with an automated process for determining if a current drug investigative suspect is under active investigation by one or more other participating agencies. The system went operational in early 1998, with participation by DEA, FBI, the U. S. Customs Service, and a wide range of federal, state and local law enforcement agencies.

Legal Representation, Enforcement of Federal Laws, and Defense of U.S. Interests

Automated Litigation Support (ALS)

"Automated Litigation Support" refers to the wide range of contractor-provided services used by the Department's attorneys and their support staffs throughout the life of a case or project. The contractors perform such discovery activities as document imaging and indexing, and provide a wide range of other case-oriented services such as clerical support, paralegal research, database development, and document center creation and operation. ALS contracts enable the Department to respond efficiently to the fluctuations in the need for such resources, especially for large and complex cases. ALS is not an IT endeavor in the usual sense of IT, since IT is only one of many ALS aspects.

Case Management Systems

The Department*s litigating divisions, the United States Attorneys, and the United States Trustees have case management systems to track key information on litigation and other matters. Some components use the case management systems to record and track attorney time spent on particular matters. Each component has implemented its own system according to particular needs (i.e., data requirements) of the component. In general, the systems have data about the nature of a case, its filing date and litigation history, the court in which the case is brought, the identities of the parties and attorneys involved, and such elements as interrogatories, depositions, and witnesses. Some components are migrating to client-server commercial case-management software products.

Geographic Information Systems (GIS)

GIS technology enables attorneys and others to query and work with large data sets of demographic data and to perform requisite data analyses in a timely manner. Graphical representations of spatial data have proven to be effective investigative support tools and prosecutorial aids in presenting evidence to jurors. Such tools are used particularly in the activities of the Department's Civil Rights and Criminal Divisions.

Immigration

Automated Biometric Identification System (IDENT)

The IDENT system is a two-print biometric identification functionality that collects fingerprints and photographs and is linked to other information about an individual stored in the Enforcement Integrated Database (EID). The INS uses the IDENT capability to identify criminals and other removable aliens, as well as asylum applicants using different identities to obtain asylum benefits.

Central Index System (CIS)

The CIS serves as the INS-wide index to track the location of paper case files in file control offices, and maintain alien and other individuals of interest status information. This information is used by INS operational components, as well as by various federal and state entitlement programs, for enforcement and benefits operations.

Computer-Linked Application Information Management System (CLAIMS 3)

CLAIMS 3 was placed into service as a LAN-based system at each of INS's four service centers. The system is a major component of the INS Direct Mail Program, in which petitions and applications can be mailed to any one of the four service centers for data entry and in which the petitions and/or applications can be made ready to be adjudicated by an INS officer.

Computer-Linked Application Information Management System (CLAIMS 4)

CLAIMS 4 provides a current-technology IT platform to support INS benefits processing nationwide, starting with naturalization. This system incorporates all individual casework-oriented software subsystems that support the processing of naturalization applications. CLAIMS 4 provides for the recording of fees paid, data entry, application adjudication processing, interview and oath ceremony scheduling, the granting of benefits, the issuance of identification documentation, and reporting.

Enforcement Case Tracking System (ENFORCE)

The Enforcement Case Tracking System (ENFORCE) is a case management system for INS enforcement activities that integrates a wide range of booking case management and functional systems for arrest bookings. By automating manually intensive booking processes, ENFORCE streamlines business procedures and builds a knowledge base from which criminal activities can be analyzed to identify local and international criminal organizations involved in alien smuggling, document counterfeiting, and fraudulent immigration schemes. ENFORCE has the capability to interface and/or exchange data with systems external to INS (e.g., U.S. Customs Service inspection lookout systems, the Bureau of Prisons SENTRY system, state prison information systems, the Executive Office for Immigration Review information system, and the Department of State information systems). ENFORCE provides enforcement subject processing and performs statistical and management reporting for enforcement case management.

I-94 Automation

The Automated I-94 System was developed to automate the INS current manual process of obtaining arrival and departure information on non-immigrants. The system electronically records arrival and departure information on non-U.S. citizens traveling through selected airports of entry. It alleviates data-entry errors, improves the timeliness of data availability, and enhances the capability of matching arrival/departure records.

Integrated Card Production System (ICPS)

The ICPS was developed to provide a common platform for producing the Employment Authorization Document (EAD), the Permanent Resident Card (PRC) and the Laser Visa (LV). The ICPS includes both a platform and sophisticated printers capable of personalizing these INS issued cards, giving them a common, readily-recognized appearance. The ICPS personalizes cards from receipt of the electronic file through completion with minimal human intervention, enhancing the quality control and integrity of the process. Each ICPS unit operates as a very sophisticated network printer, using card order information that is transferred directly from INS case processing systems, with card production information then returned directly to those systems.

