United States General Accounting Office

GAO

Report to Congressional Requesters

November 2002

INFORMATION TECHNOLOGY

Justice Plans to Improve Oversight of Agency Projects

GAO

Accountability ★ Integrity ★ Reliability

GAO
Accountability·Integrity·Reliability
Highlights

November 2002

INFORMATION TECHNOLOGY

Justice Plans to Improve Oversight of Agency Projects

Highlights of GAO-03-135, a report to the House Committee on the Judiciary and Subcommittee on Immigration, Border Security, and Claims

Why GAO Did This Study

To help carry out its mission to protect the public from criminal activity, the Department of Justice invests about $2 billion annually in information technology (IT). In particular, the Immigration and Naturalization Service (INS), a Justice agency, invested about $459 million in IT in fiscal year 2002. GAO was asked to determine, for key INS IT system investments, whether Justice's oversight has been effective, ensuring that these systems deliver promised capabilities and benefits on time and within budget.

What GAO Recommends

GAO recommends that Justice treat oversight of IT investments as a departmental priority, that it expeditiously plan and implement initiatives to introduce missing oversight controls and capabilities, and that INS adhere to existing life cycle and investment requirements to manage cost, schedule, capability, and expectations. Justice stated that it generally agreed with the substance of our report.

www.gao.gov/cgi-bin/getrpt?GAO-03-135

To view the full report, including the scope and methodology, click on the link above. For more information, contact Randolph C. Hite at (202) 512-3439 or hiter@gao.gov.

What GAO Found

Justice has not effectively overseen INS's investment in IT systems. A key indicator of oversight effectiveness is the quality of the process followed in conducting oversight. In this regard, successful public and private organizations ensure that such processes, at a minimum, provide for measuring progress against investment commitments—that is, project agreements defining what system capabilities and benefits will be delivered, by when, and at what cost. Justice does not yet have such an oversight process. Moreover, for four key INS IT investments that GAO was asked to review (see table), oversight activities that Justice has performed have not included measuring progress against approved cost, schedule, performance, and benefit commitments. As a result, Justice has not been positioned to take timely corrective action to address its component agencies' deviations from established investment commitments, and adequately ensure that promised capabilities are delivered on time and within budget. According to Justice officials, the department has not conducted this level of oversight because it has not given enough priority to the task, and because INS does not have the data that Justice would need to conduct such oversight.

Justice recognizes the need to strengthen its oversight of component agencies' IT investments, and has plans to do so. Among these is an initiative to develop steps and procedures for overseeing component agency IT investments so that they meet cost, schedule, and performance goals. However, these initiatives have not progressed to the point that the department has detailed plans governing what will be done and when it will be done. Moreover, the process improvements that these initiatives are intended to put in place must still be implemented and followed before they will produce real benefits.

INS Systems That GAO Was Asked to Review

System	Function
Automated I-94 System	Captured arrival and departure data at selected air ports of entry (system retired in February 2002 because it did not meet mission needs)
Enforcement Case Tracking System	Provides a standardized method to book an apprehended individual and sends data to a common database; is planned eventually to support all INS enforcement case processing and management functions
Automated Biometric Identification System	Screens aliens encountered by INS using biometric or other unique identification data and verifies and authenticates asylum benefit applicants; collects fingerprints, photographs, and biographical data and compares to data for previously apprehended aliens and aliens that have been previously deported or have a significant criminal history
Integrated Card Production System	Produces three types of cards: Employment Authorization Document, Permanent Resident Card ("Green Card"), and Laser Visa/Border Crossing Card (allowing Mexican nationals entrance into the United States)

Source: GAO analysis based on INS data.

Contents

Letter

Appendixes

Table

Figures

Abbreviations

CIO	Chief Information Officer
CLAIMS	Computer-Linked Application Information Management System
EID	Enforcement Integrated Database
ENFORCE	Enforcement Case Tracking System
FBI	Federal Bureau of Investigation
GAO	General Accounting Office
IAFIS	Integrated Automated Fingerprint Identification System
ICPS	Integrated Card Production System
IDENT	Automated Biometric Identification System
IG	Inspector General
INS	Immigration and Naturalization Service
IT	information technology
LAN	local area network
NPS	National Production Server
OMB	Office of Management and Budget
TCP/IP	Transmission Control Protocol/Internet Protocol
WAN	wide area network

United States General Accounting Office
Washington, D.C. 20548

November 22, 2002

The Honorable F. James Sensenbrenner, Jr.
Chairman, Committee on the Judiciary
House of Representatives

The Honorable John Conyers, Jr.
Ranking Minority Member, Committee on the Judiciary
House of Representatives

The Honorable George W. Gekas
Chairman, Subcommittee on Immigration, Border Security, and Claims
Committee on the Judiciary
House of Representatives

The Honorable Sheila Jackson Lee
Ranking Minority Member, Subcommittee on Immigration, Border Security, and Claims
Committee on the Judiciary
House of Representatives

The Department of Justice (Justice) and its subsidiary agencies play a key role in protecting the public from violence and criminal activity, such as drug smuggling and acts of terrorism. To execute this role, Justice and its agencies rely extensively on information technology (IT), investing about $2 billion annually in this area. The Immigration and Naturalization Service (INS), in particular, invested about $459 million in fiscal year 2002 to fulfill its part of Justice's mission. As the parent organization, Justice is responsible for overseeing its subsidiary agencies' investments in IT to ensure that they meet system commitments, including delivery of promised system capabilities and benefits on time and within budget.

As agreed with your offices, our objective was to determine whether Justice has exercised effective oversight of four key INS system investments. Our objective, scope, and methodology are discussed in detail in appendix I. The four systems are described in detail in the background section of this report and in appendix II.

Results in Brief

Justice has not effectively overseen INS's investment in IT systems, but improvements are planned. One indicator of oversight effectiveness is the quality of the oversight process followed, particularly whether the process provides for measuring progress against such commitments as what system capabilities and benefits will be delivered, by when, and at what cost. Justice does not yet have such an oversight process in place. Moreover, our analysis of four key INS projects showed that Justice oversight activities have not addressed such progress so that timely corrective action could be taken to address deviations from commitments. According to Justice officials, the department is not conducting such oversight because it has not given enough priority to the task, and because INS does not have the project data that would enable Justice to conduct effective oversight. As a result, Justice has allowed INS—an agency that we and the Justice Inspector General (IG) have reported to be challenged in managing IT—to largely go unchecked in its attempts to leverage IT to improve mission performance.

Justice's new Chief Information Officer (CIO) agreed with our assessment of the department's oversight process and its application, and has launched initiatives to strengthen oversight of Justice agency IT investments. However, detailed plans defining these initiatives and their implementation have not yet been developed. Accordingly, we are making recommendations to the Attorney General to help ensure that needed improvements are properly implemented.

In written comments on a draft of this report, Justice stated that it generally agreed with the substance of our report. Justice also provided minor comments that have been incorporated as appropriate throughout this report.

Background

Justice is headed by the Attorney General of the United States. Along with INS, which controls the border and provides services to lawful immigrants, Justice's other major components include the U.S. attorneys, who prosecute federal offenders and represent the United States in court; the Federal Bureau of Investigation (FBI) and the Drug Enforcement Administration, which gather intelligence, investigate crimes, and arrest criminal suspects; the U.S. Marshals Service, which protects the federal judiciary, apprehends fugitives, and detains persons in federal custody; the Bureau of Prisons, which confines convicted offenders; and the Office of Justice Programs and the Office of Community Oriented Policing Services, which provide grants and other assistance to state and local governments and community groups to support criminal and juvenile justice improvements.

To fulfill its diverse missions, the department employs more than 130,000 persons located across the country and overseas. Its field locations range from one- or two-person Border Patrol stations in sparsely populated regions to large offices in major metropolitan cities.

IT plays a vital role in Justice's ability to fulfill its missions, including its important role in protecting Americans against the threat of terrorism. For example, Justice reports that it has about 250 IT systems, ranging from asset control and financial management systems to automated fingerprint identification and criminal case management systems. In fiscal year 2002, Justice reportedly invested about $2.1 billion in IT, and it plans to invest about the same amount in fiscal year 2003.

IT management responsibility within Justice is vested with the CIO. The CIO's responsibilities include overseeing the department's IT investments, with particular focus on major systems[1] and investments that span more than one Justice bureau. The CIO is also responsible for overseeing the IT investments and IT management processes of Justice component agencies, such as INS.

INS: A Brief Description

The mission of INS is twofold: immigration enforcement (enforcing laws regarding illegal immigration) and immigration services (providing immigration and naturalization services for aliens who enter and reside legally in the United States). INS's enforcement mission includes conducting inspections of persons entering the United States, detecting and preventing smuggling and illegal entry, and identifying and removing illegal entrants. INS's immigration mission includes granting legal permanent residence status, nonimmigrant status (e.g., students and tourists), and naturalization.

IT plays a significant role in INS's ability to carry out its responsibilities. Examples of key IT systems that were the focus of our review are described in the next section. Other examples include the Deportable Alien

[1] Justice defines major systems as (1) systems with an annual cost of greater than $10 million, or total life-cycle cost of greater than $50 million; (2) any financial information system with an annual cost of greater than $500,000; (3) any investment that is mandated for use departmentwide; (4) any investment that has significant multiple-component impact; (5) any investment required by law or designated by Congress as a "line item;" and (6) any investment that due to the high risk or political sensitivity, as determined by the Justice CIO, warrants special consideration.

Control System, which is intended to automate many of the functions associated with tracking the location and status of illegal aliens in removal proceedings, including detention status; the Integrated Surveillance Intelligence System, which is to provide “24-7” border coverage through ground-based sensors, fixed cameras, and computer-aided detection capabilities; and the Computer-Linked Application Information Management System 4, which is a centralized case management tracking system intended to support a variety of tasks associated with processing and adjudicating naturalization benefits. INS’s IT portfolio includes 107 systems, including 11 major systems. In fiscal years 2001 and 2002, respectively, INS reportedly invested about $297 million and $459 million in IT-related activities, and in fiscal year 2003, it plans to invest about $494 million.

Key INS Systems: A Brief Description

Four of INS’s 107 key systems are the Automated I-94 System, the Enforcement Case Tracking System, the Automated Biometric Identification System, and the Integrated Card Production System. Each of these systems has been in development and/or operation and maintenance for at least the last 5 years. INS reported that it has invested about $207 million through fiscal year 2001 in these systems. Each of these systems has an estimated total life-cycle cost exceeding $50 million, and they are therefore considered major investments, according to Justice guidance.

Below is a brief description of each system. Appendix II describes the technical architectures for the Enforcement Case Tracking System, the Automated Biometric Identification System, and the Integrated Card Production System (we do not include the architecture for the Automated I-94 System because it has recently been retired).

Automated I-94 System

The I-94 is the paper form that INS uses to capture nonimmigrant data at air, land, or sea ports of entry.[2] In 1995, INS began automating its I-94

[2] Form I-94 is the arrival/departure record that is completed for nonimmigrants entering and leaving the United States (nonimmigrants from Mexico and Canada are not required to submit a form I-94). The form contains biographical information. When a nonimmigrant enters the United States, the INS inspector provides the nonimmigrant the departure portion of the form and sends the arrival portion to a contractor, who enters the data into the Nonimmigrant Information System (an on-line, automated, central repository of information designed to track and maintain the status of all foreign visitors and immigrants). Upon departure, the nonimmigrant provides the departure portion of the I-94 form, and the forms are collected and provided to the contractor for entry into the same system.

process to address concerns about the reliability of the data collected on this form. About this same time, Congress passed the Illegal Immigration Reform and Immigrant Responsibility Act of 1996,[3] which directed the Attorney General to develop an automated entry/exit control system to collect records of arrival and departure from every alien entering and leaving the United States. Because the main source of information on individuals entering and leaving the United States was the Form I-94, INS planned to meet the 1996 act's requirements with the Automated I-94 System.[4]

INS introduced the Automated I-94 System in 1997 as a pilot at the Philadelphia international airport and later at the Pittsburgh, Charlotte, and St. Louis international airports. It captured Form I-94 arrival and departure data electronically at these airports and transmitted them to INS's Nonimmigrant Information System.[5] INS planned to implement the Automated I-94 System at 17 airports in fiscal year 2002 and 18 additional airports in fiscal year 2003. INS also planned to eventually deploy the system to all air, land, and sea ports of entry.

However, in August 2001, the Justice IG concluded that INS had not adequately managed the Automated I-94 project and did not know if the system was meeting its intended goals.[6] The IG reported that INS had not (1) established measurable objectives to determine whether the system is achieving its goals, (2) established baseline data against which to measure progress, or (3) developed a cost-benefit analysis to know if investment in the system was justified. Subsequently, INS concluded that the Automated I-94 System did not effectively meet its current mission needs, and it retired

[3] Section 110 of Pub. Law No. 104-208, which has been amended and is codified as 8 U.S.C. 1365a.

[4] Section 1365a requires INS to implement an entry/exit control system using all available data that are currently collected to account for immigrants and nonimmigrants entering the country at ports of entry and to account for them when they depart. The overall goal of this act is to ensure that all alien arrival and departure data are available to immigration officers at all ports of entry by December 31, 2005.

[5] The Nonimmigrant Information System is an on-line, automated, central repository of information designed to track and maintain the status of all foreign visitors and immigrants.

[6] Office of the Inspector General, Department of Justice, *The Immigration and Naturalization Service's Automated I-94 System*, Report No. 01-18 (Aug. 6, 2001).

the system in February 2002.[7] According to INS, it had invested about $31.4 million in the Automated I-94 System through February 2002, including $200,000 to retire it.

Enforcement Case Tracking System

The Enforcement Case Tracking System (ENFORCE) currently consists of a single module, the ENFORCE Apprehension Booking Module, which supports INS's apprehension and booking process for illegal aliens. This module is supported by the Enforcement Integrated Database, which also stores biometric data obtained through the Automated Biometric Identification System (discussed below).

ENFORCE is intended to be an integrated system that supports all INS enforcement case processing and management functions. INS plans to use it to manage data on individuals, entities, and investigative cases, and to support enforcement case processing. INS plans provide for three additional modules, which are also to be supported by the Enforcement Integrated Database. Table 1 summarizes these ENFORCE components.

[7] At the time the system was retired, it was operational on U.S. Airways European flights at Philadelphia, Pittsburgh, and Charlotte and on TWA London service at St. Louis.

Table 1: Summary of Function and Status of ENFORCE Modules

Component	Function	Status
Modules		
Apprehension Booking Module	Provide a standardized method to book an apprehended individual	Operational
Removals Module	Support removal efforts, including detention, removal casework, and transportation	Development
Investigations Case Management and Intelligence Module	Support the investigative reporting capability and facilitate the collection, organization, and analysis of intelligence and investigative data	Development
Inspections Port-of-Entry Processing Module	Support all enforcement case processing and management functions of the Office of Inspections	Not yet started
Database		
Enforcement Integrated Database	Serve as a central data repository for INS enforcement systems, including the Enforcement Case Tracking System and the Automated Biometric Identification System	Operational

Source: GAO analysis based on INS data.

ENFORCE is also to interface to non-INS databases, such as the FBI's National Crime Information Center and other external sources of intelligence information. It may also interface with other INS databases, such as the National Automated Inspections Lookout System[8] and INS benefit systems, such as the Computer-Linked Application Information Management System[9] and the Refugee, Asylum, and Parole System.[10]

[8] The National Automated Inspections Lookout System contains approximately 1.2 million lookout records and is used by INS to determine a traveler's admissibility to the United States.

[9] The Computer-Linked Application Information Management System is a distributed transaction-based system designed to (1) support high-volume processing of applications and petitions received by the INS, (2) capture fees and provide fund control for all monies received via the application/petition process, (3) provide case status to applicants/petitioners, and (4) support and record the results of the adjudication of each application/petition.

[10] The Refuge, Asylum, and Parole System is intended to support the tracking and processing of asylum applications filed with the INS.

According to INS, it has invested about $47 million in ENFORCE through fiscal year 2001.

Automated Biometric Identification System

The Automated Biometric Identification System (IDENT) is a biometric identification system designed to quickly screen aliens encountered by INS using biometric or other unique identification data and to verify and authenticate asylum benefit applicants. IDENT collects two fingerprints, a photograph, and biographical data on aliens and compares these fingerprints to two databases. These databases include (1) a "lookout" database that contains fingerprints and photographs of aliens who have been previously deported by INS or who have a significant criminal history and (2) a recidivist database that contains fingerprints and photographs of over a million illegal aliens who have been apprehended by INS. IDENT can be deployed as a stand-alone system or it can be deployed along with the ENFORCE system (discussed above) to provide biometric identification support for INS enforcement activities.

IDENT was deployed in 1994 and is presently operational (about 1,908 IDENT and IDENT/ENFORCE workstations are currently deployed at border patrol locations, ports of entry, district offices, and asylum offices). According to INS, it has invested about $103 million in IDENT through fiscal year 2001.

INS currently is investing in two major IDENT initiatives. The first is the IDENT/IAFIS program, a major Justice initiative, intended to integrate IDENT data and capabilities into the FBI's Integrated Automated Fingerprint Identification System (IAFIS). IAFIS is an automated 10-fingerprint matching system based on rolled fingerprints, whereas IDENT collects sets of 2 flat pressed prints.[11] IAFIS contains criminal histories of over 42 million arrestees and a database of digitized fingerprint images from people in its Criminal Master File. It accepts both electronic and paper card submissions from INS, representing criminal and civil subjects. According to INS, Justice has invested about $12 million in the IDENT/IAFIS integration through fiscal year 2001.

The second initiative is the Information Technology Dissemination Plan, which is an initiative to train INS personnel on the operational use of the ENFORCE/IDENT systems and to coordinate the deployment of the IDENT

[11] IAFIS requires 10 rolled fingerprints to support matching of latent fingerprints found at crime scenes.

equipment with the delivery of the training.[12] According to INS, it has invested about $5 million in the plan in fiscal year 2002.

Integrated Card Production System

The Integrated Card Production System (ICPS) produces three types of cards: the Employment Authorization Document, which proves that a person is allowed to work in the United States; the Permanent Resident Card, commonly known as a Green Card, which documents a person's status as a lawful permanent resident with a right to live and work permanently in the United States; and the Laser Visa/Border Crossing Card,[13] which allows certain Mexican nationals entrance into the United States.