Integrated Surveillance Information System (ISIS)

ISIS is an integration of three separately identifiable subsystems, including Remote Video Surveillance (RVS), Integrated Computer Assisted Detection (ICAD III), and seismic, magnetic and thermal detection sensors. The ISIS program improves the ability of the INS and U.S. Border Patrol to secure the land borders, ports of entry, and coasts of the United States against illegal migration. The result of providing remote detection and tracking capabilities is increased deterrence of illegal border crossing by apprehending and removing those who attempt to or illegally enter and increased officer safety. ISIS also provides 24 hour per day all-weather coverage of the border.

Automated Nationwide System for Immigration Review (ANSIR)

The Executive Office for Immigration Review (EOIR) uses the ANSIR system to fully support its mission through case management, office automation, and legal research functions and resources. ANSIR encompasses all of EOIR's information resources (hardware, software, and data).

Detention and Incarceration

SENTRY

The SENTRY system is BOP's primary mission support system. There are more than 20,000 SENTRY terminals and printers located at BOP institutions, regional offices, and other government agencies throughout the United States. The SENTRY network provides for the processing of inmates at all phases of incarceration including admission, release, transfer, and furlough. SENTRY also includes many administrative subsystems such as e-mail and property management. SENTRY uses the Department's shared computing resources, including the Justice Data Center, JOIN, and JCN.

Automated Prisoner Scheduling System (APSS)

The USMS transports prisoners to fulfill judicial mandates to produce prisoners for court and to transport them to detention facilities. The APSS is the detainee scheduling system that allows the automation of the scheduling process for prisoner movement on trips that exceed 250 miles. This allows district and headquarters staff to track prisoners during transport, allowing the USMS to manage prisoner handling efficiently and from an aggregate level.

Justice Detainee Information System (JDIS)

The JDIS will integrate all USMS offender-based applications into one integrated application. The objective of the project is to integrate the functions of the Prisoner Tracking System (PTS), the Warrant Information Network (WIN), the Automated Prisoner Scheduling System (APSS), and the Partial Automated Booking Station (ABS), which will be compatible with the Department's Joint Automated Booking System (JABS).

Prisoner Tracking System (PTS)

The PTS supports the management of prisoners in USMS custody by allowing staff access to automated federal prisoner status information. PTS provides information on federal and non-federal prisoners. The system allows deputies to keep track of all prisoners that are received into custody and released to detention facilities.

Warrant Information Network (WIN)

The WIN system provides a centralized automated system for tracking fugitives and warrants, automating routine tasks, sharing interagency and interoffice information, and feeding critical offender-based data to higher level management and analytical systems. The WIN system tracks the number of incoming warrants, arrests, age of warrant, top 15 cases, international and domestic warrants, and type of warrant. WIN data also has criminal history information on the wanted individuals.

DOJ Component Information

The Department of Justice publishes information on 38 organizational entities – their missions, organizational structure, budgets and accomplishments – as well as overall departmental information, such as its strategic plan, accountability reports, inventory of commercial activities, and detailed information about contracting, including specific information technology procurement projects.

Much of this information is found directly on the Department's principal publication Web site at www.usdoj.gov. However, a considerable additional amount of component-specific information is published on component sites such as www.fbi.gov, www.ojp.usdoj.gov, www.bop.gov, and www.ins.usdoj.gov. Besides being quite thorough in themselves, these Department sites often include links to further information available from mission partners. All the component sites are linked to the main Department site at www.usdoj.gov, and persons seeking basic or overall information are encouraged to first visit the main site.

The information available on the Web sites and through their links is more comprehensive than the information offered in this IRM Overview booklet. The IRM Overview was prepared to give prospective suppliers and business partners an introduction to some of the IRM/IT aspects of the Department. Consequently, while the booklet merely highlights selected initiatives, the Web sites offer information on all the Department's major information systems. Persons who would like to learn about those systems will find their descriptions in the Freedom of Information Act (E-FOIA) Electronic Reading Rooms on the DOJ component Web pages.

We welcome comments on our publishing. Reactions and suggestions can be sent to the feedback links on the Department's Web pages or addressed to the persons identified in Appendices B and C of this booklet.