Requests for production of these cards are processed and routed to one of six ICPS printer devices[14] operating at three different sites in the United States (in Kentucky, Nebraska, and Vermont).[15] In fiscal year 2000, INS augmented its employment authorization card production capability by contracting for servicing from a private firm at the Kentucky site.

The ICPS equipment was acquired in 1996, and the system was deployed in 1998. According to INS, it has invested $25 million in ICPS through fiscal year 2001.

Previous Reviews of INS Show That It Has Been Challenged in Managing IT Investments

We and the Justice IG have issued a series of reports citing deficiencies in INS's IT management and performance. For example, in August 2000, we reported that INS did not have an enterprise architecture[16] to manage its IT efforts effectively and efficiently or the fundamental management structures and processes needed to effectively develop one, and we made

[12] This plan was developed in response to several Justice IG recommendations to improve the operation of IDENT and the training and education associated with IDENT and its uses.

[13] INS began producing the Laser Visa in April 1998 to replace the Border Crossing Card.

[14] Five of these printers can print any of the three types of cards. The sixth printer can only print the Employment Authorization Card.

[15] The Kentucky site houses four ICPS printer devices, and the Nebraska and Vermont sites each house one ICPS printer device.

[16] An enterprise architecture is an institutional systems blueprint that defines in both business and technological terms the organization's current and target operating environments and provides a roadmap for moving from one to the other.

recommendations to address these weaknesses.[17] Since then, INS has made progress implementing our recommendations. For example, it has established architecture management structures, it has drafted architecture products detailing both its current and its target architectures, and it has plans for completing and using these products. In December 2000, we also reported that INS lacked defined and disciplined processes to select, control, and evaluate its IT investments, and as a result, it did not know whether these investments would produce value commensurate with costs and risks or whether each investment was meeting its cost, schedule, and performance commitments.[18] To address these weaknesses, we made a series of recommendations, and INS has since taken steps to implement them. For example, it has (1) developed policies and procedures for implementing its investment management process and (2) established selection criteria for assessing the relative merits of each IT investment that address cost, schedule, benefits, and risk.

In addition, the Justice IG reported in July 1999 that estimated completion dates for some IT projects had been delayed without explanation, project costs had increased with no justification for how funds are spent, and projects were nearing completion with no assurance that they would meet performance and functional requirements.[19] Further, in March 2000, the IG reported on weaknesses in the design and implementation of INS's IDENT system, including that IDENT was not linked with other INS or criminal databases (such as the FBI's IAFIS database) and that INS had failed to effectively train INS personnel on using IDENT. [20] Since then, INS has been working with the FBI to integrate IDENT and IAFIS, and to coordinate the deployment of the IDENT equipment with the delivery of user training. Later, in August 2001, the IG reported that although INS had spent $31.2 million to develop and deploy the Automated I-94 System, INS had not

[17] U.S. General Accounting Office, *Information Technology: INS Needs to Better Manage the Development of Its Enterprise Architecture*, GAO/AIMD-00-212 (Washington, D.C.: Aug. 1, 2000).

[18] U.S. General Accounting Office, *Information Technology: INS Needs to Strengthen Its IT Investment Management Capability*, GAO-01-146 (Washington, D.C.: Dec. 29, 2000).

[19] Office of the Inspector General, Department of Justice, *Follow-up Review: Immigration and Naturalization Service Management of Automation Programs*, Audit Report 99-19 (July 1999).

[20] Office of the Inspector General, Department of Justice, *The Rafael Resendez-Ramirez Case: A Review of INS's Actions and the Operation of Its IDENT Automated Fingerprint Identification System*, Special Report (Mar. 20, 2000).

(1) established measurable objectives to determine whether the system is achieving its goals, (2) established baseline data against which to measure progress, or (3) developed a cost-benefit analysis to justify investment in the system.[21]

Justice Has Not Effectively Overseen INS's IT Projects, but Improvements Are Planned

According to federal requirements and guidance,[22] departments are responsible for ensuring that IT investments are being implemented at acceptable costs and within reasonable and expected time frames and that they are contributing to observable improvements in mission performance. While such departmental oversight is vital for all component agency IT investments, it is particularly important for agencies that have been challenged in their ability to manage these investments. However, Justice has not established an effective process for overseeing its component agency IT investments, and for the four key INS system investments that we reviewed, it has not ensured that INS satisfied approved cost, schedule, and performance investment commitments. According to Justice officials, doing so has not been a high enough priority to warrant allocation of the necessary oversight resources. Further, Justice officials stated that INS has not consistently been able to provide the project data necessary to effectively measure investments' progress. Unless it can measure its component agencies' progress against project commitments and take appropriate actions to address significant deviations, Justice increases the risk of investing millions of dollars in IT projects that do not perform as intended, improve mission performance, or meet cost and schedule goals. Justice recognizes this and has plans to strengthen oversight of its subsidiary agencies' IT investments.

Justice Does Not Have an Effective Process in Place for Overseeing Agency IT Investments

Congress and the Office of Management and Budget (OMB) recognize the need for federal agencies to implement effective oversight processes to help ensure that IT investments meet expected cost, schedule, and performance commitments. Together, the Clinger-Cohen Act of 1996 and OMB Circular A-130 require that federal departments establish oversight

[21] Office of the Inspector General, Department of Justice, *The Immigration and Naturalization Service's Automated I-94 System*, Report No. 01-18 (Aug. 6, 2001).

[22] Clinger-Cohen Act of 1996, Public Law 104-106, and Office of Management and Budget Circular A-130, *Management of Federal Information Resources* (Washington, D. C.: Nov. 30, 2000).

processes to periodically review and monitor actual performance against expected cost, schedule, and performance commitments. Such processes provide visibility into the investments' actual progress and allow management to take appropriate actions when performance deviates significantly from the approved commitments.

Leading private and public sector organizations' IT investment oversight processes generally include, among other things, (1) a written policy that establishes the organization's commitment to monitoring performance against approved commitments and taking corrective actions when actual performance deviates significantly from these commitments; (2) clearly defined roles and responsibilities for implementing the policy; (3) documented procedures defining the process steps and controls for implementing the policy; (4) adequate resources (e.g., skills, training, funding, and tools) for implementing the detailed process; and (5) established measures to ensure adherence to the process and to identify opportunities for improving it.[23]

Justice has satisfied two of these five elements of an effective oversight process. First, Justice has issued policies addressing its commitment to monitoring performance against approved commitments. Second, Justice has defined high-level roles and responsibilities for doing so. Specifically, Justice's Information Resources Management policy, dated March 2001, requires the CIO to perform oversight of components' IT investments through the annual budget process, technical assessments, and regularly scheduled component briefings of IT investments. In addition, Justice's IT investment management process guide,[24] dated August 2001, states that the CIO and staff are responsible for monitoring components' major IT investments, and requires that Justice components report, on a quarterly basis, progress against approved investment baselines (technical, cost, and schedule), including deviations from established cost and schedule commitments of 10 percent or greater.

[23] See, for example, U.S. General Accounting Office, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity* (Exposure Draft), GAO/AIMD-10.1.23 (Washington D.C., May 2000), and Carnegie Mellon Software Engineering Institute, *Software Capability Maturity Model (SW/CMM^{SM})*, Version 1.1 (1993), and *Capability Maturity Model Integrated for Systems Engineering/Software Engineering/Integrated Product and Process Development (CMMI^{SM})*, Version 1.02 (November 2000).

[24] Department of Justice, *Guide to the DOJ Information Technology Investment Management Process*, Version 1.1 (August 2001).

However, Justice has not yet (1) established specific procedures and controls for implementing its policies or (2) allocated human capital (both in terms of numbers or expertise) for overseeing components' IT investments. For example, Justice officials stated that only one staff member is dedicated to overseeing INS's IT investment portfolio, which includes 107 IT systems, and this staff member also oversees other Justice components' IT investments. Additionally, since Justice has not established oversight procedures, it has also not established measures to assess the performance of its oversight process and identify potential improvements, another key element of effective oversight practiced by successful organizations.

Without an effective process for overseeing its component agency IT investments, Justice is not positioned to exercise effective oversight, and thus is limited in its ability to take timely action and reduce the chances that these investments do not perform as intended and cost more and take longer than planned.

Justice Has Not Effectively Overseen Key INS Systems

Justice and INS guidance states that baseline cost, schedule, performance, and benefit commitments should be developed, documented, and kept current and that progress against these commitments should be measured.[25] This guidance is consistent with the elements of effective oversight practiced by successful organizations. In effect, Justice and INS recognize that baseline investment information is vital to Justice's ability to oversee progress and performance in delivering promised system capabilities and value, on time and within budget.

For the four key IT investments that we reviewed, Justice has not followed its own guidance and measured progress against approved cost, schedule, performance, and benefit commitments. Furthermore, Justice officials stated that their current oversight activities are not focused on monitoring such progress. Rather, these officials described their oversight of INS's IT investments as consisting of (1) reviewing INS's annual IT budget submissions, (2) reviewing INS's annual budget submissions for its major

[25] Department of Justice, *Systems Development Life Cycle Guidance Document* (March 2000); Immigration and Naturalization Service, *Systems Development Life Cycle Manual*, Version 6.0 (Nov. 13, 2001).

systems, (3) attending INS's Executive Steering Committee[26] meetings, (4) holding ad hoc meetings with INS project staff, and (5) conducting quarterly reviews of the progress in executing approved annual budget allocations. According to these officials, these oversight activities do not address progress against project commitments, such as delivery of expected benefits and promised system functionality and performance. Our review of available Justice documentation associated with these oversight activities confirmed this, including our review of quarterly progress reports and progress review minutes.

According to Justice officials, they do not monitor the progress of INS IT investments against project commitments because doing so has not been a high enough priority to justify adequate oversight resources and because INS does not have up-to-date baseline and project data available to permit such oversight.

We confirmed that INS does not have the kind of meaningful project data that would allow the measurement of progress against commitments. For the four IT investments, INS could not provide us with information needed to measure the progress of the four INS investments against commitments, such as projects plans with current baseline cost and schedule data, current cost/benefit analyses, and reports measuring progress against current baseline cost and schedule data and against expected benefits. According to INS officials who are responsible for ensuring that IT investments meet their commitments, INS has not monitored IT investments' progress against established baseline commitments for cost, schedule, performance, and benefits. Our review of available project documentation verified this, showing that INS did not maintain complete and updated baseline cost and schedule data for the systems that we reviewed. In the case of IDENT, for example, INS did not update the project plan or cost/benefit analyses to reflect significant project scope changes that materially affected the project's cost, schedule, performance, and benefits, such as not implementing IDENT at its Forensic Document Lab and Law Enforcement Support Center or integrating IDENT with certain

[26] This committee was established to ensure that INS IT investments are selected, evaluated, and controlled appropriately and follow the IT investment management processes approved by Justice's Investment Approval Board. The committee consists of the following INS officials: portfolio managers, a representative from both the Office of Budget and the Office of Policy and Planning, and the Director, Office of Strategic Information and Technology Development.

existing systems.[27] Similarly, in the case of the Automated I-94 System, the Justice IG reported that INS had not developed a project plan with cost and schedule data, and it had not established (1) measurable objectives to determine whether the system was meeting performance goals and (2) baseline data against which to measure progress.[28]

Justice Has Plans for Strengthening Its IT Oversight, but Much Work Remains

Justice's new CIO stated that his recent assessment of Justice's oversight activities is consistent with ours and he recognizes the need to improve IT oversight of all components, including INS. To this end, the CIO has outlined several strategic initiatives designed to strengthen the department's management and oversight of its IT investments. Specifically, Justice intends to (1) develop process steps and procedures for managing investments in departmentwide IT projects; (2) implement a tool to improve its collection and oversight of component agency budget information and assist in overseeing these agencies' IT investments; (3) develop a process to support the department in overseeing component agency IT investments so that they meet cost, schedule, and performance goals; and (4) identify and assess the skills, staffing, and other resources needed to conduct this oversight, among other things. These initiatives, if properly executed, could address the previously described three missing elements in Justice's oversight process. However, these initiatives are currently goals and objectives rather than well-defined projects that are under way and being guided by detailed plans with measurable outputs and milestones. Moreover, assuming that these process changes are developed, they still need to be effectively implemented before needed oversight improvements, and the associated benefits, can be realized.

Conclusions

Justice cannot effectively oversee what it cannot measure. In the case of INS's IT investments, meaningful progress measurement has not occurred, and the result has been limited success in leveraging IT to improve mission performance and accountability. To Justice's credit, it recognizes that it

[27] The plan called for IDENT to be integrated with the Refuge, Asylum, and Parole System, the Computer Linked Application Information Management System, the INS Passenger Accelerated Service System, Justice's National Crime Information Center System, and the Integrated Automated Fingerprint Identification System.

[28] Office of the Inspector General, Department of Justice, *The Immigration and Naturalization Service's Automated I-94 System*, Report No. 01-18 (Aug. 6, 2001).

needs to strengthen its oversight of the IT investments made by its component agencies. To this end, it has initiatives planned that, if properly implemented, will go a long way to strengthen its oversight practices. A key to success in doing so will be for Justice leadership to treat IT investment oversight as a management priority and allocate sufficient resources to its performance. Given the department's plans for investing heavily in IT, it is extremely important for Justice to ensure that establishing missing oversight controls and capabilities is treated as a priority, and that these are implemented effectively.

Recommendations for Executive Action

To strengthen Justice's oversight of its component agency IT investments, we recommend that the Attorney General direct the Justice CIO to ensure that oversight of IT investments is treated as a departmental priority, that initiatives intended to introduce missing oversight controls and capabilities are expeditiously planned and implemented, and that significant deviations from these oversight improvement initiative plans be reported to the Attorney General. Additionally, we recommend that the Attorney General direct the CIO to ensure that the oversight improvement initiatives provide for addressing the missing controls and capabilities discussed in this report, including

- having process steps and procedures for implementing the policy;
- devoting adequate resources (e.g., skills, training, funding, and tools) for implementing the process; and
- measuring process implementation and performance and identifying and implementing potential improvements.

Further, in order to ensure that INS develops and collects the requisite data needed to measure IT project progress and performance and to perform departmental oversight, we recommend that the Attorney General direct the Commissioner of INS to ensure that INS adheres to existing agency system life cycle and investment requirements governing management of system cost, schedule, capability, and benefit parameters and expectations.

Agency Comments and Our Evaluation

In written comments on a draft of this report, Justice stated that it generally agreed with the substance of our report. Justice also mentioned its CIO's initiatives to improve Justice's oversight of its information technology projects, which are described in our draft report. In addition, Justice noted that INS is currently improving its processes and documentation related to baseline cost and schedule data, and it provided what it characterized as minor, technical comments, which are incorporated as appropriate throughout this report.

We are sending copies of this report to the Chairmen and Ranking Minority Members of the Senate Committee on the Judiciary; the Subcommittee on Immigration; the Senate Committee on Appropriations; the Subcommittee on Commerce, Justice, State, and the Judiciary; the House Committee on Appropriations; and the Subcommittee on Commerce, Justice, State, and Judiciary. We are also sending copies to the Attorney General, the Commissioner of the Immigration and Naturalization Service, and the Director of the Office of Management and Budget. Copies will be made available to others on request. In addition, this report will be available at no charge on our Web site at http://www.gao.gov.

Should you or your staff have any questions on matters discussed in this report, please contact me at (202) 512-3439. I can also be reached by E-mail at HiteR@gao.gov. Key contributors to this report were Michael Alexander, Barbara Collier, Deborah Davis, Neil Doherty, Neha Harnal, and Richard Hung.

Randolph C. Hite

Randolph C. Hite
Director, Information Technology Architecture
and Systems Issues

Objective, Scope, and Methodology

Our objective was to determine whether the Department of Justice (Justice) has effectively overseen four key Immigration and Naturalization Service (INS) information technology (IT) investments: the Automated I-94 System, the Enforcement Case Tracking System, the Automated Biometric Identification System, and the Integrated Card Production System. To address our objective, we evaluated Justice's process for overseeing INS's IT investments, determined adjustments Justice has made to its process in the last 2 years and its plans to improve the process, and assessed Justice's application of its established process in overseeing each of the above systems.

To evaluate Justice's process for overseeing INS's IT investments, we first analyzed relevant federal laws and guidance[29] and leading public and private sector practices on IT management and oversight.[30] Next, we assessed documentation on the process, procedures, and practices Justice used to oversee each of the four systems. To determine what INS project oversight data are reviewed and how oversight decisions are made, documented, and communicated to INS, we interviewed Justice officials, including officials of the Justice Management Division's Information Management Security Staff and Budget Staff. We then compared Justice oversight process, policies, procedures, and practices with the federal laws, guidance, and leading practices, and we discussed any variances with cognizant Justice officials, including the Chief Information Officer.

To determine what adjustments Justice has made to its oversight process for the last 2 years and its plans for further changes, we obtained and reviewed documentation addressing changes to Justice's oversight process. We also discussed with Justice officials the changes and plans for changes to Justice's oversight process, the reasons for changes, and how changes will improve Justice's oversight.

[29] Clinger-Cohen Act of 1996, Public Law 104-106; Office of Management and Budget Circular A-130, *Management of Federal Information Resources* (Washington, D.C.: Nov. 30, 2000).

[30] See, for example, U.S. General Accounting Office, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity* (Exposure Draft), GAO/AIMD-10.1.23 (Washington D.C., May 2000), and Carnegie Mellon Software Engineering Institute, *Software Capability Maturity Model (SW/CMM^{SM})*, Version 1.1 (1993), and *Capability Maturity Model Integrated for Systems Engineering/Software Engineering/Integrated Product and Process Development (CMMI^{SM})*, Version 1.02 (November 2000).

To determine whether Justice has followed its established process in overseeing the four systems, we first analyzed description and status data on each of them, including hardware platform elements (e.g., computers, servers, network connectivity, and communications) and software platform elements (e.g., operating system, database, and applications). We then obtained and reviewed Justice oversight documentation, including management decisions, annual IT budget submissions, budget submissions to the Office of Management and Budget and associated review comments, quarterly reviews, meeting minutes addressing Justice involvement with project activities, documentation on issues/concerns raised, and actions taken for each of the four systems. We also interviewed Justice Management Division officials to discuss the extent to which Justice follows its oversight process.