Justice Management Division
Information Resources Management

Janis A. Sposato
Acting Chief Information Officer
Acting Assistant Attorney General for Administration
Justice Management Division
Room 1744, Main Justice Building
950 Pennsylvania Avenue, NW
Washington, DC 20530
(202) 514-3101
Janis.Sposato@usdoj.gov

Linda D. Burek
Deputy Chief Information Officer
Deputy Assistant Attorney General
Information Resources Management
Justice Management Division
Room 1129, Main Justice Building
950 Pennsylvania Avenue, NW
Washington, DC 20530
(202) 514-0507
Linda.Burek@usdoj.gov

Michael D. Duffy, Director
Wireless Management Office Staff
Information Resources Management
Justice Management Division
12801 Fair Lakes Pkwy, Room 100
Centreville, VA 20120
(703) 322-1660
Michael.Duffy@usdoj.gov

Jim Gallagher, Director
Systems Engineering and Development Staff/
Systems Technology Staff
Information Resources Management
Justice Management Division
Room 4607, Patrick Henry Building
601 D St NW
Washington, DC 20530
(202) 514-3404
Jim.Gallagher@usdoj.gov

Michael D. Duffy, Director
Telecommunications Services Staff
Information Resources Management
Justice Management Division
Room 3029, Bicentennial Building
600 E St NW
Washington, DC 20530
(202) 514-1600
Michael.Duffy@usdoj.gov

Linda Burek, Acting Director
Information Management and Security Staff
Information Resources Management
Justice Management Division
Suite 1220, National Place Building
1331 Pennsylvania Avenue NW
Washington, DC 20530
(202) 514-4292
Linda.Burek@usdoj.gov

James E. Price, Director
Computer Services Staff
Information Resources Management
Justice Management Division
1151-D Seven Locks Rd, Room 205
Rockville, MD 20854
(202) 307-6900
James.E.Price@usdoj.gov

DOJ Information Resources Management
Component Chief Information Officers

Sheldon Adelberg
Director
Information Systems
United States Parole Commission
Room 440, PPB Building
5550 Friendship Blvd.
Chevy Chase, MD 20815
TEL: (301) 492-5980 FAX: (301) 492-6694
Internet: Sheldon.Adelberg@usdoj.gov

Carl Anderson
Chief, Information Systems Support Group
Antitrust Division
1110 Vermont Avenue, NW, Room 5007
Washington, DC 20005
TEL: (202) 633-1413 FAX: (202) 633-2528
Internet: Carl.Anderson@usdoj.gov

Zal Azmi
Chief Information Officer
Executive Office for U.S. Attorneys
Room 8009, Bicentennial Building
600 E Street, NW
Washington, DC 20530
TEL: (202) 616-6973 FAX: (202) 305-1706
Internet: Zal.Azmi2@usdoj.gov

George Bohlinger
Executive Associate Commissioner
Office of Management
Immigration and Naturalization Service
Room 7006, CAB Building
425 Eye St., NW
Washington, DC 20536
TEL: (202) 514-3182 FAX: (202) 514-8045
Internet: George.H.Bohlinger@usdoj.gov

David Bonski
Chief
Technical Services Division
National Drug Intelligence Center
319 Washington St., 5th Floor
Johnstown, PA 15907-1622
TEL: (814) 532-4795 FAX: (814) 532-4686
Internet: djb@cospo.osis.gov

Daryl Borgquist
Media Affairs Officer
Community Relations Service
Suite 6000, Bicentennial Building
600 E St., NW
Washington, DC 20530
TEL: (202) 305-2966 FAX: (202) 305-3009
Internet: Daryl.Borgquist@usdoj.gov

Sandra J. Bright
Acting Executive Officer
Office of Administration
Criminal Division
1331 F. St., NW, Room 700
Washington, DC 20530
TEL: (202) 514-5749 FAX: (202) 514-1792
Internet: SandieB@Coar.usdoj.gov

Robert Bruffy
Executive Officer
Environment and Natural Resources Division
801 PA Building, Suite 620
Washington, DC 20530
TEL: (202) 616-3091 FAX: (202) 616-3362
Internet: robert.bruffy@usdoj.gov

Linda D. Burek
Deputy Assistant Attorney General
Information Resources Management
Justice Management Division
Room 1129, Main Justice Building
950 Pennsylvania Avenue, NW
Washington, DC 20530
TEL: (202) 514-0507 FAX: (202) 514-1225
Internet: Linda.Burek@usdoj.gov
Alex Chiu

Acting Chief Information Officer
U.S. Marshals Service
600 Army Navy Drive
CS 3, 9th floor
Arlington, VA 22202
TEL: (202) 307-9386 FAX: (202) 353-8340
Internet: Alex.Chif@usdoj.gov

Henry Coffman
Information Resources Manager
United States National Central Bureau - INTERPOL
Room 600, Bicentennial Building
600 E St., NW
Washington, DC 20530
TEL: (202) 616-7984 FAX: (202) 616-8400/1357
Internet: Henry.Coffman@usdoj.gov

Bob Dies
Assistant Director
Information Resources Division
Federal Bureau of Investigation
Room 5829, JEH Building
935 Pennsylvania Avenue, NW
Washington, DC 20530
TEL: (202) 324-4507 FAX: (202) 324-1576
Internet: bobdies@fbi.gov

William Dziwura
Executive Officer
Office of the Pardon Attorney
500 First St., NW, 4th Floor
Washington, DC 20530
TEL: (202) 616-6070 FAX: (202) 616-6069
Internet: WilliamDf098c@COAR.usdoj.gov

DeDe Greene
Executive Officer
Civil Rights Division
Room 5058, NYAV Building
1425 New York Avenue, NW
Washington, DC 20530
TEL: (202) 514-4224 FAX: (202) 514-1783
Internet: DeDe.greene@usdoj.gov

John Hardwick

Deputy Assistant Director
Information Resources Management
Bureau of Prisons
Room 354, HOLC Building
320 First Street, NW
Washington, DC 20534
TEL: (202) 307-3065 FAX: (202) 307-1261
Internet: John.Hardwick@usdoj.gov

Scott O. Hastings
Associate Commissioner
Information Resources Management
Immigration and Naturalization Service
Room 700, Tech World
801 I Street, NW
Washington, DC 20536
TEL: (202) 514-2547 FAX: (202) 514-5761
Internet: S.Hastings@usdoj.gov

Dennis McCrary
Deputy Assistant Administrator
Office of Information Systems
Drug Enforcement Administration
600 Army Navy Drive, Suite E-3105
Arlington, VA 22202
TEL: 307-7454 FAX: 307-4684
Internet: dmccrary@dialup.usdoj.gov

Wendy Miller
Acting Assistant Director
Office of Administration
Community Oriented Policing Services
1100 Vermont Avenue, 10th Floor
Washington DC 20530
TEL: (202) 305-3853 FAX: (202) 616-2914
Internet: Wendy.Miller@usdoj.gov

Greg Peters
Deputy Assistant Inspector General
Office of the Inspector General
Room 7000, NYAV Building
1425 New York Avenue, NW
Washington, DC 20530
TEL: (202) 616-4558 FAX: (202) 616-9810
Internet: GregP3@COAR.usdoj.gov

Tom Phalen
Manager, MIS
Federal Prison Industries
5th Floor, ACACIA Building
320 First St., NW
Washington, DC 20530
TEL: (202) 305-3420 FAX: (202) 305-7252
Internet: Tphalen@central.unicor.gov

John R. Rich
Deputy Assistant Director
Information Resources Management
Executive Office for Immigration Review
5107 Leesburg Pike, Suite 2300
Falls Church, VA 22041
TEL: (703) 605-1327 FAX: (703) 305-1702
Internet: John.Rich@usdoj.gov

Gary Silver
Director of Administration
Office of Justice Programs
810 7th St., NW, Room 3423
Washington, DC 20001
TEL: (202) 307-0087 FAX: (202) 307-1020
Internet: GarySdeb89@COAR.usdoj.gov

Kathleen C. Smith
Office of Attorney Recruitment and Management
Room 6150, Main Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530
TEL: (202) 514-8905 FAX: (202) 514-0713
Internet: Kathleen.C.Smith@usdoj.gov

Larry Solomon
Deputy Director
National Institute of Corrections
500 First St., NW - 7th Floor
Washington, DC 20530
TEL: (202) 307-3106 - X155 FAX: (202) 307-3361
Internet: LarryB.S@COAR.usdoj.gov

Josephine Thomas
Executive Officer
Executive Office for U.S. Trustees
901 E. St., NW, Room 732
Washington, DC 20530
TEL: (202) 616-1113 FAX: (202) 307-3960
Internet: Josephine.Thomas@usdoj.gov

Joseph Young
Executive Officer
Tax Division
Suite 7100, PHB Building
601 D St., NW
Washington, DC 20004
TEL: (202) 616-0010 FAX: (202) 305-8897
Internet: JosephE.Y@COAR.usdoj.gov

Kenneth L. Zwick
Director
Office of Management Programs
Civil Division
Room 3140, Main Justice Building
950 Pennsylvania Avenue, NW
Washington, DC 20530
TEL: (202) 514-4552 FAX: (202) 514-8071
Internet: KenZ2@COAR.usdoj.gov