We also determined the status of the four systems, including how INS measures progress against approved baseline cost, schedule, and performance commitments. To do so, we obtained and reviewed project data, such as project justification documents, project plans, requirements documentation, cost and benefit analyses, budget submissions, quarterly reports, status reports, and project meeting minutes. We also interviewed various INS officials involved with the projects, including portfolio managers, project mangers, and Information Resources Management staff to determine reported cost, schedule, and performance status information. To meet our reporting time frames, we were not able to independently verify reported status information in all cases. In cases where status information was not available or variances were found, we interviewed INS officials responsible for the project and Justice officials responsible for overseeing the projects.

We conducted our work at Justice and INS headquarters in Washington, D.C., from March through September 2002 in accordance with generally accepted government auditing standards.

Architectural Descriptions for Three Key Systems

We provide here architectural descriptions for the Enforcement Case Tracking System (ENFORCE), the Automated Biometric Identification System (IDENT), and the Integrated Card Production System (ICPS) (we do not include the architecture for the Automated I-94 System because it has recently been retired). These descriptions are based on INS-provided data and are technical in nature.

ENFORCE System Architecture

ENFORCE, which is envisioned to eventually include four modules, currently consists of one module, the Enforce Apprehension Booking Module (EABM), as well as the Enforcement Integrated Database (EID).

- EABM supports the apprehension and booking process for illegal aliens; the data that it collects are maintained in EID.
- EID is the common database repository for several INS enforcement systems, including ENFORCE and IDENT; it defines all data elements that must be recorded during INS enforcement processing, and stores and manages these data.

ENFORCE also receives biometric data (such as fingerprints and photographs) from the IDENT system (described next); these data are linked to the other information about an individual stored in EID. Currently, all ENFORCE workstations are integrated with IDENT.[31]

Figure 1 (pp. 24–25) is a simplified diagram of the ENFORCE system architecture.

Hardware

ENFORCE/IDENT workstation hardware includes a desktop or laptop computer running Windows 95 and various peripherals, including a LaserJet printer and IDENT-specific peripherals:

- camera to take digital photos and
- fingerprint scanner.

[31] According to INS officials, IDENT also functions as a stand-alone system at Inspections sites.

Each ENFORCE/IDENT client workstation also includes a video capture board (a device that captures digital photos and fingerprints). Workstations are located at INS Border Patrol stations, ports of entry to the United States, district offices, and asylum offices in the United States and U.S. territories.

The ENFORCE system hardware also includes two report servers, desktop PCs running Windows NT, which handle reporting requests from client workstations to EID and return completed reports to the client workstations. Each report server acts as a backup for the other.

EID is housed on two high-capacity, centralized servers running Digital Unix. These two servers also act as backups for each other.

Software

ENFORCE is an Oracle database application implemented in a traditional client-server architecture. Servers and client workstations run Oracle, Visual C++, and embedded SQL for database access.

EID is an Oracle database that stores INS enforcement data and provides the interfaces between ENFORCE and IDENT. (Most of the data exchanges between the ENFORCE and IDENT systems are accomplished through EID.)

Network

ENFORCE uses an enterprisewide private network that connects approximately 1,000 sites. The primary communications protocol is Transmission Control Protocol/Internet Protocol (TCP/IP).

The ENFORCE application workstations on each INS local area network (LAN) connects to EID over the INS wide area network (WAN) through routers.[32] (Remote-access dial-in capabilities are possible via the INS WAN). In addition, each LAN has a NetWare server for connectivity between workstations and peripherals. Information is passed around the LAN by Ethernet switches[33] (at new sites) and hubs[34] (at old sites). All

[32] A router is a device in a network that handles message transfer between computers.

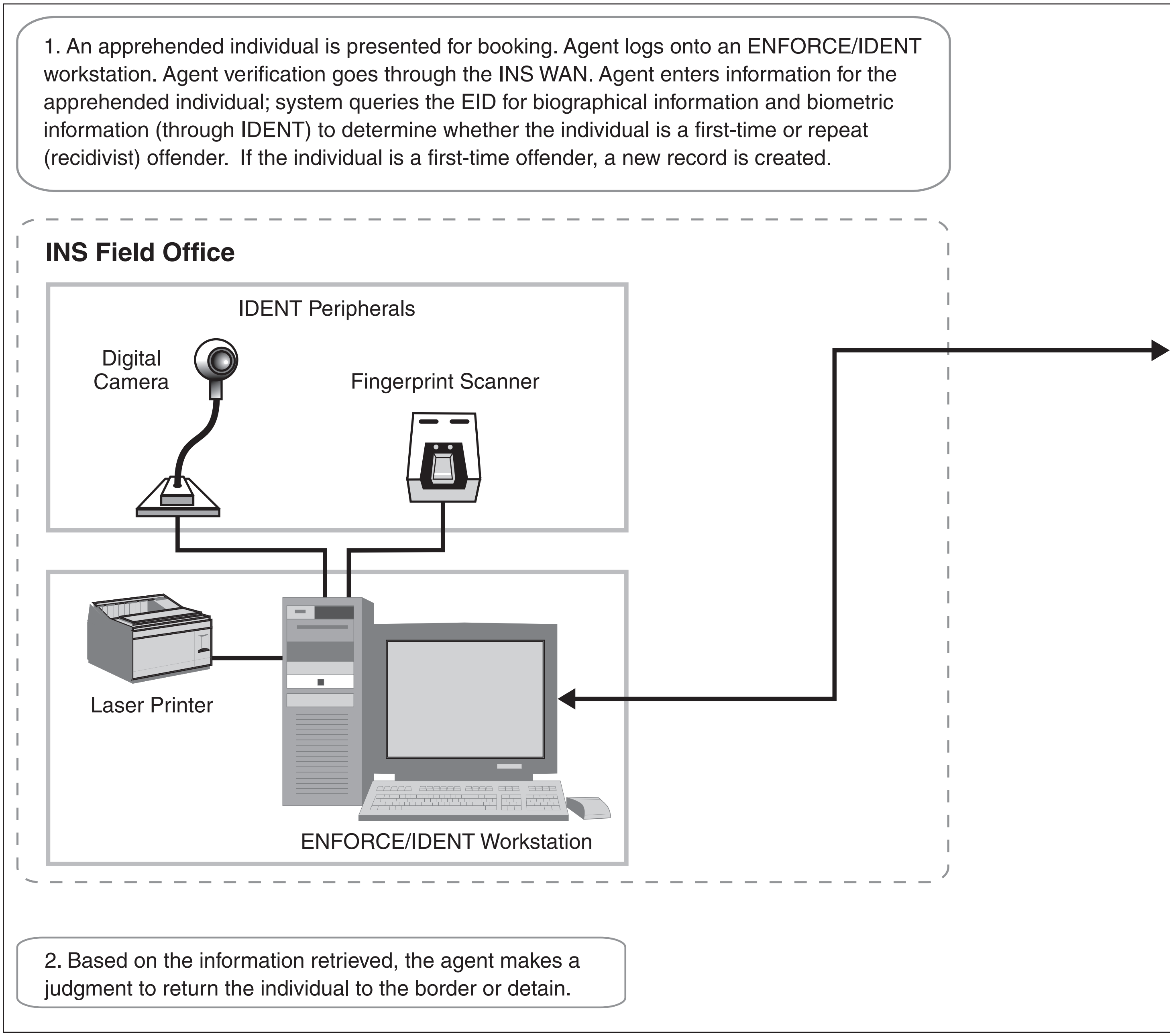
[33] A switch is a device that directs incoming messages along a path in a network.

[34] A hub is a device used to connect several computers together.

external connections (including to other government agencies, private contractors, and local law enforcement offices) are controlled through firewalls that prevent unauthorized access to or from the network.

[This page intentionally left blank.]

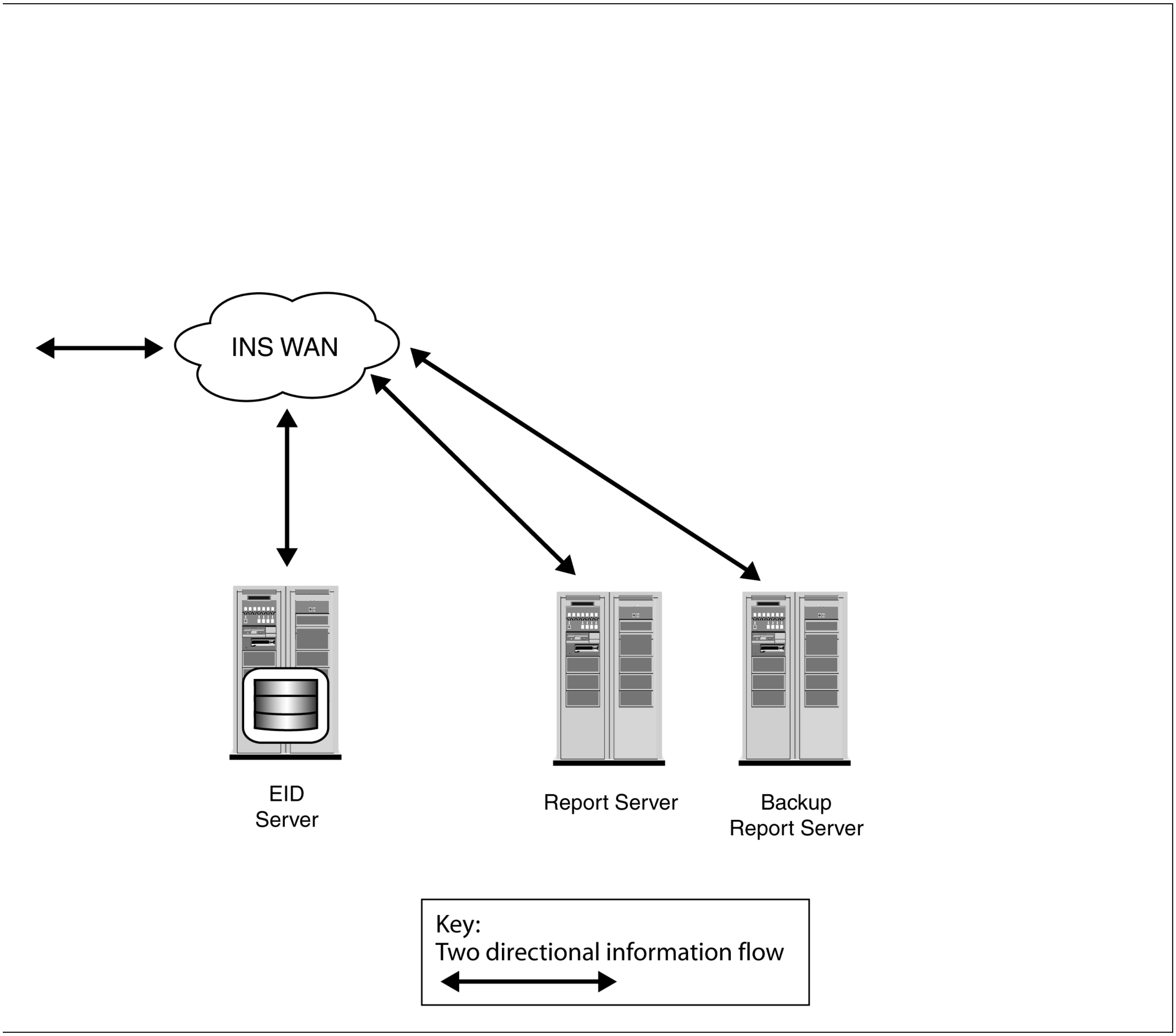
Figure 1: Simplified Diagram of ENFORCE System Architecture



1. An apprehended individual is presented for booking. Agent logs onto an ENFORCE/IDENT workstation. Agent verification goes through the INS WAN. Agent enters information for the apprehended individual; system queries the EID for biographical information and biometric information (through IDENT) to determine whether the individual is a first-time or repeat (recidivist) offender. If the individual is a first-time offender, a new record is created.

2. Based on the information retrieved, the agent makes a judgment to return the individual to the border or detain.

Source: GAO analysis based on INS data.


INS WAN
EID Server
Report Server
Backup Report Server
Key:
Two directional information flow

IDENT System Architecture

IDENT is a two-fingerprint identification system to allow INS offices to identify criminal aliens and repeat offenders of U.S. Immigration law. IDENT captures biometric, photographic, and biographical data. IDENT's basic function is to accept a pair of fingerprints, extract information from the prints, search the system's databases for prior encounters, create a new record when there is no prior encounter, and identify the current immigration status of those people already in the database or report that a new record is being created.

Like ENFORCE, IDENT is deployed to INS locations at Border Patrol stations, ports of entry, district offices, detention facilities, and asylum offices. At most sites, IDENT is integrated with ENFORCE's apprehension booking module; there is also a stand-alone IDENT capability for sites without ENFORCE. (That is, the IDENT client may reside on the same PC as the ENFORCE client, or it may reside on a PC without ENFORCE.)

Figure 2 (pp. 28–29) is a simplified diagram of the IDENT architecture.

Hardware

Each IDENT workstation (both stand-alone and ENFORCE/IDENT) includes the same hardware as described for the ENFORCE workstations: a desktop or laptop computer with a LaserJet printer, and IDENT-specific peripherals:

- camera to take digital photos and
- fingerprint scanner.

Each IDENT workstation also includes a video capture board (a device that captures digital photos and fingerprints).

The IDENT server application runs on a platform running the HP-UX operating system.

EID is also part of the IDENT architecture: this database is housed on two high-capacity, centralized servers, running Digital Unix, which act as backups for each other.

Software

IDENT is a client-server system, made up of client components geographically dispersed at numerous field sites and server components at a central site. The client and support components are connected with the server components through INS's WAN. IDENT can be integrated with ENFORCE or it can stand alone.

IDENT is an Oracle database application that processes the following databases, which are integrated into EID:

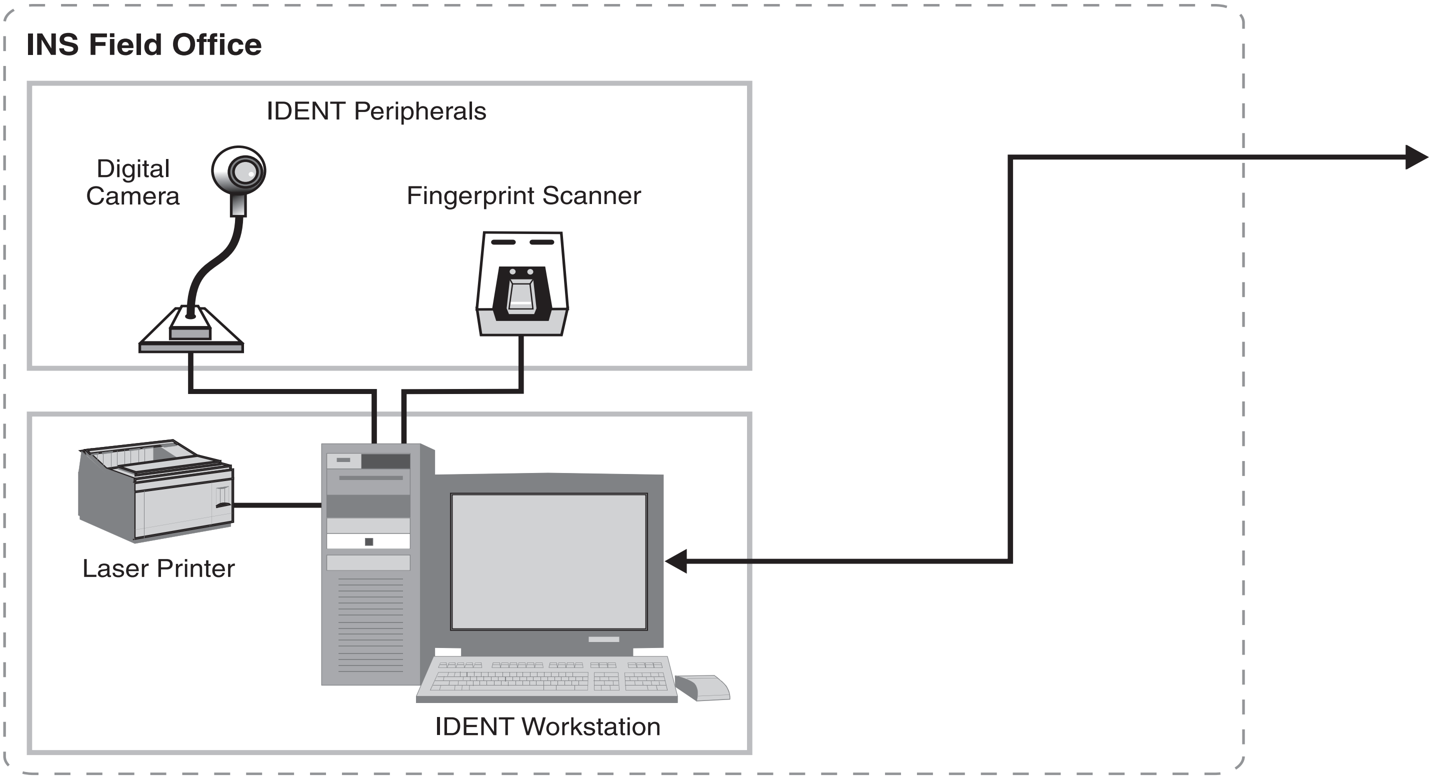
- Recidivist Database: This database contains enrollment records of repeat IDENT enrollees.
- Lookout Database: This database contains alien criminal records and selected recidivist records.

The IDENT application is implemented in C and C++, and it uses embedded SQL to access the database. IDENT uses proprietary biometric matchers. The database server is the same as that for ENFORCE.

Network

IDENT uses INS's WAN as its primary telecommunications network. In addition, similar to ENFORCE, the IDENT application workstations on each INS LAN connect to EID over the INS WAN through routers. In addition, each LAN has a server for connectivity between workstations and peripherals. Information is passed around the LAN by Ethernet switches (at new sites) and hubs (at old sites). All external connections (including to other government agencies, private contractors, and local law enforcement offices) are controlled through firewalls that prevent unauthorized access to or from the network.

Figure 2: Simplified Diagram of IDENT System Architecture

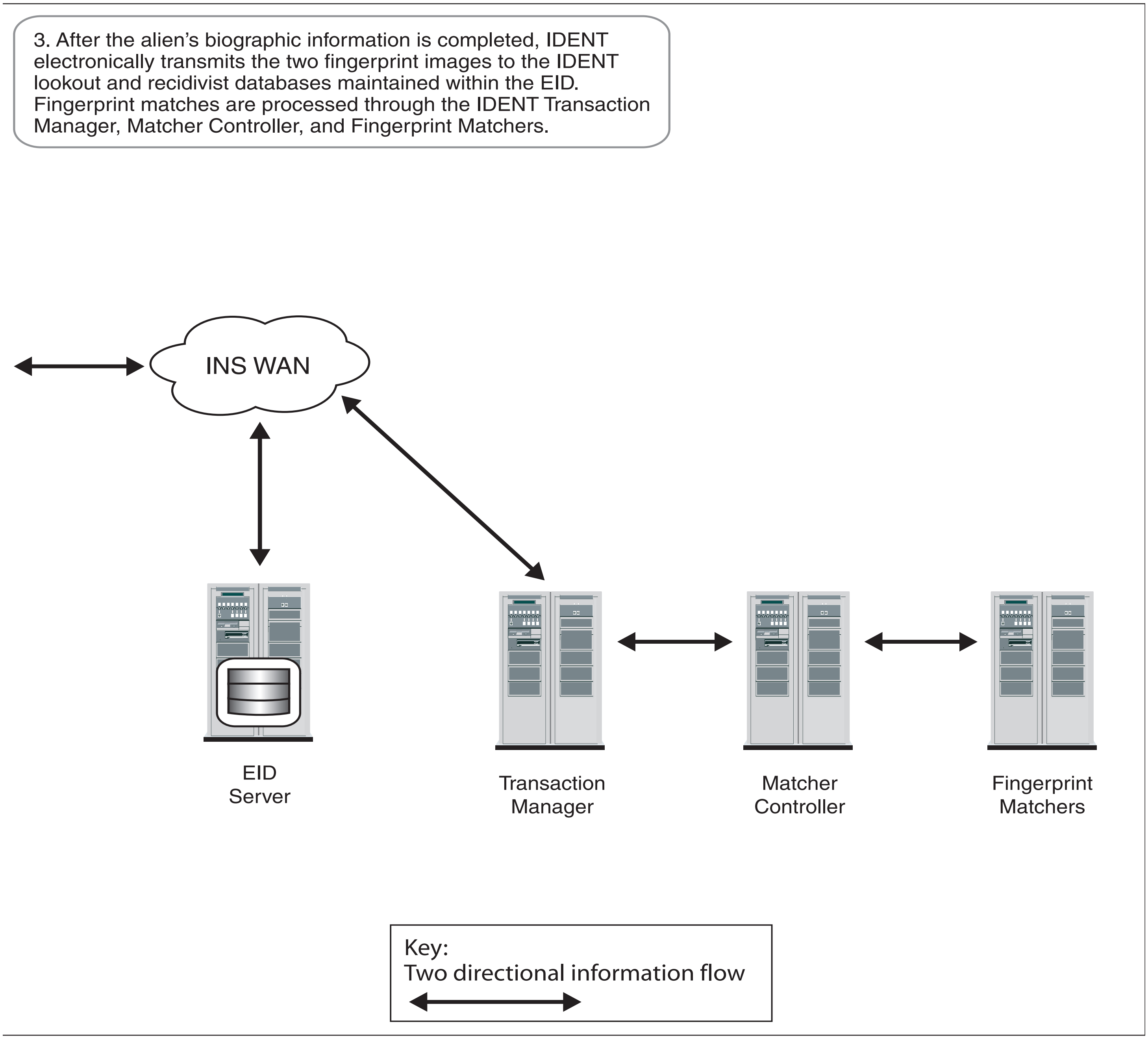


1. An apprehended individual is presented for verification/booking. Agent logs onto an IDENT workstation. The agent uses the fingerprint scanner to individually capture the alien's two index fingerprints, after which the IDENT camera automatically turns on and the agent takes the alien's picture.

2. Next, the agent inputs biographical information about the alien. The agent must enter the alien's sex, country of birth, country of citizenship, location of apprehension, date and time of apprehension, method of apprehension, name of the apprehending officer, the apprehending station, and the length of time the alien was illegally in the United States.

4. When IDENT identifies a potential fingerprint match, the IDENT terminal displays the photographs and fingerprints of the apprehended alien next to the photographs and fingerprints of the possible matches. If a match is visually confirmed by the agent, IDENT consolidates the records under a unique fingerprint identification number for the alien. When a match to a previous enrollment is not verified or there are no possible matches found, IDENT creates a new fingerprint identification number for the alien.

Source: GAO analysis based on INS data.



3. After the alien's biographic information is completed, IDENT electronically transmits the two fingerprint images to the IDENT lookout and recidivist databases maintained within the EID. Fingerprint matches are processed through the IDENT Transaction Manager, Matcher Controller, and Fingerprint Matchers.

ICPS System Architecture

The Integrated Card Production System (ICPS) consists of two main components: ICPS Print Services and the National Production Server (NPS). This system produces and prints three types of benefit cards:

- the optical Permanent Resident Card,[35]
- the Employment Authorization Document,[36] and
- the optical Laser Visa/Border Crossing Card.[37]

Depending on the card type, ICPS card production requests originate either at one of the five INS Service Centers in the United States or at the Department of State's Consular Affairs office. The requests are first processed through either of two card production request systems:

- the INS's Computer-linked Application Information Management System 3 (CLAIMS 3) system,[38] which processes Permanent Resident Cards and Employment Authorization Documents, or
- the Department of State's Consular Affairs System (DoSBCC),[39] which processes Laser Visas/Border Crossing Cards.

[35] A Permanent Resident Card, commonly known as a Green Card, documents a person's status as a lawful permanent resident with a right to live and work permanently in the United States. It also is evidence of registration in accordance with U.S. immigration laws.

[36] An Employment Authorization Document authorizes a person to work in the United States.

[37] The Border Crossing Card allows certain Mexican nationals entrance into the United States. Beginning in April 1998, INS began producing the Laser Visa, a new type of Border Crossing Card, to replace the previously issued paper-based card. INS prints the Border Crossing Card for the State Department, which is responsible for issuing visas.

[38] CLAIMS 3 is a distributed transaction-based system designed to (1) support high-volume processing of applications and petitions received by the INS, (2) capture fees and provide fund control for all monies received via the application/petition process, (3) provide case status to applicants/petitioners, and (4) support and record the results of the adjudication of each application/petition.

[39] DoSBCC is an Oracle-based system maintained by the INS to receive requests for Laser Visas/Border Crossing Cards submitted through the Department of State.

NPS then routes card production requests to any of six printer devices at three INS sites. (NPS also tracks card orders between the card production request systems and the printer devices.)

Five of the printers are identical brand printers and can print any of the three types of ICPS cards. The sixth printer can print only the Employment Authorization Document.

Figure 3 (pp. 34–35) is a simplified diagram of the ICPS system architecture.

Hardware

ICPS hardware includes

- 6 Oracle Windows NT servers for the “Gateway” database[40] (1 at each Service Center and 1 at the production facility),
- 1 Oracle Windows NT server for the NPS database,
- 11 Windows 95 client workstations for Print Services applications (2 at each Service Center and 1 at the production facility), and
- 6 printers.

The DoSBCC system includes the following system hardware: one Windows NT server.

Software

The ICPS is a client-server-based architecture. The ICPS and NPS servers run on the Windows NT operating system, with the client workstations operating on Windows 95. The NPS and Gateway databases are relational databases using an Oracle database management system.

[40] The Gateway database serves as the intermediary storage facility for the card orders and card production results. It captures print requests and sends them to the NPS.

ICPS Print Services consists of three Visual Basic executable components:

- CPR Loader: Extracts card production request data from CLAIMS 3 and inserts the data to the local Gateway database. Runs at all INS Service Centers. The executable files are 422 kilobytes (KB) in size.
- ProdReq Image Builder: Extracts images from printer Gateway databases to prepare them for use in printing.[41] Runs only at printer sites. The executable files are 305 KB in size.
- Results Processor: Extracts card production results data from the Gateway database and updates CLAIMS 3. Runs at all INS Service Centers. The executable files are 271 KB in size.

Additional software includes the following:

- ADO software (NPS and Service Centers): Middleware software used to communicate between Visual Basic and the Oracle database.
- Crystal Reports (NPS): Report generation software used to display data in the form of on-line reports via the NPS Web site. It is installed only on the INS Intranet Web server, not on any of the NPS servers.

The DoSBCC system software suite includes the following:

- BCC executive
- Applicant Processor
- CPR Loader and Results Processor

Network

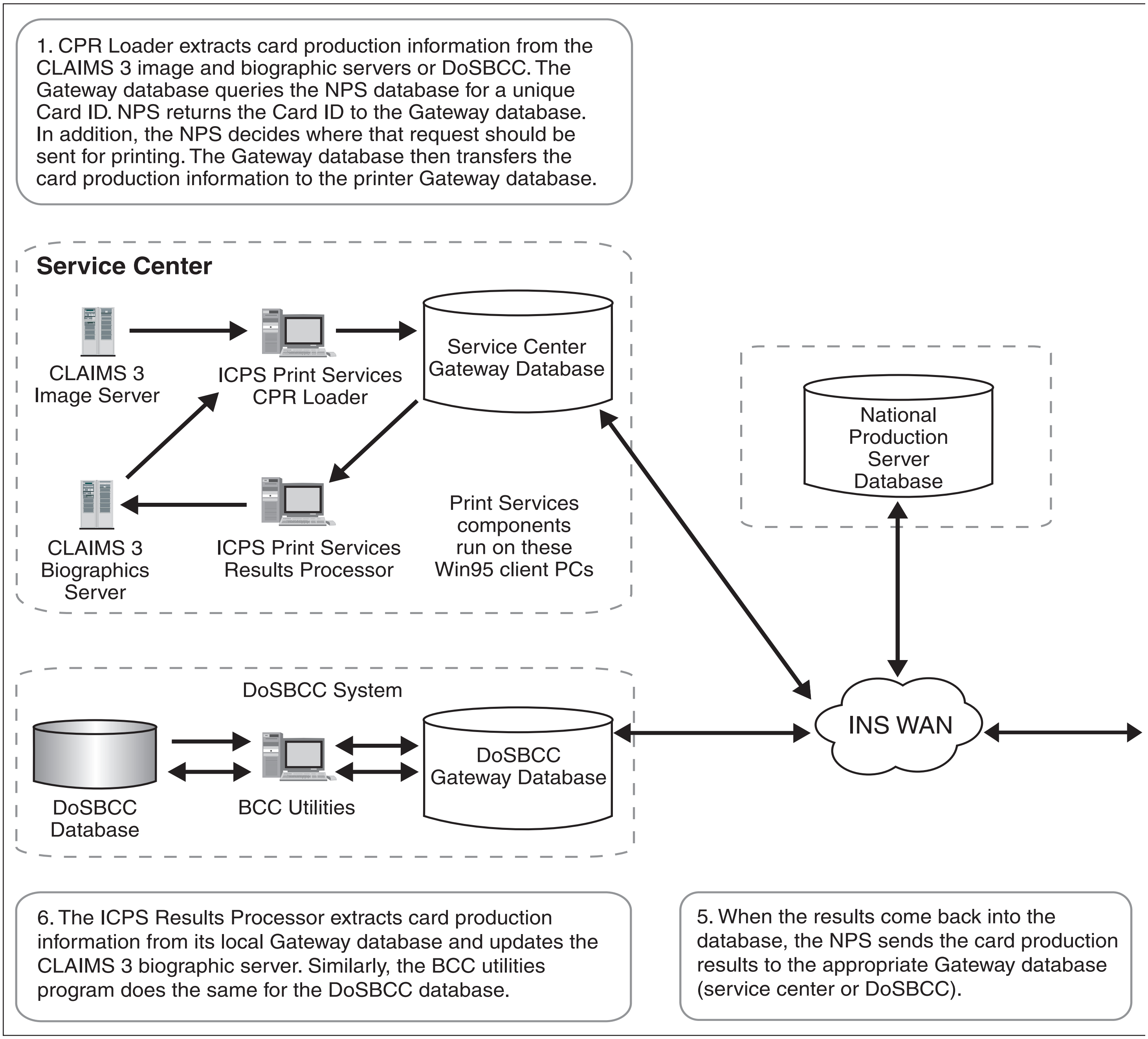
The primary communications protocol is TCP/IP, which is used for communication between the ICPS client and server through the INS LAN

[41] The Central Manufacturing Executive (CME) software controls each of the assembly line devices involved in card production.

and WAN. The Gateway databases are connected to each other in a star configuration[42] via database links across the INS WAN, allowing every database to communicate with every other database. This provides a path for card transfer in the event of a failure of the central NPS system.

[42] In a star configuration, all messages go through a central node that serves as a switch, receiving messages and forwarding them to a destination node.

Figure 3: Simplified Diagram of ICPS System Architecture

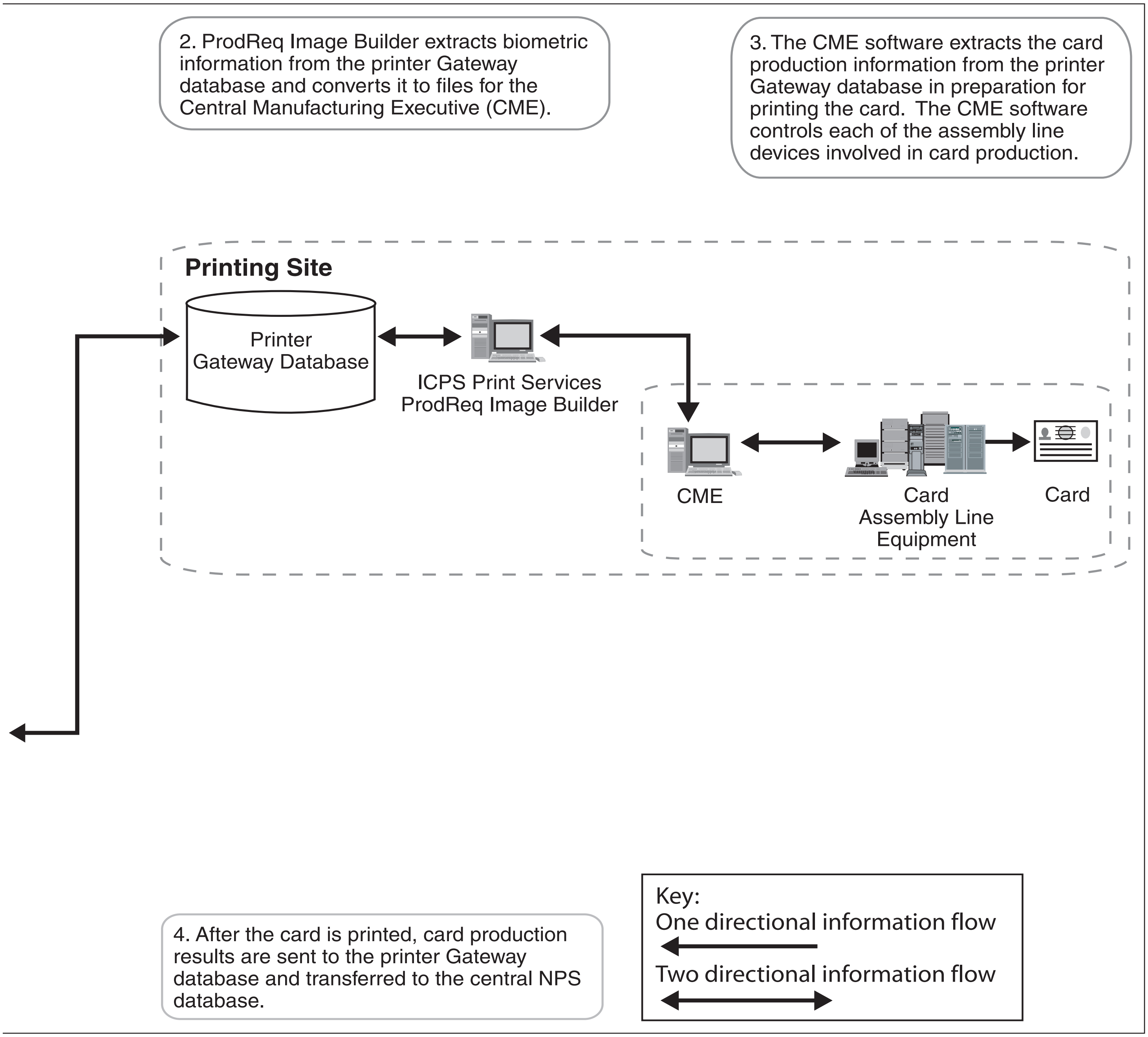

Service Center
CLAIMS 3 Image Server
ICPS Print Services CPR Loader
Service Center Gateway Database
CLAIMS 3 Biographics Server
ICPS Print Services Results Processor
Print Services components run on these Win95 client PCs
National Production Server Database
DoSBCC System
DoSBCC Database
BCC Utilities
DoSBCC Gateway Database
INS WAN

1. CPR Loader extracts card production information from the CLAIMS 3 image and biographic servers or DoSBCC. The Gateway database queries the NPS database for a unique Card ID. NPS returns the Card ID to the Gateway database. In addition, the NPS decides where that request should be sent for printing. The Gateway database then transfers the card production information to the printer Gateway database.

6. The ICPS Results Processor extracts card production information from its local Gateway database and updates the CLAIMS 3 biographic server. Similarly, the BCC utilities program does the same for the DoSBCC database.

5. When the results come back into the database, the NPS sends the card production results to the appropriate Gateway database (service center or DoSBCC).

Source: GAO analysis based on INS data.



2. ProdReq Image Builder extracts biometric information from the printer Gateway database and converts it to files for the Central Manufacturing Executive (CME).

3. The CME software extracts the card production information from the printer Gateway database in preparation for printing the card. The CME software controls each of the assembly line devices involved in card production.

4. After the card is printed, card production results are sent to the printer Gateway database and transferred to the central NPS database.

Printing Site
Printer Gateway Database
ICPS Print Services ProdReq Image Builder
CME
Card Assembly Line Equipment
Card
Key:
One directional information flow
Two directional information flow

GAO's Mission

The General Accounting Office, the investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to daily E-mail alert for newly released products" under the GAO Reports heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone:	Voice:	(202) 512-6000
	TDD:	(202) 512-2537
	Fax:	(202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, managing director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON ♻ RECYCLED PAPER

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Service Requested

Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00

[redacted]